

# Hitachi NAS Platform and Hitachi Unified Storage System Installation Guide

---

Release 13.8

# Legal Notices

© 2011, 2019 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

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 Vantara LLC 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 Vantara LLC.

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.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found at <https://www.hitachivantara.com/en-us/company/legal.html>.

---

# Contents

<b>Legal Notices.....</b>	<b>2</b>
<b>Chapter 1: About this document.....</b>	<b>7</b>
Accessing product documentation.....	8
Getting help.....	8
Comments.....	8
Applicable products.....	8
Target configurations.....	9
Target audience.....	10
Related documentation.....	10
Training offerings.....	11
<b>Chapter 2: System requirements.....</b>	<b>12</b>
General specifications.....	12
Browser support.....	12
License key overview.....	13
<b>Chapter 3: Verifying your system components.....</b>	<b>14</b>
Installation and configuration process flowchart.....	14
System contents.....	19
Checkpoint.....	19
System layouts.....	19
Possible system layout scenarios.....	23
Checkpoint.....	24
<b>Chapter 4: Assembling the physical layer.....</b>	<b>25</b>
Recommended toolkit.....	25
Preparing for an installation.....	26
Attaching a rack stabilizer plate.....	27
Mounting the PDUs.....	27
Installing the PDU rack cabling tray.....	28
Mounting the storage.....	29
Reviewing the HUS controller box hardware.....	29
Reviewing the HUS drive box hardware.....	33
Mounting the storage components.....	36
Mounting the FC switches.....	37

Mounting the 10 GbE switches.....	38
Configuring the Ethernet switch to the storage system .....	38
Configuring HyperTerminal for the Ethernet switch configuration.....	38
Recovering from a lost password during switch configuration.....	39
Mounting an HNAS or HUS File Module server.....	39
Reviewing the server hardware.....	40
Server installation requirements.....	45
Mounting the server components.....	48
Installing the Ethernet and FC port adapters.....	48
Mounting an external SMU.....	50
Reviewing the SMU 400 hardware.....	50
SMU 400 installation requirements.....	52
Mounting an SMU 400.....	54
Cabling the system.....	56
Connecting to the server.....	65
Connecting to the storage.....	67
Connecting the power cables.....	70
Checkpoint.....	70
<b>Chapter 5: Configuring the logical layer.....</b>	<b>72</b>
Preparing for system configuration.....	72
Configuring the storage system.....	73
Creating the RAID groups.....	74
Creating the storage volumes.....	76
Configuring the host groups.....	78
Configuring additional storage settings based on firmware.....	81
Setting up the OS and software on an SMU.....	86
Configuring a server administrative IP to access embedded SMUs.....	86
Installing the CentOS operating system.....	88
Initially configuring an external SMU.....	90
Installing and configuring the SMU software.....	91
Configuring an HNAS Platform or HUS File Module server.....	94
Configuring the first HNAS or HUS File Module server.....	95
Configuring the second HNAS or HUS File Module server.....	99
Adding the servers as managed servers in the SMU.....	103
Building a two-node cluster.....	103
Configuring the Ethernet switch as a cluster switch.....	106
Configuring the Ethernet switch to the storage system .....	108
Configuring HyperTerminal for the Ethernet switch configuration.....	108
Recovering from a lost password during switch configuration.....	108
Configuring a system with an embedded SMU.....	109
Customizing the server administrative IP address.....	109



Using the server setup wizard.....	110
Configuring a system with an external SMU.....	112
Initially configuring an external SMU.....	112
Selecting external NAS Manager-managed servers.....	113
Using the server setup wizard with a single-node configuration.....	114
Backing up configuration files.....	115
Backing up the server registry.....	115
Backing up the external SMU configuration.....	115
<b>Chapter 6: Accepting your system.....</b>	<b>116</b>
Checkpoint.....	116
Additional system verification tests.....	118
Verifying the SD superflush settings.....	118
<b>Appendix A: Upgrading storage firmware.....</b>	<b>119</b>
Upgrading storage array firmware.....	119
<b>Appendix B: Configuring superflush settings.....</b>	<b>122</b>
Configuring the superflush settings.....	122
<b>Appendix C: Upgrading HNAS or HUS File Module server software.....</b>	<b>123</b>
Upgrading operating systems.....	123
Upgrading the server software.....	123
Upgrading server firmware.....	124
Upgrading firmware on servers not usually managed by the SMU.....	124
<b>Appendix D: Running the NAS-PRECONFIG script.....</b>	<b>126</b>
Running the <b>NAS-PRECONFIG</b> script.....	126
<b>Appendix E: Using a virtual SMU.....</b>	<b>128</b>
About configuring a virtual SMU.....	128
Installation requirements.....	130
Configuring vSwitches.....	130
Deploying CentOS SMU VMs.....	131
Installing SMU software in a VM.....	132
Configuring VM resource allocations.....	134
Installing VMware tools.....	134
Upgrading the OS for a virtual SMU.....	135
<b>Appendix F: Upgrading an external SMU.....</b>	<b>136</b>
About upgrading an external SMU.....	136
Upgrading the SMU OS.....	136
Upgrading the NAS Manager software.....	138

<b>Appendix G: Running the SMU-CONFIG script.....</b>	<b>140</b>
Running the SMU-CONFIG script.....	140
<b>Appendix H: Adding nodes to an N-way cluster (three-plus nodes).....</b>	<b>144</b>
Maximum number of nodes supported.....	144
Adding nodes to an N-way cluster.....	145
Cluster cable configurations.....	146

---

## Chapter 1: About this document

This manual guides you through the installation process, one phase at a time, with checkpoints at the end of each phase to minimize potential delays.

The installation process includes the following phases:

- *Systems Assurance*

Before arriving onsite, the *systems assurance* phase should have been completed, which includes capturing the architecture and design expectations related to the installation and the related site survey information. This must be performed in advanced to ensure an appropriate solution is architected for the customer's needs. Results of the systems assurance is shipped with the system in the enclosed documentation wallet.

- *Preinstallation Verification*

During this phase, the shipment is confirmed, and an installation date and duration should be agreed on. The systems assurances and environmental requirements will be reviewed one final time to ensure a smooth installation is accomplished.

- *Physical Layer Installation*

During this phase, all system components are unpacked, racked, and cabled according to the preestablished design. At the end of this phase, the system undergoes a power-on check to ensure all the hardware and related components are healthy.

- *Logical Layer Installation*

Most of this phase is designed to be completed by the customer, as it involves the use of configuration wizards to enter various customer, infrastructure, and network service information. During this phase, a basic system is automatically configured with a storage pool, file system, and a single share and export. This allows for the connection of clients to the system to verify it is complete and healthfully operating.

- *Service Acceptance*

The final phase is used to establish a connection to customer support, verify the Call-Home information is received by the customer support database automatically, and establish service entitlement to confirm support levels and support portal access.

## Accessing product documentation

Product user documentation is available on Hitachi Vantara Support Connect: <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

[Hitachi Vantara Support Connect](https://support.hitachivantara.com) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: [https://support.hitachivantara.com/en\\_us/contact-us.html](https://support.hitachivantara.com/en_us/contact-us.html).

[Hitachi Vantara Community](https://community.hitachivantara.com) is a global online community for Hitachi Vantara 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](https://community.hitachivantara.com), register, and complete your profile.

## Comments

Please send us your comments on this document to [doc.comments@hitachivantara.com](mailto: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 Vantara LLC.

**Thank you!**

## Applicable products

Applicable products include:

Server Series	Server Model	Current Offerings	Discontinued, but still supported
4000	4060, 4080 and 4100	VSP G200, VSP G350, VSP G370, VSP G400, VSP G600, VSP G700, VSP G800, VSP G900, VSP G1000, VSP G1500, VSP F200, VSP F350, VSP F370, VSP F400, VSP F600, VSP F700, VSP F800, VSP F900, VSP 5100/5500, VSP 5100H/5500H, VSP E990	HUS VM, HUS 110, HUS 130, HUS 150, VSP
4000	4040	VSP G200, VSP G400, VSP G600, VSP G800, VSP G1000, VSP G1500, VSP F200, VSP F400, VSP F600, VSP F800	HUS VM, HUS 110, HUS 130, HUS 150, VSP
3000	3080 and 3090	VSP G200, VSP G400, VSP G600, VSP G800, VSP G1000, VSP G1500, VSP F200, VSP F400, VSP F600, VSP F800	HUS VM, HUS 110, HUS 130, HUS 150, VSP

## Target configurations

Configurations include:

- Single server systems with storage (SAN or direct-attached)
- Clustered systems with up to two nodes with storage (SAN or direct-attached)
- Cluster (two or more nodes in a cluster, up to the supported maximum number of nodes, with an attached SAN)
- System management unit (SMU) as required by the customer site for the above configurations
- Optional standby SMU, if required by the customer configuration



**Note:** A server is called a node in clustered configurations.

## Target audience

Before attempting to install a Hitachi NAS Platform system and storage arrays, the following are required:

- Training with the Hitachi NAS Platform server and storage arrays, and their installation procedures.
- Basic Microsoft Windows and UNIX administration skills.

## Related documentation

*System Access Guide* (MK-92HNAS014) (MK-92USF002): In PDF format, this guide 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) (MK-92USF007): In PDF format, this guide provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading firmware, monitoring servers and clusters, the backing up and restoring configurations.

*Storage System User Administration Guide* (MK-92HNAS013) (MK-92USF011): In PDF format, this guide 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) (MK-92USF003): In PDF format, this guide 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) (MK-92USF004): In PDF format, this guide 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) (MK-92USF005): In PDF format, this guide provides information about the Data Migrator feature, including how to set up migration policies and schedules.

*Storage Subsystem Administration Guide* (MK-92HNAS012) (MK-92USF006): In PDF format, this guide 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) (MK-92USF008): In PDF format, this guide provides information about configuring the server to take and manage snapshots.

*Replication and Disaster Recovery Administration Guide* (MK-92HNAS009) (MK-92USF009): In PDF format, this guide 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) (MK-92USF010): In PDF format, this guide 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) (MK-92USF012): In PDF format, this guide provides information about configuring the server to work with NDMP, and making and managing NDMP backups. Also includes information about Hitachi NAS Synchronous Image Backup.

*Command Line Reference*: Describes how to administer the system by entering commands at a command prompt.

*Hitachi NAS Platform 3080 and 3090 G1 Hardware Reference*(MK-92HNAS016): In PDF format, this guide provides an overview of the first-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.

*Hitachi NAS Platform 3080 and 3090 G2 and Hitachi Unified Storage File Module Hardware Reference* (MK-92HNAS017) (MK-92USF001): In PDF format, this guide provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.

*Hitachi NAS Platform and Hitachi Unified Storage File Module Series 4000 Hardware Reference* (MK-92HNAS030) (MK-92HNAS030): In PDF format, this guide provides an overview of the HNAS Series 4000 and Hitachi Unified Storage File Module server hardware, describes how to resolve any problems, and how to replace potentially faulty components.

*Release notes*: Provides the most up-to-date information about the system, including new feature summaries, upgrade instructions, and fixed and known defects.



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

## Training offerings

Hitachi Vantara offers formalized training to authorized partners and customers. Please contact your Hitachi Vantara representative for more information, as it is required before attempting any system installation or repairs.

---

## Chapter 2: System requirements

Confirm the system meets the minimum requirements to efficiently use the system and take advantage of its features.

### General specifications

Hitachi Vantara provides support for a final quote and configuration review. Key account information and solution attributes will be recorded, and the overall delivery objectives, goals, and prerequisites will be discussed.

Because the type and number of components might differ for each system and storage server, refer to the documentation wallet provided with the system to ensure its requirements are met before any hardware components arrive onsite. Contact customer support immediately if you have any questions or concerns.

See the *Hitachi NAS Platform Series 4000 Hitachi Unified Storage File Module Hitachi High-performance NAS Platform* and the specifications provided for the 4000 series system for more information.

See the *Hitachi NAS Platform 3080 and 3090 G2 Hardware Reference* and the specifications provided for the HNAS 3080 and HNAS 3090 servers for more information.

### 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 Internet Explorer: version 11.0 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.



## License key overview

Servers are provided with the software already installed. You add the licenses for the services you want. When you replace a server, you need to manually order a replacement set of licenses. This is a two stage process, where you first obtain a set of emergency license keys to get the system up and running, and then obtain a permanent set of keys.

- Licensed services (keyed)

License keys are required to add services to servers and can be purchased and added as required by the customer. A License Certificate identifies all of the purchased services and should be kept in a safe place. The User Documentation Wallet that was shipped with the system includes the License Certificate. Licensed software packages are described in [Building a two-node cluster \(on page 103\)](#).

- Obtaining customer license keys

License keys are included in the normal Insight order process. If you encounter problems with the key process, please email: <mailto://tbkeys@hds.com>

- Permanent key

The permanent key is obtained through a specialized process requiring both customer and system information. Typically the information will include the customer number, serial number of the storage system, and the feature to be activated.



**Note:** Permanent license keys for a replacement server are *normally* provided within seven days.

- Temporary key

For customers who want to test a particular feature, a temporary key is available. The temporary key enables software features for a specified period of time (60 days), after which the function is disabled. During or after the trial period, the customer may elect to purchase a permanent key. A 60-day All Suite temporary key can be ordered in Insight. However, [tbkeys@hds.com](mailto://tbkeys@hds.com) can assist for keys required outside of the Insight ordering process.

- Emergency key

Emergency key generation tools for all current NAS File OS versions are kept in each contact center. For emergency situations, an emergency key can be obtained from the GCC for your geography. Emergency keys will remain functional for 14 days from the creation date. Emergency keys must be replaced with a permanent key.



**Note:** See the *System Access Guide* for a complete list of End Licensing Agreements.

---

## Chapter 3: Verifying your system components

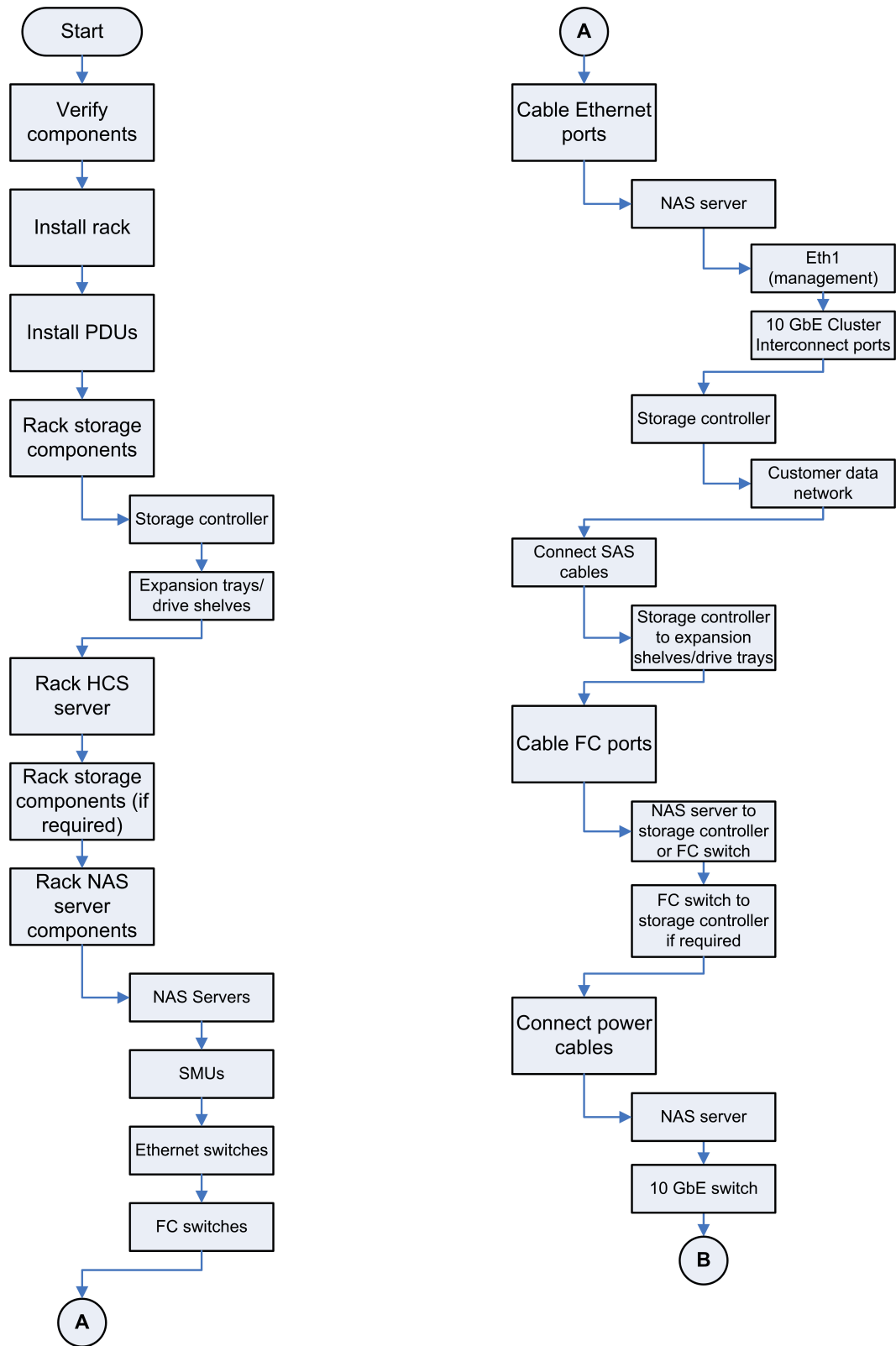
The logistics of installation location, timing, and onsite resources are determined in advance, including the need for any additional support from Hitachi Vantara for any partners. Confirmation of shipping materials are verified and a preinstallation checklist is reviewed with the customer.

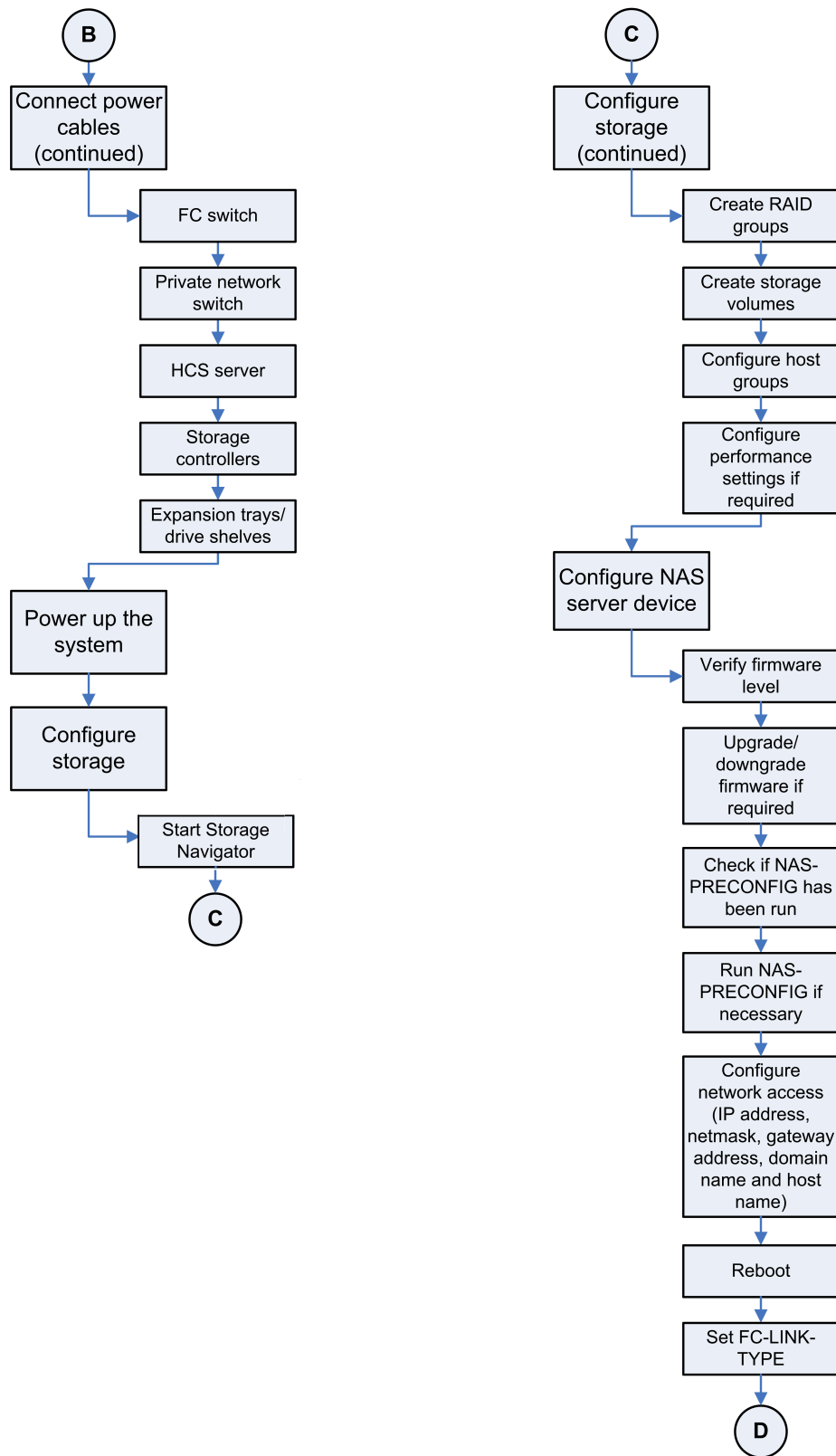


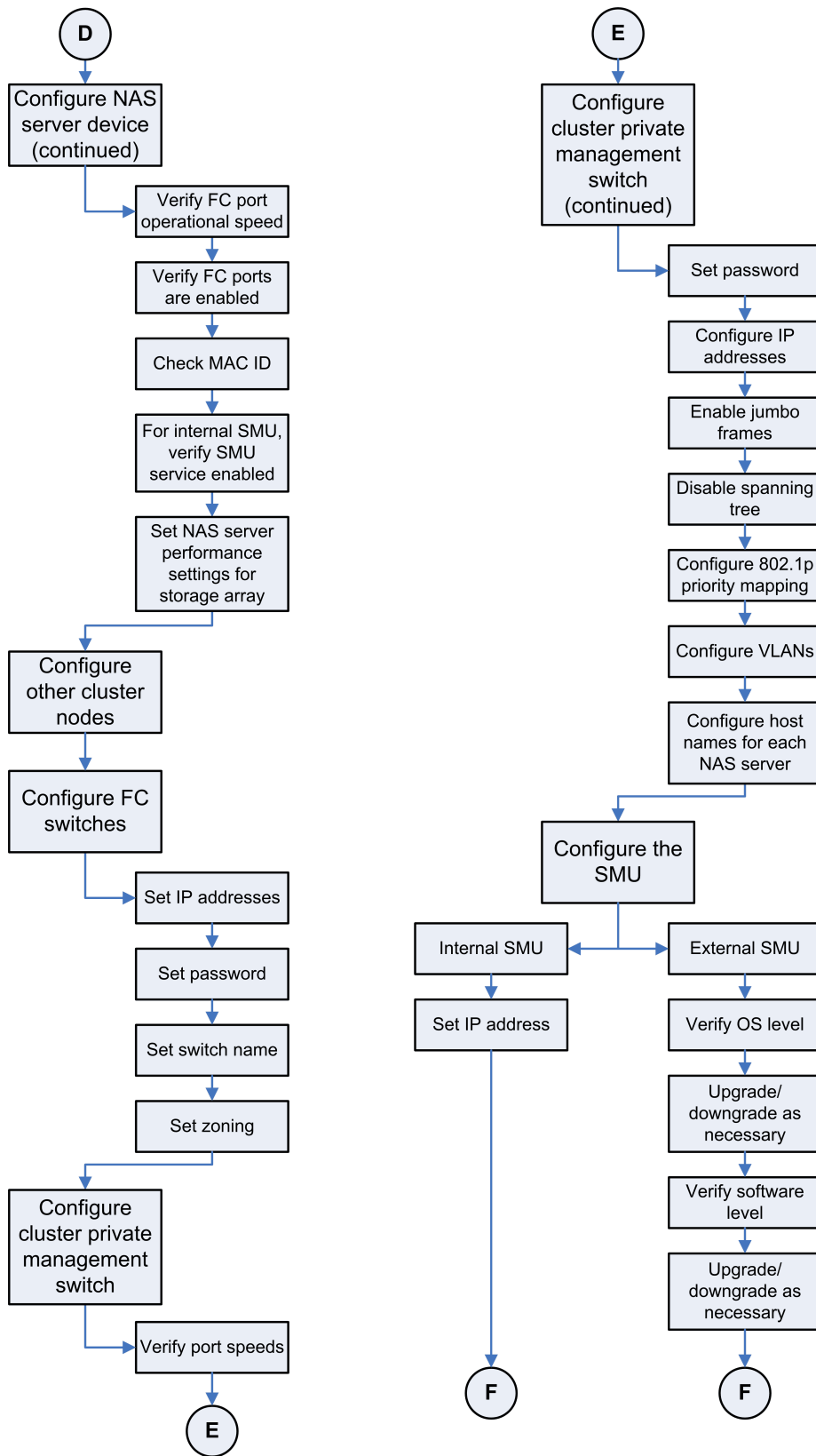
### Installation and configuration process flowchart

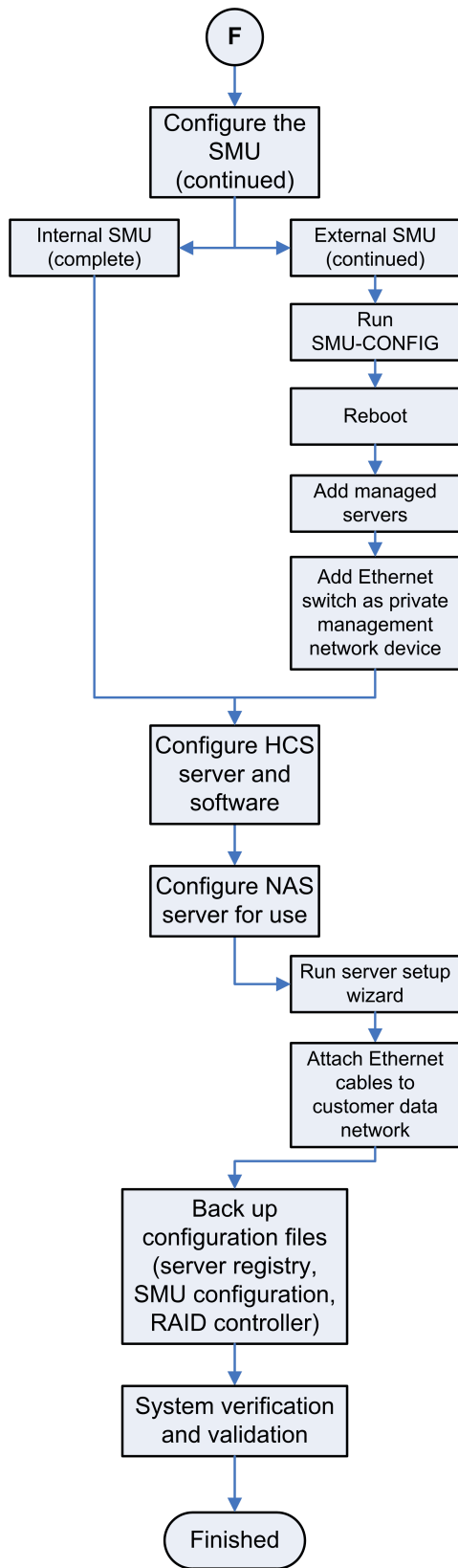
The flowchart in this section shows the high-level process steps you can follow when installing and setting up a system.

**!** **Important:** If any step in the process does not apply to your configuration, skip that step.









## System contents

The following checklist includes the components necessary for a basic system configuration:

- Server (also called a *node* in clustered configurations)
  - Documentation wallet (includes the checklist needed to verify that all components have arrived)
  - Mounting kit (rails, nuts, screws, and so on)
  - Management Ethernet cross-over cable for connecting a laptop
  - Power cable
- Storage array or arrays, depending on the customer order. Each array consists of at least one controller tray, and may also include additional drive trays. For each tray, there should be:
  - A mounting kit (rails, nuts, screws, and so on)
  - Cables for connection to the server or two-node cluster (in direct-attach configurations) or FC switches (for clusters of 3 or more nodes)
  - Power cables
  - For each array, there should also be documentation and software

## Checkpoint

### Procedure

1. Locate the system checklist in the documentation wallet included with the storage system.
2. Verify that the system checklist matches your order.
3. Using the checklist, verify that all components have arrived safely, and that you have all the items needed for your installation.


### Result

Contact the customer support if you are missing any components and are unable to pass this checkpoint.

## System layouts

This section provides recommendations for a single server with direct-attached storage layout and one and two-node clusters with direct-attach storage and SMU. Before installing any components, refer to your system layout plan.

Depending on the system, design the layout in blocks: management, server, and storage.

Block type	Description
Management block	In a single-server configuration, the embedded system management unit (SMU) manages the system and provides management Ethernet connections. In clustered systems and some single-node systems, an external system management unit (SMU) provides the management functionality.
Server block	<p>The server block includes the Hitachi NAS Platform or the Hitachi Unified Storage File Module server.</p> <p> <b>Note:</b> You may connect the storage by using either direct FC connections (DAS) to a storage array or tape library, or an FC switch (SAN); however, Hitachi Data Systems recommends using one connection scheme as opposed to mixing both DAS and SAN connections.</p>
Storage block	The storage block consist of the storage arrays. To keep the storage array together, you may float the server block to avoid spanning it. Avoid crossing FC cables over management or server blocks, or from the management cabinet to an expansion cabinet.

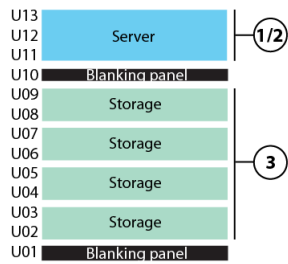
The location of these blocks can vary depending on the enclosure layout. For instance, in a basic configuration, the provides both management and server block functionality as a standalone unit.

All components can be mounted in standard EIA 19-inch cabinets that have a minimum depth of 1000mm.



**Note:** Always install hardware starting from the bottom of the cabinet to avoid personal injury. The documents listed below provide a full specification on how to configure and administer the storage enclosures attached to the storage server.

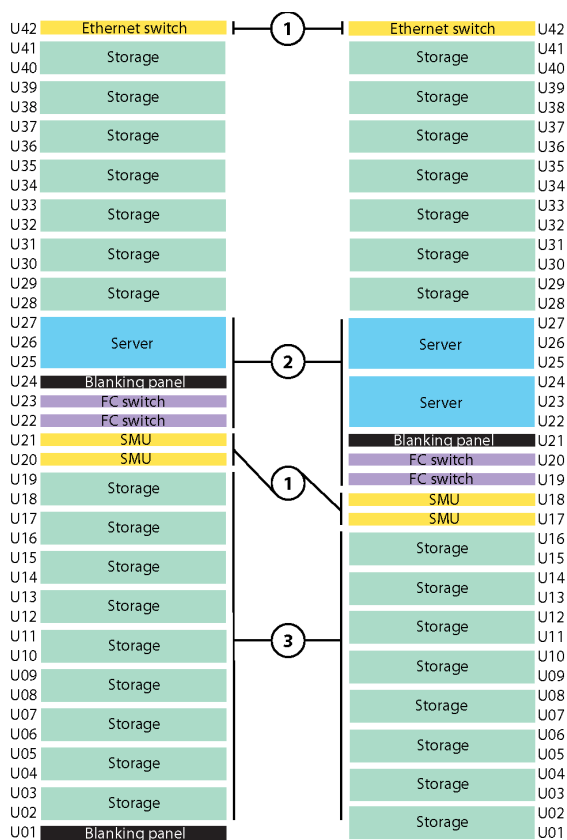




**Figure 1 Single server with direct-attach storage**

**Table 1 Basic configuration layout for single server with direct-attach storage**

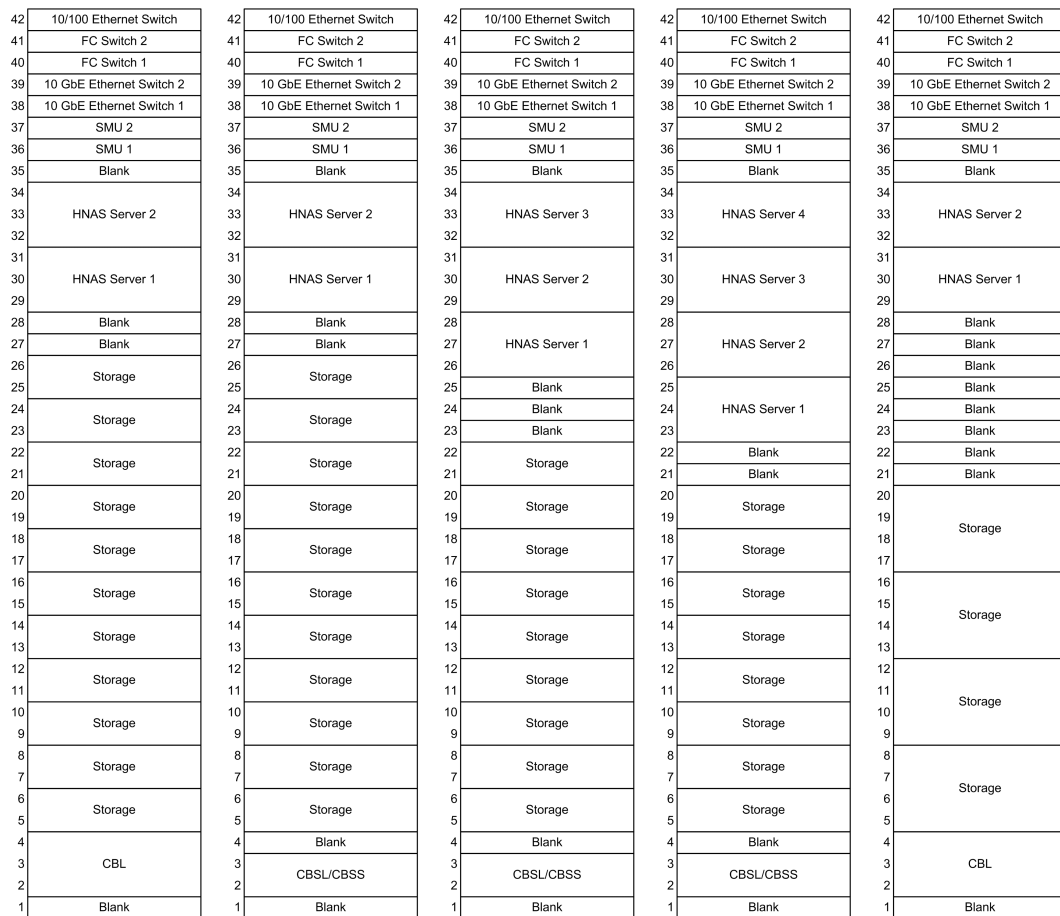
Item	Description
1	Management block
2	Server block
3	Storage block



**Figure 2 NAS Platform 4040: examples of one and two-node clusters with storage and SMUs**

**Table 2 Configuration layout for a single server and two-node cluster with storage and SMUs**

Item	Description
1	Management block
2	Server block
3	Storage block



**Figure 3 Various examples of two-node and N-way (3+ node) clusters with storage and SMUs**



**Note:** CBSL, CBSS, CBL: Controller box small large, small small, large, respectively.

## Possible system layout scenarios

A number of system layout scenarios are possible, but the one you use depends on your system components and environment. This section describes the building rules and cabling for the system assembly operation. These scenarios detail build situations for the different systems.

While there are established scenarios, there can always be exceptions. Decisions about alterations for specific situations are made by Technical Specialists. If you have one of these exceptional situations, consult with a Technical Specialist.

Ground rules for the build:

- If the ICC switches are non-existent, those spots stay blank.
- If the second SMU is non-existent, that spot stays blank.
- If the FC switches are non-existent, those spots stay blank.
- If there is more storage ordered than what can be mounted up until U26, a second rack must be ordered, or the excess storage must shipped separately.
- In the case of three or four servers, storage can go up to 1U below the first server.

General notes:

- The blank space on U4 will only be filled if a CBL (controller box large format) is ordered, otherwise this space stays blank.
- U1 will always remain blank.
- There must always be at least one blank space between the storage and the server.

## Checkpoint

### Procedure

1. Locate the *storage array configuration* insert in the documentation wallet included with the storage server.
2. Locate the system layout plan that was developed with your account representative.
3. If you are using an existing rack for installing the system, ensure there is enough unit (U) space available to accommodate your system layout.
4. If you ordered a system cabinet, ensure there is enough floor space available.
5. Ensure the system's power and cooling requirements are met, as indicated on the configuration insert in the documentation wallet.

### Result

Contact the customer support if for any reason the location selected is unsuitable and you are not able to pass this checkpoint.

---

## Chapter 4: Assembling the physical layer

Assembling the physical layer is identifying and installing the hardware components for the system.

### Recommended toolkit

The following tools are recommended:

- Antistatic protectors
- Phillips-head screwdrivers: heavy duty #2 x 100mm and #3 x 150mm, and electrostatic discharge (ESD) safe #0 x 50mm with cushioned grips (optionally, a screwdriver with an angled head for tight spaces)
- Allen-head screwdriver, 1/8 in.
- Flat-head screwdriver
- Standard socket set, which includes 1/2 and 9/16 in. six-point sockets
- Reversible ratchet, 1/4 in.
- Crescent wrench, 1 in.
- Proto adjustable wrench, 6 in.
- Locking tape measure, 12 ft
- Pliers
- Electrical scissors
- Utility knife
- Cage-nut tool
- Velcro tie-wraps
- Wire ties/wire-tie gun (for power cables only, as wire-ties might damage fiber cables)
- Label maker (optionally, select one that is specifically for labeling cables)

- Flashlight
- Heavy-duty wireless power drill/screwdriver (optional)
- LC loopback
- Fiber adapter with duplex LC-to-LC
- Latest copies of Hitachi NAS File Operating System, in case the system requires an update
- Laptop with terminal emulator
- KVM Console to USB 2.0 Portable Laptop Crash Cart Adapter

## Preparing for an installation

To expedite your installation experience, consider the following recommendations:



**Note:** Time requirements for completing tasks are based on a two-person installation team following these recommendations.

### Procedure

1. Unpack all system components from their shipping containers, and organize them near the cabinet to which they are to be installed. Take an inventory to ensure all the components arrived, and are in working condition.



**Caution:** Lift the server from the bottom of the chassis. Do NOT lift the server chassis by the plastic handles. These handles are for sliding the server in to the rack. Do NOT lift the server chassis by placing your hands inside the casing, as it can bend the chassis and make it difficult to install the bezel.

2. Gather all the rail kits, which are shipped with their respective components.



**Caution:** Use caution when handling the rails as they can have extremely sharp edges.

3. Unwrap rails and separate the items in the kit, grouping component items.
4. Sort the right and left side for a component (such as storage array rails), and place in front of the rack.
5. Sort all clips, screws, and washers for front and rear mountings for the component, and place them by the rack.

6. Install the storage array rails, starting from the bottom of the rack.

Size one rail to the rack and lock it in position with a clip or screw, then use the rail as a guide when assembling the remaining rail kits.

7. Install the server rails.
8. Install remaining storage array rails, if necessary.

9. Insert and secure components in their respective rails, starting from the bottom.

## Attaching a rack stabilizer plate

A rack stabilizer plate and mounting hardware are supplied with some system configurations. Hitachi Vantara recommends that you always use the stabilizer plate when provided. Use of a stabilizer plate is required for those installations with dense trays.

The stabilizer contains two holes for securing it to the ground. Use suitable screws to secure the stabilizer.



**Note:** Attach the stabilizer plate to the rack **before** loading the cabinet.

### Procedure

1. Place the stabilizer plate up against the bottom of the front side of the cabinet.
2. Align the holes from the stabilizer plate to the holes on the bottom of the cabinet.
3. Place the screws in the holes and secure them into the cabinet.

## Mounting the PDUs

Before you mount the system components, mount the power distribution unit (PDU) or units in the rack before installing other equipment. The PDU is your grounded power connection for all the system components in the rack. The PDUs described in this section are designed exclusively for the Hitachi family of racks.

The number of PDUs that are required depends on your system configuration. The Hitachi Solutions rack has space for four PDUs; however, the use of two PSUs per rack is standard.

Where you mount the PDUs depends on the rack that you use. Consult the specifications that come in the PDU packing materials if available. As a general guideline, consider the density of component cable connections and then space the PDUs out according to where you intend to mount the components. As an example, if you use four PDUs, you can mount the PDUs as shown in the following table.

PDU	Mounting location
1	Left side rear of the rack between units (U) 10 to 19
2	Right side rear of the rack between U 10 to 19
3	Left side front of the rack between U 31 to 40
4	Right side rear of the rack between U 31 to 40



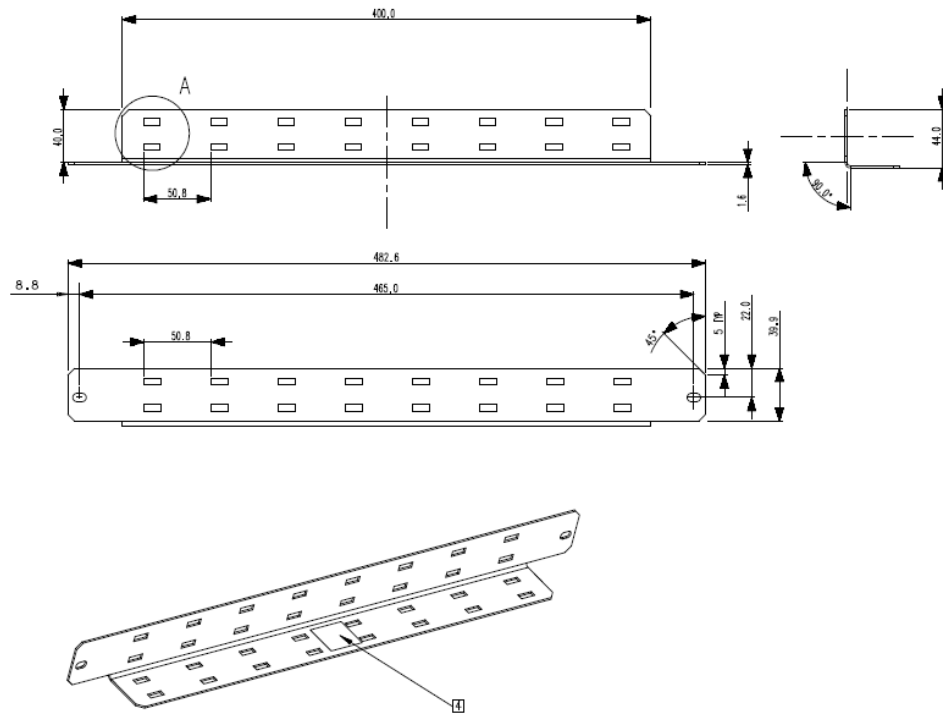
**Figure 4 16 Amp PDU and 32 Amp PDU**

Item	Description
1	16 Amp PDU
2	32 Amp PDU

## Installing the PDU rack cabling tray

To mount the power distribution unit (PDU), you must first install the rack cabling tray. The 19-inch tray allows you to mount the PDU and then position your power and data cabling for the best access to the components in the rack. Use of the tray also allows you to keep your cabling secure and away from potential hazards.





**Figure 5 19 inch rack cabling tray and bracket**

### Procedure

1. Assemble the parts for the PDU rack cabling tray.
2. Position the left side tray against the rack at the front left side and insert the screws.
3. Position the right side tray against the rack at the front right side and insert the screws.

## Mounting the storage

Determine which storage module the customer has ordered. Mount the storage module in the rack according to the prescribed diagrams that come with the storage module.

## Reviewing the HUS controller box hardware

Use the figures in this section to review the HUS storage controller box front and back panel hardware for the various HUS models. The different models share the same front panel hardware.

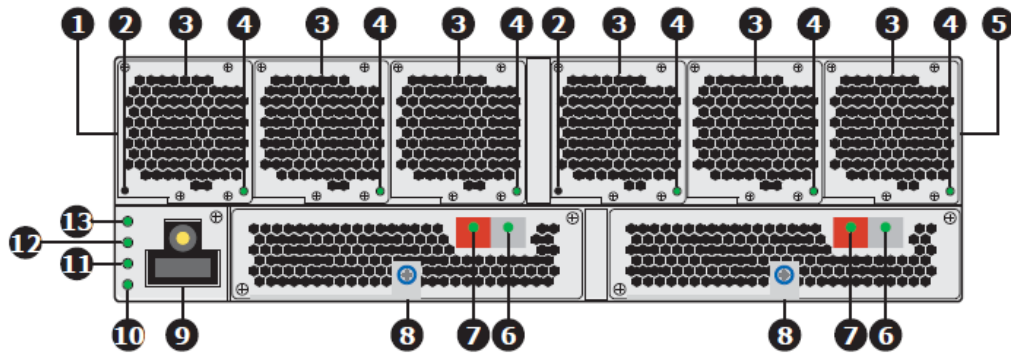


Figure 6 HUS 150 Controller Box front panel

Table 3 HUS 150 Controller Box front panel component descriptions

Item	Description	Item	Description
1	Controller 0	2	Reset switch
3	Fan 4	4	FAN-ALM LED
5	Controller 1	6	RDY LED
7	ALM LED	8	Cache backup battery
9	Main switch	10	ALM LED
11	WARN LED	12	RDY LED
13	PWR LED		

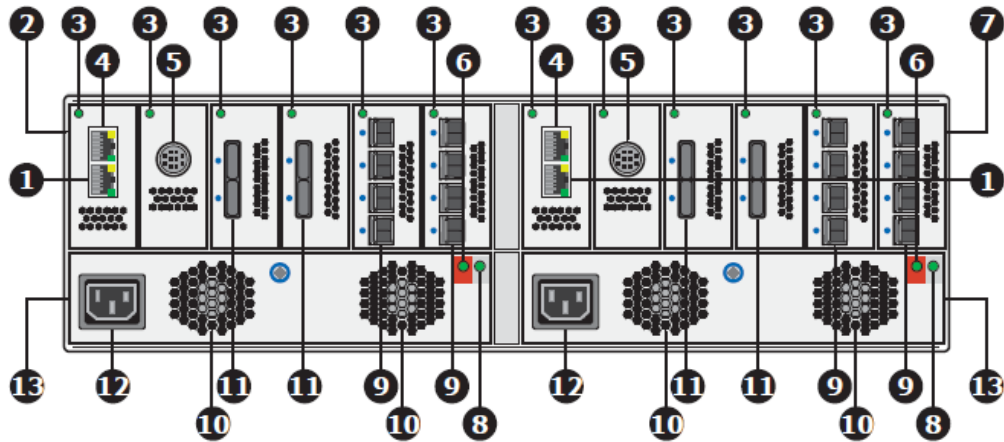


Figure 7 HUS 150 Controller Box rear panel

Table 4 HUS 150 Controller Box rear panel component descriptions

Item	Description	Item	Description
1	LAN 0 maintenance port	2	Controller 0
3	STATUS LED	4	LAN management port
5	Uninterruptible power supply port	6	ALM LED
7	Controller 1	8	RDY LED
9	Host I/O ports	10	Fan
11	Drive I/O ports	12	AC power socket
13	Power unit		

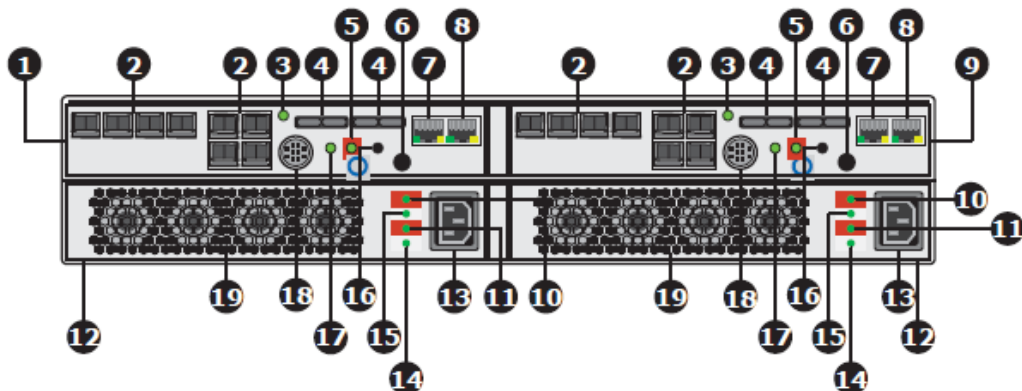


Figure 8 HUS 130 LFF/SFF Controller Box rear panel

**Note:** LFF represents large form factor and SFF represents small form factor.

**Table 5 HUS 130 LFF/SFF Controller Box rear panel component descriptions**

<b>Item</b>	<b>Description</b>	<b>Item</b>	<b>Description</b>
1	Controller 0	2	Host I/O ports
3	I/O module status LED	4	Drive I/O ports
5	ALM LED	6	Main switch
7	LAN 0 maintenance port	8	LAN 1 management port
9	Controller 1	10	P-RDY LED
11	B-RDY LED	12	Power unit
13	AC power outlet	14	B-ALM LED
15	P-ALM	16	Reset switch
17	STATUS LED	18	Uninterruptible power supply port
19	Fan		

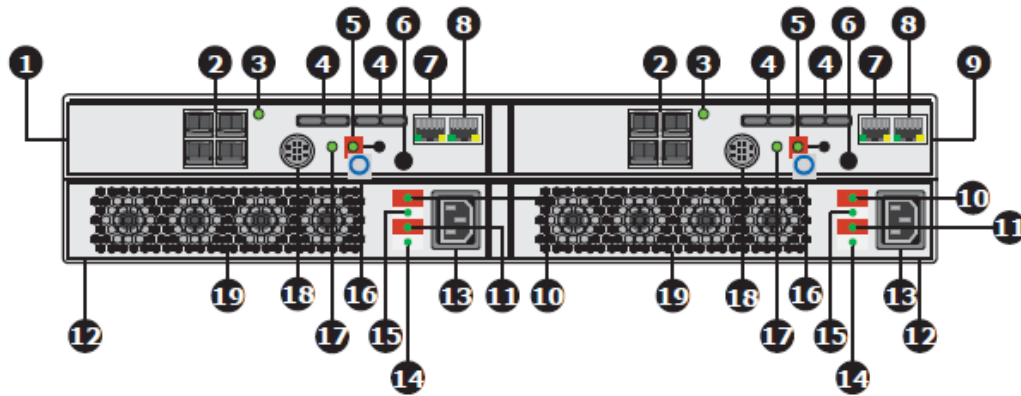


Figure 9 HUS 110 LFF/SFF Controller Box rear panel

Table 6 HUS 110 LFF/SFF Controller Box rear panel component descriptions

Item	Description	Item	Description
1	Controller 0	2	Fiber Channel ports
3	I/O module status LED	4	Drive I/O ports
5	ALM LED	6	Main switch
7	LAN 0 maintenance port	8	LAN 1 management port
9	Controller 1	10	P-RDY LED
11	B-RDY LED	12	Power unit
13	AC power outlet	14	P-ALM LED
15	B-ALM	16	Reset switch
17	STATUS LED	18	Uninterruptible power supply port
19	Fan		

## Reviewing the HUS drive box hardware

Use the figures in this section to review the HUS storage drive box front and back panel hardware for the various HUS models. The different models share the same front panel hardware.



**Note:** LFF represents large form factor and SFF represents small form factor.

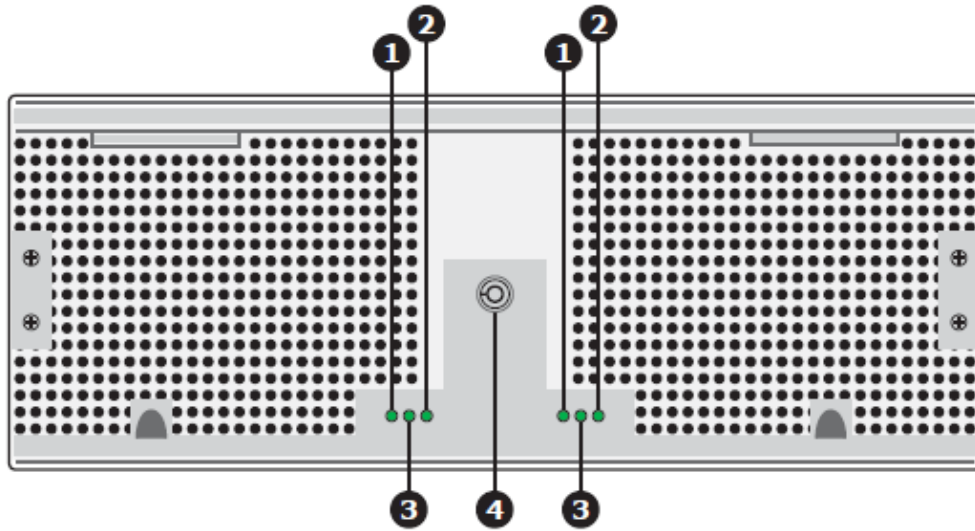


Figure 10 HUS 150 LFF Drive Box front panel

Table 7 HUS 150 LFF Drive Box front panel component descriptions

Item	Description	Item	Description
1	LOCATE LED	2	READY LED
3	POWER status LED	4	Bezel lock

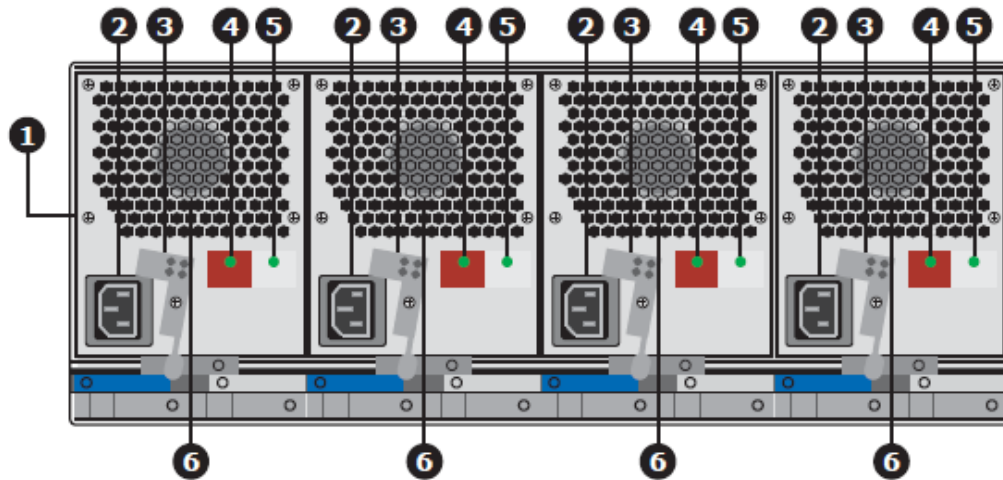


Figure 11 HUS 150 LFF Drive Box rear panel

Table 8 HUS 150 LFF Drive Box rear panel component descriptions

Item	Description	Item	Description
1	Power unit	2	AC power socket
3	AC power plug retainer	4	ALM status LED
5	RDY LED	6	Fan

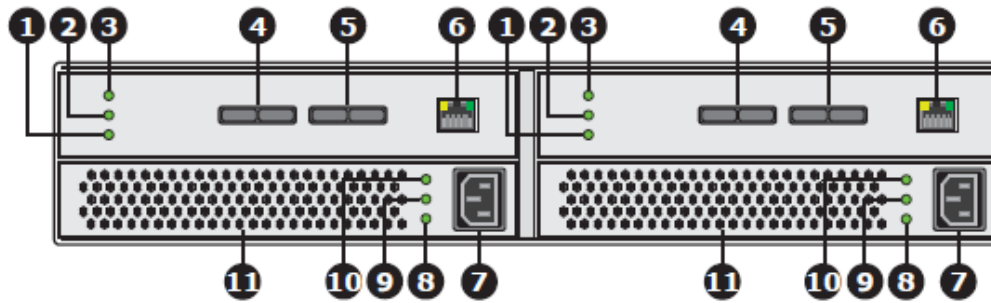


Figure 12 HUS 130 and HUS 110 LFF/SFF Drive Box back panel

Table 9 HUS 130 and HUS 110 LFF/SFF Drive Box back panel component descriptions

Item	Description	Item	Description
1	ALARM LED	2	LOCATE LED
3	POWER status LED	4	IN port
5	OUT port	6	CONSOLE port
7	AC power socket	8	ALM LED
9	AC-IN status LED	10	RDY LED
11	Fan		

## Mounting the storage components

The storage components are designed to be installed in a Hitachi rack or equivalent.

To rack the storage components:

### Procedure

1. Verify the rack is secure and is in no danger of falling over, and that all rack stabilizers are mounted.
2. Adjust the length of the mounting rails as needed.  
The rear rail slides inside the front rail. The rail halves are riveted together and use no adjustment screws.
3. Attach the mounting rail assemblies to the outside of the rack posts, using the attaching screws and flange nuts from your rack system.
  - a. Position the front rail support on the bottom facing inward.
  - b. Fit the alignment pins into the rack holes above and below the attaching screws.
  - c. Use the attaching screws and flange nuts from your rack system.
  - d. Tighten the screws and flange nuts according to your rack system instructions.
4. Place the controller box on the rails, and secure it to the rack.



- a. Insert one screw on each side, in the upper hole only, using the attaching screws and flange nuts from your rack system.
  - b. Tighten the screws and flange nuts according to your rack system instruction.
5. Place the storage module on the rails, and secure it to the rack.
  - a. Insert one screw on each side, in the upper hole only, using the attaching screws and flange nuts from your rack system.
  - b. Tighten the screws and flange nuts according to your rack system instruction.
6. Place any additional drive boxes on the rails, and secure them to the rack.
  - a. Insert one screw on each side, in the upper hole only, using the attaching screws and flange nuts from your rack system.
  - b. Tighten the screws and flange nuts according to your rack system instruction.

## Mounting the FC switches

The Brocade Fibre Channel (FC) switch is designed to fit in server racks and it consumes only one unit (U) of rack space. If a racked system has been purchased, the FC switch or switches (as ordered) may already be installed in the rack. Install the switch using the parts that are provided in the switch packaging.



### Note:

- This guide describes a Brocade FC switch, but the system also supports FC switches from other manufacturers, including Cisco and others.
- For the parts list, see the switch mounting instructions that come with the Brocade switch.

The Brocade rail kit allows you to install their switch in a recessed position. Installing the switch in this way positions the switch with its rear panel ports at the same depth in the rack as the server.

### Procedure

1. Assemble the FC switch rails.
2. Use the rack to set the correct length, and anchor it with one screw.
3. After you install the rail, use a flathead screwdriver to separate the two parts while tightening to ensure the needed spacing occurs.
4. Attach the inner rail to the FC switch tray.
5. Secure the rear of the rail with two screws and large washers.
6. Before inserting the switch, tighten the three anchor screws to hold the rail length while using a flathead screwdriver to separate the two pieces.
7. Insert and secure the switch.

Use the tapered screw in the center hole to secure the rail; the top and bottom rail holes secure the switch once it is inserted.

## Mounting the 10 GbE switches

The Brocade 10 Gigabit Ethernet (10 GbE) switch is designed to fit in server racks and it consumes only one unit (U) of rack space.



**Note:**

- This guide describes a Brocade VDX 6740 10GbE switch.

A switch rack mount kit with short mounting brackets ships with the Brocade switch. The parts list is included with the switch mounting instructions that come with the switch. Use the switch mounting instructions to mount the switch.

The Brocade kit allows you to mount their switch in the rack in a recessed position. Mounting the switch in this way positions the port on its rear panel at the same depth in the rack as the server.



**Note:** Make sure you use the screws supplied with the mounting brackets. Using the wrong screws could damage the switch and would invalidate your warranty.



**Figure 13 Brocade VDX 6740 10 GbE switch front view**



**Figure 14 Brocade VDX 6740 10 GbE switch rear view**

## Configuring the Ethernet switch to the storage system

After the switches are racked, see the *Brocade VDX 6740 Switch Configuration for use in an HNAS Cluster Configuration Guide* for information about switch configuration.

## Configuring HyperTerminal for the Ethernet switch configuration

You can use the HyperTerminal software to access the switch for configuration.

### Procedure

1. Start the HyperTerminal software.  
The Connection Description dialog displays.
2. In the Name field, type `TX24 Switch`, and then click **OK**.  
The Connect To dialog box displays.
3. From the **Connect using** drop down menu, select **COM1**, and then click **OK**.
4. Enter the following values in the COM1 properties dialog:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
5. Click **OK**.
6. Choose **File** and then **Save** to save the HyperTerminal configuration.

## Recovering from a lost password during switch configuration

By default, the CLI does not require passwords. However, if someone has configured a password for the device and the password has been lost, you can regain super-user access to the device using the following procedure.

### Procedure

1. Connect the null modem cable between COM1 of the Test Set PC to the switch's management serial port.
2. Start the HyperTerminal software.
3. While the system is booting, before the initial system prompt appears, type `b` to enter the boot monitor.
4. At the boot monitor prompt, issue the command: `no password`



**Note:** You cannot abbreviate the `no password` command.

The system displays: `OK! Skip password check when the system is up.`

5. At the boot monitor prompt, issue the command: `boot system flash primary`  
The device bypasses the system password check.
6. When the console prompt reappears, assign a new password.

## Mounting an HNAS or HUS File Module server

This section provides a summary of the Hitachi NAS Platform and Hitachi Unified Storage File Module server components.

When you use two servers, the servers are referred to as a cluster, and the servers are then referred to as nodes.

When you are using two servers, you must determine which node is node 1 and which node is node 2. HDS only licenses one of the nodes completely. The node that is licensed completely is node 1, or the first node in a cluster. Look at the paper or CD license keys, cross reference the node serial numbers, and perform the work on the node that is licensed as node 1.

Node 1 should also be physically racked on top; although, sometimes customers want node 1 on the bottom.

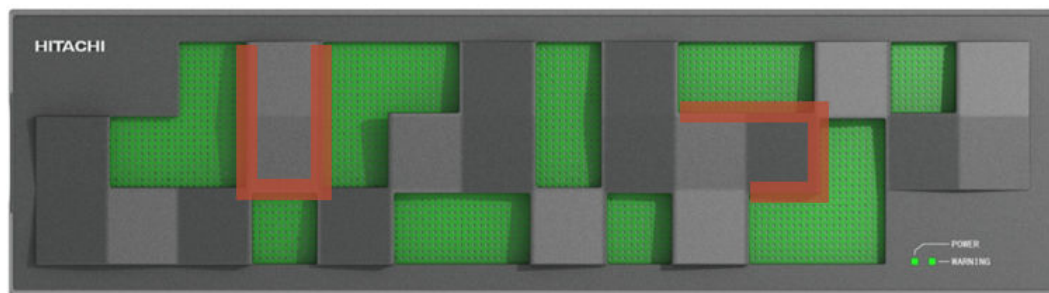
## Reviewing the server hardware

This section provides descriptions of the server front and rear panels and the externally exposed components.

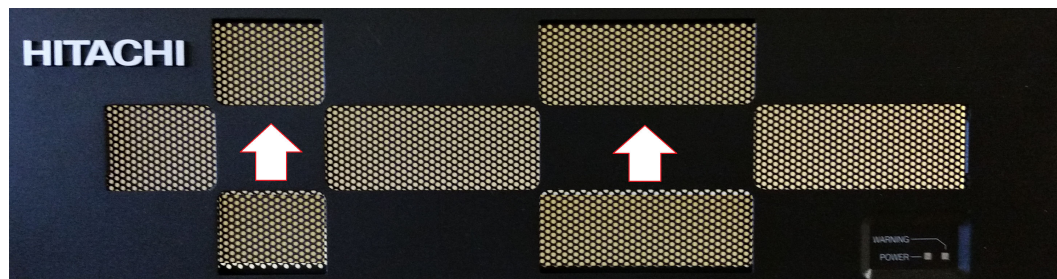


**Note:** The descriptions and figures apply to both the Hitachi Unified Storage File Module and Hitachi NAS Platform server models.

For more information, see the applicable *Hardware Reference*.



**Figure 15** Plastic front bezel with grasping areas indicated



**Figure 16** Metal front bezel with grasping areas indicated

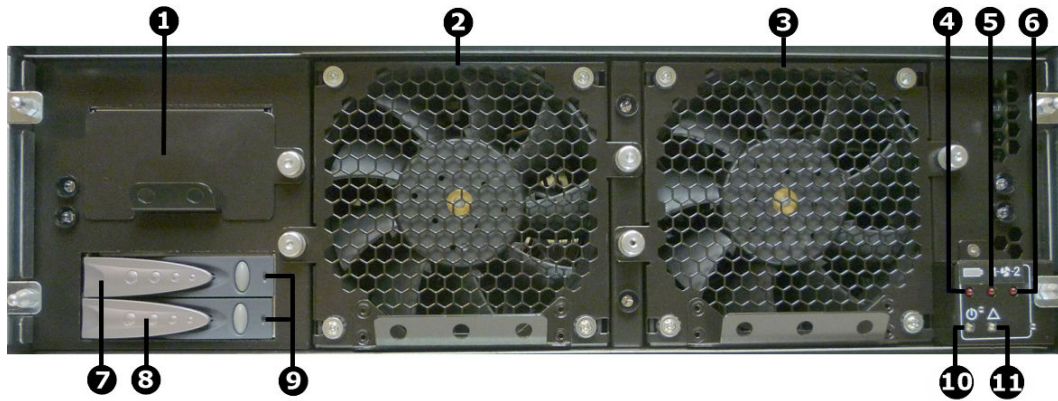


Figure 17 Model 4040 front view without bezel

Item	Description
1	NVRAM backup battery
2	Fan 1
3	Fan 2
4	NVRAM battery backup pack status LED
5	Fan 1 status LED
6	Fan 2 status LED
7	Hard disk A
8	Hard disk B
9	Hard disk status LEDs
10	Server status LED
11	Power status LED

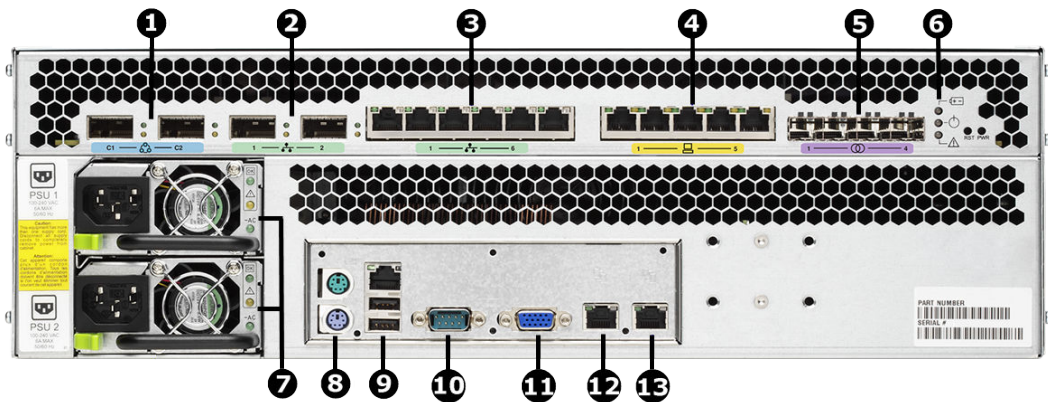


Figure 18 Model 4040 rear view

Item	Connectivity	Qty	Description
1	Clustering ports	2	Cluster management and heartbeat, connect to: <ul style="list-style-type: none"> <li>Two-way configuration: connect to corresponding cluster server ports (C1 to C1 and C2 to C2)</li> <li>N-way configuration: connect to 10 Gb switch as per SX515176</li> </ul>
2	10 GbE port	2	Connection to external data network
3	1 GbE port	6	Connection to external data network
4	1000 baseT Ethernet	5	Internal Ethernet switch, used in single-head configurations only
5	4 Gb Fibre Channel (FC) port	4	Connection to disk arrays, or where present, to the FC switches
6	n/a	n/a	Status LEDs (NVRAM, power, and server), and Power and Reset buttons
7	Power supply units: PSU 1 PSU 2	2	Connect to the rack's Fault group: <ul style="list-style-type: none"> <li>PSU 1 to Fault group A</li> <li>PSU 2 to Fault group B</li> </ul>
8	I/O ports	2	Keyboard (purple) and mouse (green) ports
9	I/O ports	2	USB ports
10	RS-232	1	Management interface ( <i>reserved for Customer Service Engineer</i> )
11	Video port	1	Video management interface ( <i>reserved for Customer Service Engineer</i> )
12	1000 baseT Ethernet (gray label ETH0)	1	External system management, connect to the customer's management network
13	1000 baseT Ethernet (yellow label ETH1)	1	Management port to connect to according to configuration: <ul style="list-style-type: none"> <li>MGM ETH switch</li> <li>To the rack Ethernet switch</li> </ul>



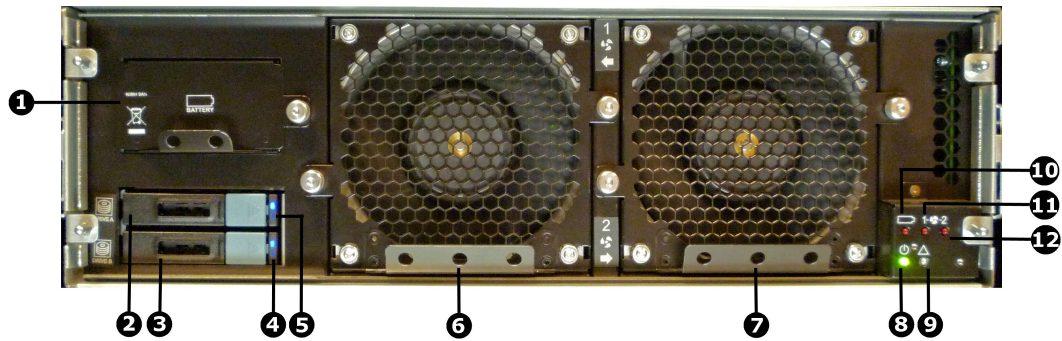


Figure 19 Models 4060, 4080, and 4100 front view without bezel

Item	Description
1	NVRAM backup battery
2	Hard disk drive (HDD) A
3	HDD B
4	HDD B status LED
5	HDD A status LED
6	Fan 1
7	Fan 2
8	Power status LED
9	Server status LED
10	NVRAM battery backup pack status LED
11	Fan 1 status LED
12	Fan 2 status LED

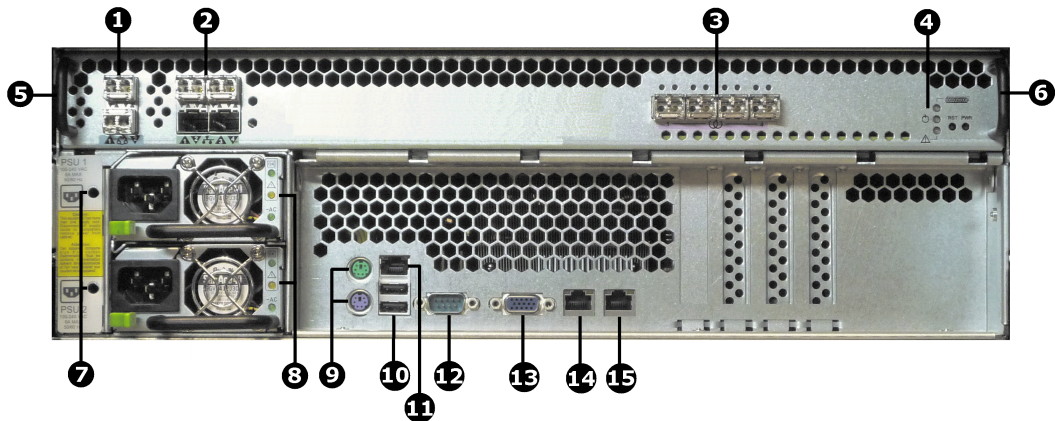



Figure 20 Models 4060, 4080, and 4100 rear view

Item	Connectivity	Quantity	Description
1	Clustering ports 10 GbE (SFP+)	2	For cluster management and heartbeat, connect to: <ul style="list-style-type: none"> <li>Two way configuration: Connect to corresponding cluster server ports (top port to top port and bottom port to bottom port).</li> <li>N-way configuration: Connect to 10 GbE switch.</li> </ul>
2	10 GbE network ports (SFP+)	4	Connection to external Ethernet data network .
3	8 G FC storage ports (SFP+)	4	Connection to disk arrays or (where present) to the FC switches.
4	n/a		Status LEDs (NVRAM, power, and server), and Power and Reset buttons.
5 and 6	n/a	2	Plastic handles.  <b>Caution:</b> Do <i>not</i> lift the server by these handles.
7	n/a	2	Holes for mounting the power supply cable retention clasps.
8	Power supply units: PSU 1 PSU 2	2	Connect to the rack's Fault group: <ul style="list-style-type: none"> <li>PSU 1 to Fault group A</li> <li>PSU 2 to Fault group B</li> </ul>
9	I/O ports		Keyboard (purple) and mouse (green) ports. <i>(Reserved for Customer Service Engineer access only.)</i>
10	I/O ports	2	USB port. <i>(Reserved for Customer Service Engineer access only.)</i>
11	IPMI port	1	Can be used for Remote Management. For further information, visit Hitachi Support Connect.
12	RS-232	1	Management interface. <i>(Reserved for Customer Service Engineer access only.)</i>
13	Video port	1	Video management interface port. <i>(Reserved for Customer Service Engineer access only.)</i>



Item	Connectivity	Quantity	Description
14	ETH0 1000baseT Ethernet (gray logo)	1	External system management. Connect to the customer's management switch.
15	ETH1 1000baseT Ethernet (yellow logo)	1	Management port. Connect to the rack's internal Ethernet switch.

## Server installation requirements

The servers come with rack mounting hardware. The server also comes with sets of SFP or SFP+ adapters (depending on server model) to be inserted in the Ethernet and Fibre Channel ports on the server.

Servers come with slider rails pre-fitted on the chassis.

The HNAS 4040, HNAS 4060, HNAS 4080, and HNAS 4100 servers feature clip-in rail kits that fit square-hole racks. However, you can still use the rail kits with round-hole racks by removing the square-hole fasteners.

### Time

Allow up to 30 minutes to complete this task.

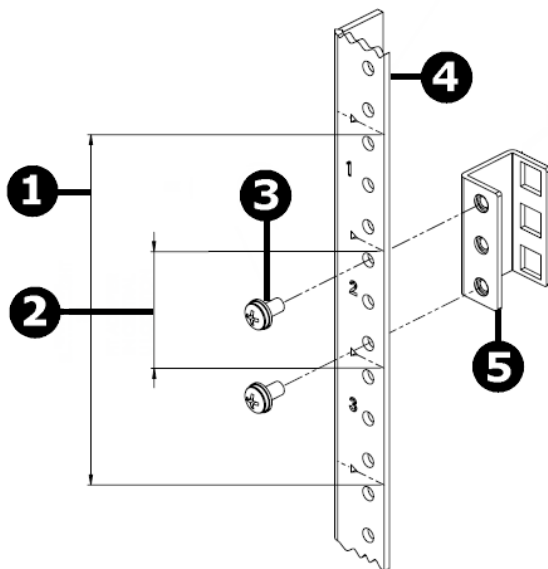
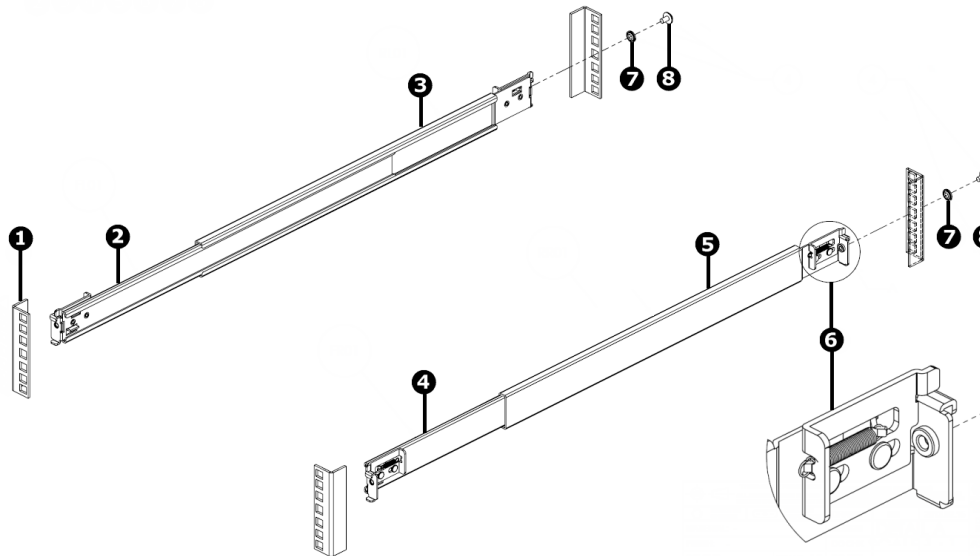


Figure 21 Round-hole rack adapter bracket

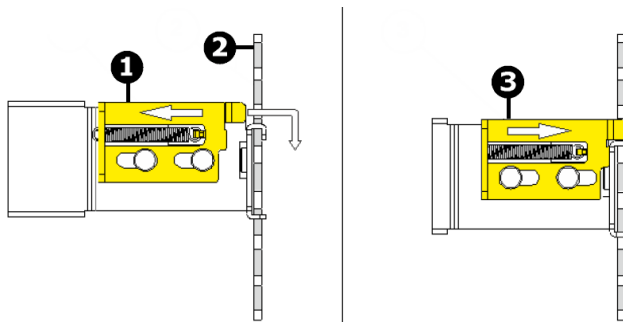
Item	Description
1	Server height 3U (three units)
2	Central location to position the adapter

Item	Description
3	Screw 10-32 x 3/8 pan head steel zinc, SEM
4	Customer round-hole rack
5	Round-hole rack adapter bracket



**Figure 22 Server clip-in rail rack kit installation**

Item	Description
1	Rack
2	Left front side rail
3	Left rear side rail
4	Right front side rail
5	Right rear side rail
6	Release latch
7	Screw 10-32 x 3/8, pan head steel zinc, SEM (optional at customer site)
8	Washer, centering, custom, conical stainless (optional at customer site)



**Figure 23 Clip-in rail release latch connection to rack**

Item	Description
1	Direction to pull the latch when inserting the rail in the rack
2	Rack
3	Direction to push the latch when removing the rail from the rack

## Mounting the server components

When mounting servers, use the clip-in rail kits for square hole racks.

### Before you begin

Plan for three units (3U) of rack space for each server.

The server mounting hardware features clip-in rail kits. Servers come with slider rails pre-fitted on the chassis.



**Note:** The HNAS 4060, 4080, and 4100 servers are shipped with mounting instructions. The HNAS 4040 server packaging might include mounting instructions.

### Procedure

1. Install the outer rails in the rack:
  - a. Position the rails inside the rack, and adjust the length of the rails to the depth of the rack.  
The rail brackets on both ends fit inside the rack.
  - b. Pull the latch on the rail bracket toward the front of the rack, and insert and lower the rail into the front of the rack.
  - c. Pull the latch on the rail bracket toward the front of the rack, and insert and lower the rail into the rear of the rack rail.



**Note:** To remove the rail bracket from the rack, push the latch toward the rear of the rack.

2. Insert the server in the rack and secure it.
3. Attach the bezel according to the instructions provided with its packaging.

## Installing the Ethernet and FC port adapters

The server comes with sets of adapters that are to be inserted in the Ethernet and Fibre Channel (FC) ports on the rear of the server. The adapters are small form-factor pluggable (XFP or SFP) or small form-factor pluggable plus (SFP+) adapters.

The adapter type used depends on the server model. The adapter type is identified by the label on the top surface of the adapter.



**Note:** Always check the part number on the label of the SFP+ adapter:

- 10 GbE SFP+: FTLX8571D3BCV
- 8 Gbps SFP+: FTLF85828P3BNV



**Caution:** Use care when inserting the adapters into the server ports to avoid damaging the adapters.

**Table 10 Server model requirements for FC port adapters**

Server model	Adapter	FC ports
HNAS 4040	SFP	4 Gb
HNAS 4060, HNAS 4080, HNAS 4100	SFP+	8 Gb

**Table 11 Server model requirements for Ethernet port adapters**

Server model	Adapter	Ethernet ports
HNAS 4040	XFP	10 GbE and C1/C2
HNAS 4060 , HNAS 4080, and HNAS 4100	SFP+	10 GbE and C1/C2

### Procedure

1. Locate the adapters and sort them.
2. Carefully insert the SFP or SFP+ adapters into the four FC ports on the rear of the server as follows:  
Position the white label on the SFP and SFP+ adapters toward the top of the port.
3. Carefully insert the XFP or SFP+ adapters into the Ethernet networking and cluster ports on the rear of the server as follows:
  - For the XFP adapters, orient the white label on the XFP adapters to the bottom of the port.
  - For the top row of ports, orient the white label on the SFP+ adapters toward the top of the port.
  - For the bottom row of ports, orient the white label on the SFP+ adapters toward the bottom of the port.

## Mounting an external SMU

The external system management unit (SMU) provides administration and monitoring tools. It supports data migration and replication, and acts as a quorum device in a cluster configuration. Although integral to the system, the SMU does not move data between the network client and the servers.

### Reviewing the SMU 400 hardware

This section provides descriptions of the supported system management unit (SMU) model 400, including the front and rear panels, and the externally exposed components. These descriptions apply to SMU 400 for the Hitachi NAS Platform servers.

The server includes an embedded SMU; however, it is not active when an external SMU is attached.



**Caution:** Lift the SMU from the bottom of the chassis. Do *not* lift the SMU chassis by the plastic handles. These handles are for sliding the SMU in to the rack.



**Note:** The ports marked with an \* (asterisk) in the following tables may be used by customer service engineers and customers that support their own SMUs.

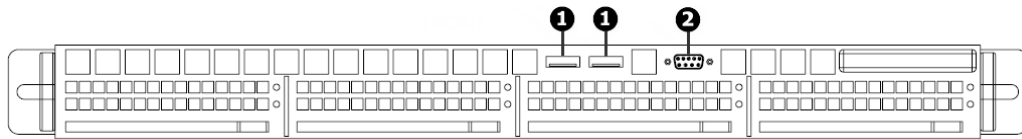


Figure 24 SMU 400 model front view and components

Item	Connectivity	Quantity	Description
1	I/O ports*	2	USB ports for keyboard or mouse
2	RS232 port*	1	Management interface (COM2)

**Note:** This port is only usable at boot time.

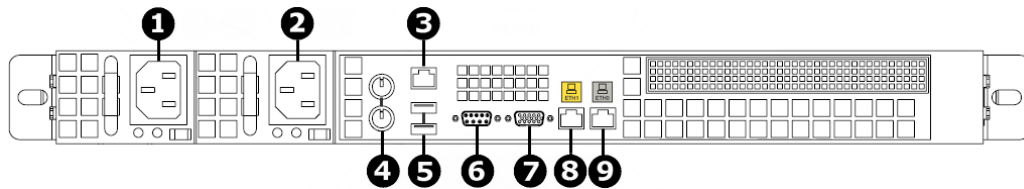



Figure 25 SMU 400 model rear view and components

**Attention:** The Ethernet (ETH) ports on the SMU 400 are in the opposite order from those on the SMU 300.


Item	Connectivity	Quantity	Description
1 and 2	Power supply units: <ul style="list-style-type: none"> <li>▪ PSU 1</li> <li>▪ PSU 2</li> </ul>	2	Connect to the rack's Fault group: <ul style="list-style-type: none"> <li>▪ PSU 1 to Fault group A</li> <li>▪ PSU 2 to Fault group B</li> </ul>
3		1	Unsupported IPMI port. (PROVIDED AS-IS, neither supported nor maintained by HNAS engineering or HDS Support.)
4	I/O ports*	2	Keyboard (purple) and mouse (green) ports.
5	I/O ports*	2	USB ports.
6	RS232 port*	1	Management interface (COM1).

Item	Connectivity	Quantity	Description
			 <b>Note:</b> This is the preferred management port.
7	Video port*	1	Video management interface port.
8	ETH1 1000baseT Ethernet (yellow logo)	1	Management port. Connect to the rack's internal Ethernet switch.
9	ETH0 1000baseT Ethernet (gray logo)	1	External system management. Connect to the customer's management switch.

## SMU 400 installation requirements


Use the rail kit components to mount the system management unit (SMU) in the rack. The SMU 400 comes with slider rails pre-fitted on its chassis and clip-in rail kits. The clip-in rail kits fit square-hole racks. However, you can still use the rail kits with round-hole racks by removing the square-hole fasteners.

### Parts list

 **Important:** The rail kit from a SMU 300 *cannot* be used to mount a SMU 400.

For round-hole racks, consider the following specifics regarding items in the installation figures:

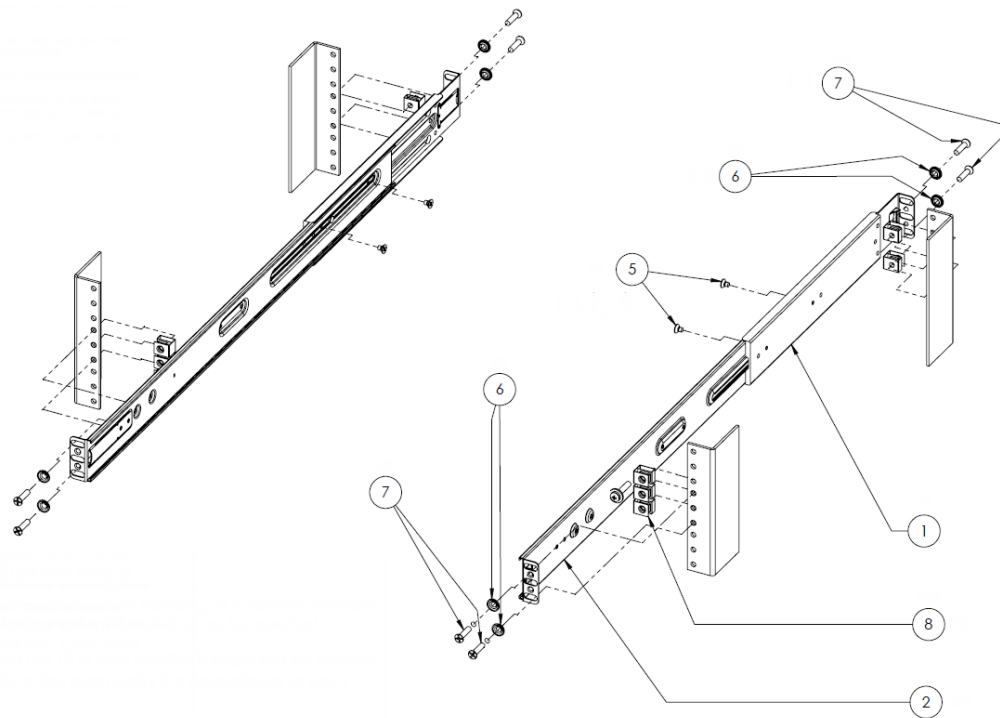
- Item 5 is optional when installing at customer premises but mandatory for HDS Distribution Centers, when the server will be transported in a fully populated rack.
- Depending on the 19 in. rack depths, it might not be possible to fit all four screws marked as item 5. In this case, you can use only two screws.
- Item 8 needs to be supplied by the customer (normally part of the 19 in. rack accessory pack). In some cases the accessory pack might contain Imperial fasteners (10-32 thread) rather than Metric. In this case, ensure that consistent type or fasteners are used, replacing item 7 with a screw compatible with the clip nut supplied.

 **Attention:** Do not attempt to fit item 7 (M5 metric fastener) into an Imperial thread nut.



**Table 12 SMU 400 clip-in rail kit parts list for a round-hole rack**

Item	Quantity	Description
1	2	Rear support bracket
2	2	Front support bracket
5	16	Phillips head M4 x 4mm
6	4	Custom washer
7	4	Flat head M5 x 16mm
8	10	10-32 clip nuts

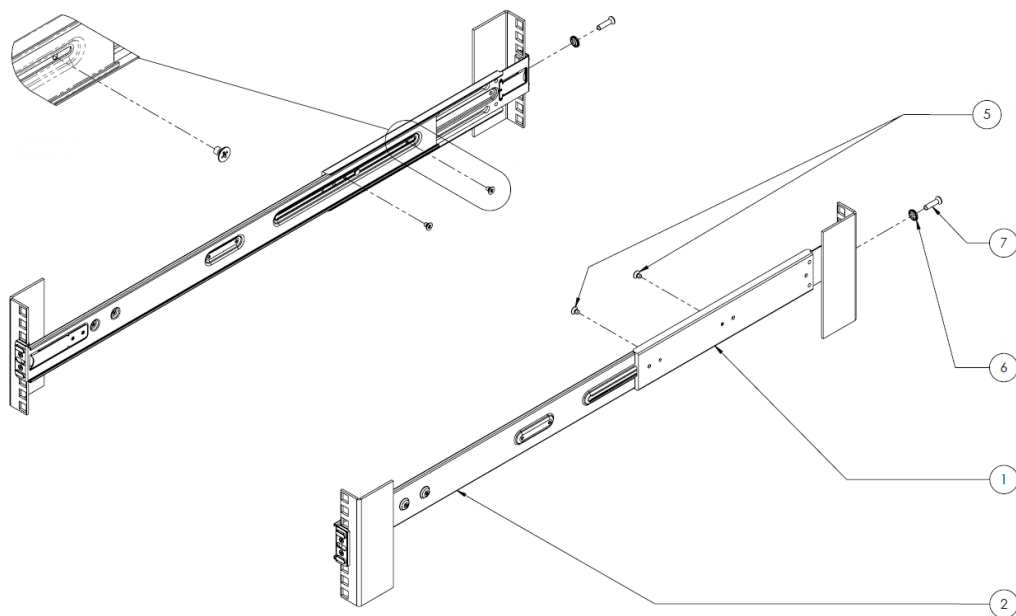
**Figure 26 SMU 400 clip-in rail kit installation in a round-hole rack**

For a square-hole rack, consider the following specifics regarding items in the installation figure:

- Items 5, 6, and 7 are optional when installing at customer premises but mandatory for HDS Distribution Centers, when the server will be transported in a fully populated rack.
- Depending on the 19 in. rack depths, it might not be possible to fit all four screws marked as item 5. In this case, you can use only two screws.

**Table 13 SMU 400 clip-in rail kit parts list for a square-hole rack**

Item	Quantity	Description
1	2	Rear support bracket
2	2	Front support bracket
5	16	Phillips head M4 x 4mm
6	4	Custom washer
7	4	Flat head M5 x 16mm
8	10	10-32 clip nuts

**Figure 27 SMU 400 clip-in rail kit installation in a square-hole rack**

## Mounting an SMU 400

Use these steps to a mount system management unit (SMU) with a clip-in rail kit into a server rack.

### Before you begin

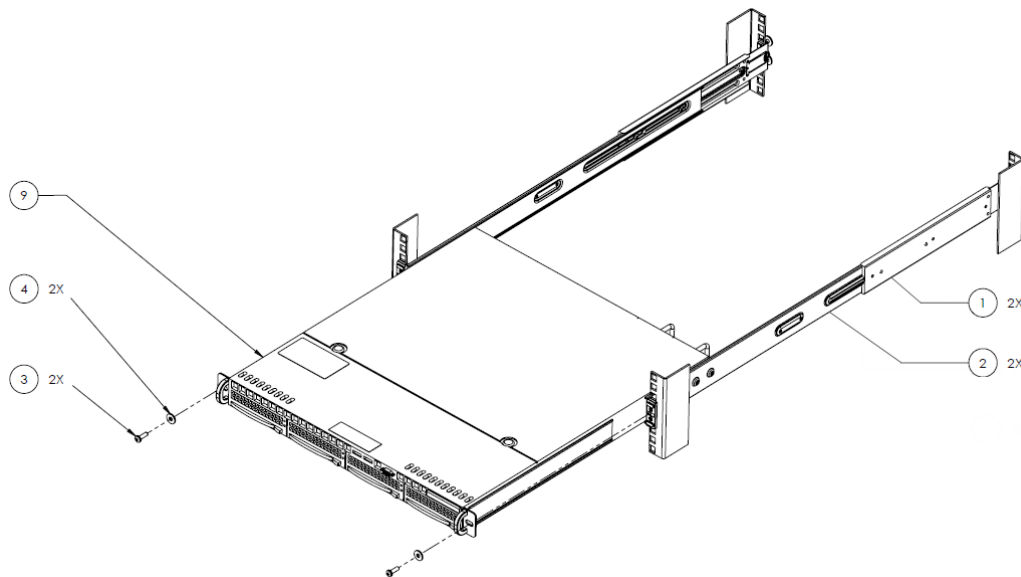
Plan for two units (2U) of rack space for each SMU. The space is required to access the serial ports and console ports on the back of the SMU.



**Note:** For the detailed parts list, see the mounting instructions that accompany the SMU.

**Table 14 SMU 400 clip-in rail kit parts list for mounting**

Item	Quantity	Description
1	2	Rear support bracket
2	2	Front support bracket
3	2	Phillips head M4 x 4mm
4	2	Custom washer
9	1	SMU

**Figure 28 SMU 400 clip-in rail kit mounting****Procedure**

1. If you have a round-hole rack, modify the square-hole rail kit to fit by performing the following steps:
  - a. Remove and discard the two M3 flathead screws.
  - b. Discard the aluminum brackets.
  - c. Repeat for each of the four rail components (items 1 and 2 for each side).
2. Install the outer rails in the rack:
  - a. Position the rails inside the rack, and adjust the length of the rails to the depth of the rack.  
The rail brackets on both ends fit inside the rack.
  - b. Pull the latch on the rail bracket toward the front of the rack, and insert and lower the rail into the front of the rack.
  - c. Pull the latch on the rail bracket toward the front of the rack, and insert and lower the rail into the rear of the rack rail.



**Note:** To remove the rail bracket from the rack, push the latch toward the rear of the rack.

3. Insert the SMU into the rack and secure it.

## Cabling the system

This section provides recommendations for cabling the server and storage components, and the Ethernet and Fibre Channel (FC) switches. Specific requirements vary based on the design of your system.



**Important:** When connecting an HNAS 4040 server model to the 1000Base-T GE Ethernet network, the ports (the six ports for customer data IO with a green label underneath) always use patch cables that fully comply with the CAT6 SF/UTP standard, such as those supplied by Harting and listed below:

- CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 1M HARTING 09474747109
- CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 2M HARTING 09474747111
- CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 3M HARTING 09474747113
- CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 5M HARTING 09474747115
- CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 10M HARTING 09474747121

The high-level steps to cable the system include the following:

1. Route and connect Ethernet cables.

Route Ethernet cables behind the rails, or in the cable management system.

2. Route and connect power cables.

3. Route and connect FC cables.

FC cables are for storage arrays only.










**Important:** Avoid cable stress, which can be caused by:

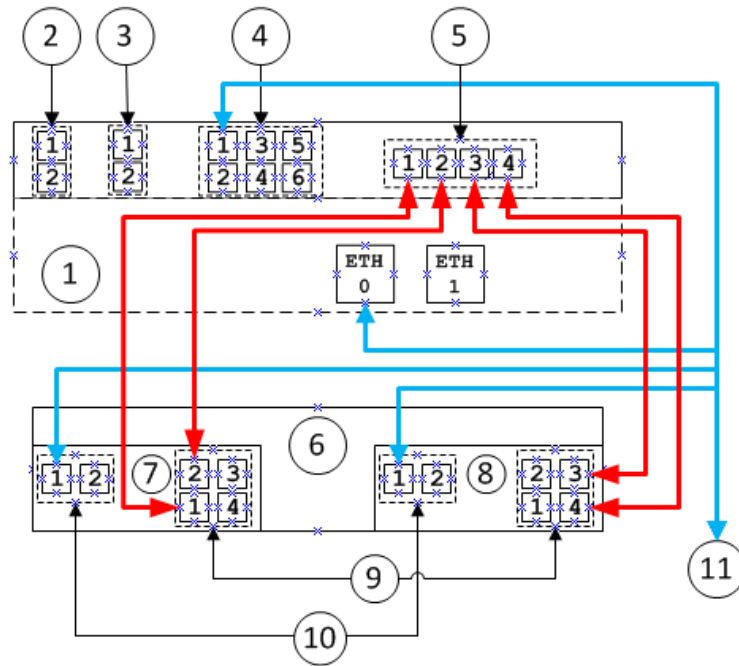
- Cable twist during pulling or installation
- Tension in suspended cable runs
- Tightly cinched cable ties
- Tight bend radii

**Table 15 Cable types and sizes**

Cable Type	Recommended Radius	
Power (PWR)	4 times diameter	15mm (0.6in.)
Unshielded twisted pair (UTP), Ethernet	4 times diameter	15mm (0.6in.)
Shielded twisted pair (ScTP), Ethernet	8 times diameter	25mm (1in.)
FC with copper (FC-Cu)	10 times diameter	50mm (2in.)
FC multimode fiber optic (FC-MMF)	10 times diameter	50mm (2in.)

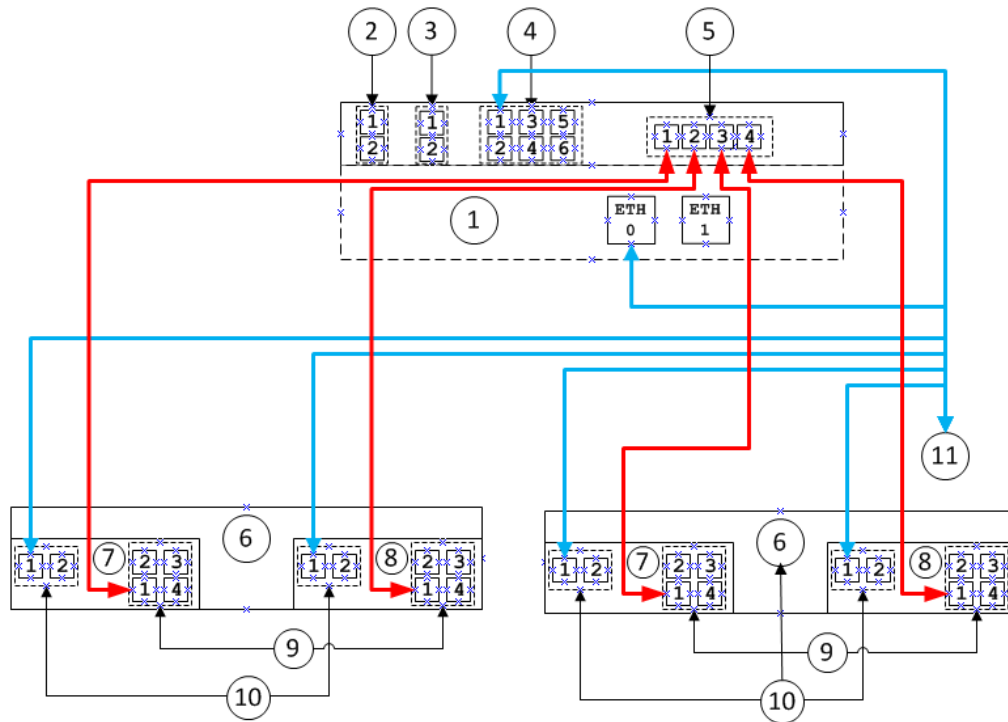
**Table 16 Server rear panel port labels**

Ports	Description	Connection
	Cluster interconnect (CI) ports	Second cluster node or 10 Gbps switch for clusters of three or more nodes
	10 GbE (gigabit Ethernet) ports	Public (data) network
	1 GbE (gigabit Ethernet) ports	Public (data) network
	10/100 Mbps Ethernet ports	Private management network
	FC network ports	Storage arrays or FC ports
	Ethernet management port 0	Public (data) network
	Ethernet management port 1	Private management network



**Figure 29 Cabling a single 4040 server direct-attach to a single storage enclosure**

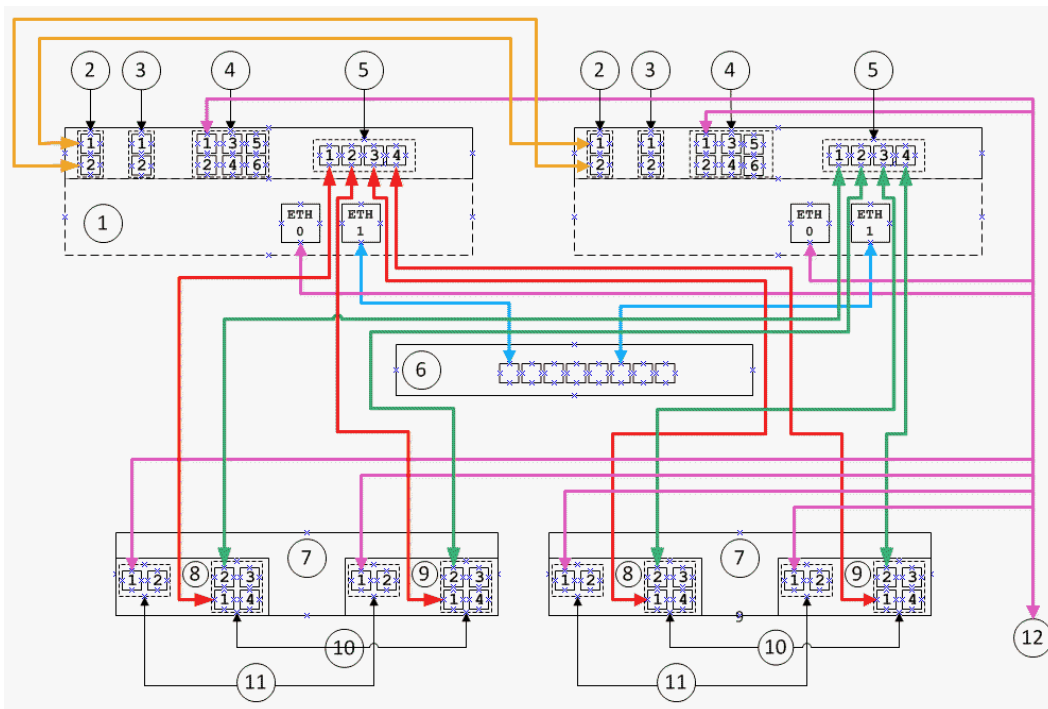
Item	Description
1	HNAS Server
2	10 GbE cluster interconnect (CI) ports
3	10 GbE public (data) network ports
4	1 GbE public (data) network ports
5	2/4 G FC ports
6	RAID enclosure
7	Controller 0
8	Controller 1
9	FC ports
10	Controller Ethernet ports
11	Data network



**Figure 30 Cabling a single 4040 server direct-attach to two storage enclosures**

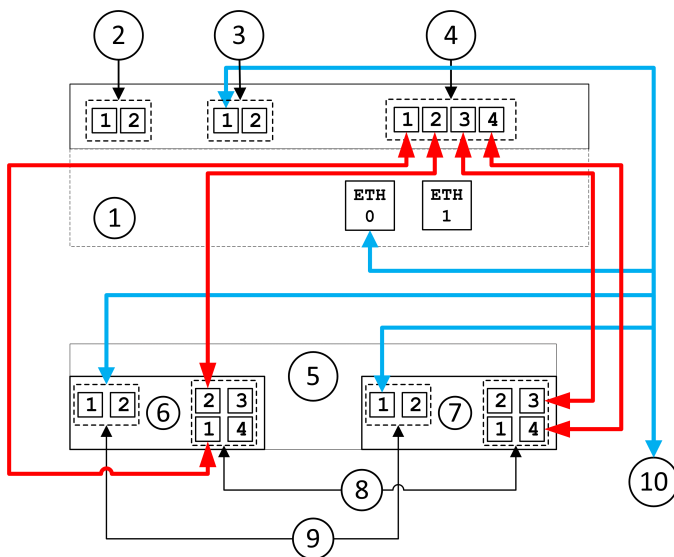
Item	Description
1	HNAS Server
2	10 GbE cluster interconnect (CI) ports
3	10 GbE (gigabit Ethernet) ports
4	1 GbE public (data) network ports
5	2/4 G FC ports
6	RAID enclosure
7	Controller 0
8	Controller 1
9	FC ports
10	Controller Ethernet ports
11	Data network

**Figure 31 Cabling a cluster of 4040 servers direct-attach to two storage enclosures**



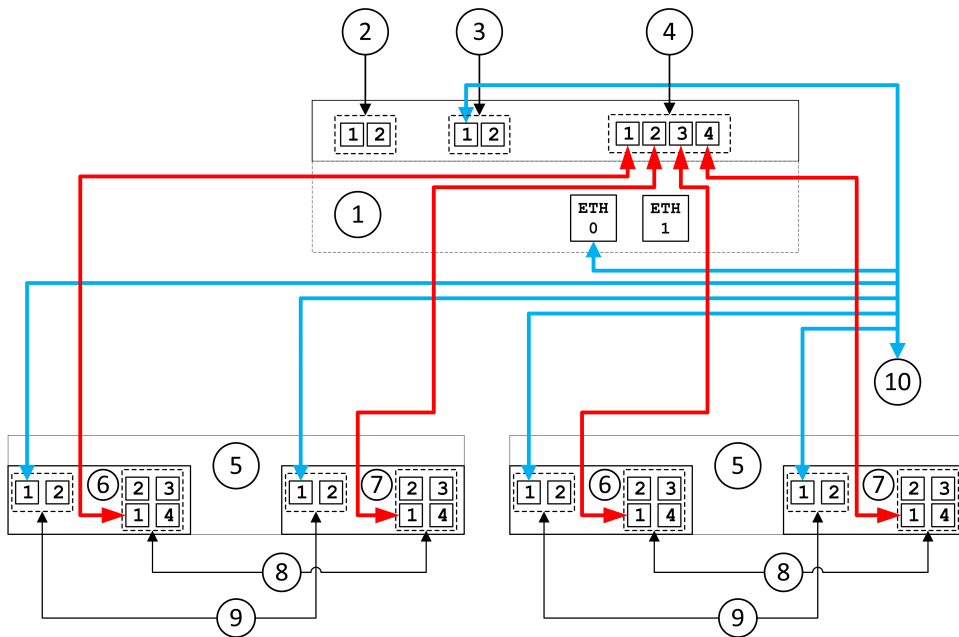
Item	Description
1	HNAS Server
2	10 GbE cluster interconnect (CI) ports
3	10 GbE public (data) network ports
4	1 GbE data network ports
5	1/2/4 G FC ports
6	Ethernet switch (private management network)
7	RAID enclosure
8	Controller 0
9	Controller 1
10	FC ports
11	Controller Ethernet ports
12	Data network





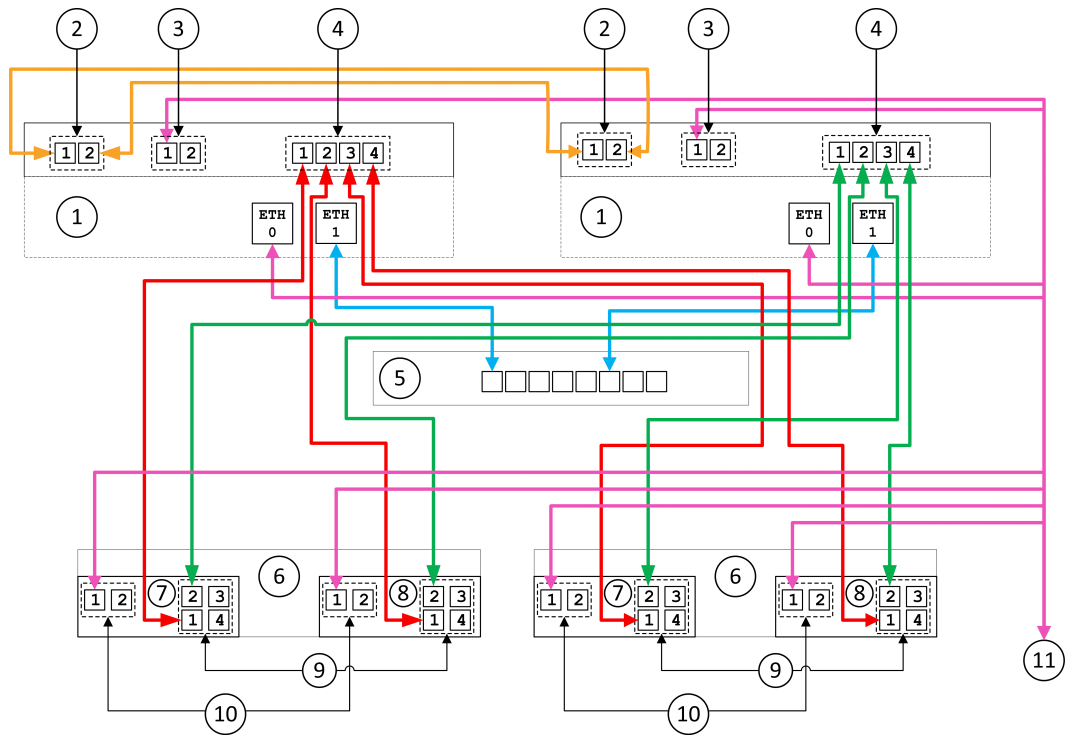
**Figure 32 Cabling a single HNAS 4060, 4080, or 4100 server direct-attach to a single storage enclosure**

Item	Description
1	HNAS Server
2	10 GbE cluster interconnect (CI) ports
3	10 GbE data network ports
4	2/4/8 G FC ports
5	RAID enclosure
6	Controller 0
7	Controller 1
8	FC ports
9	Controller Ethernet ports
10	Data network



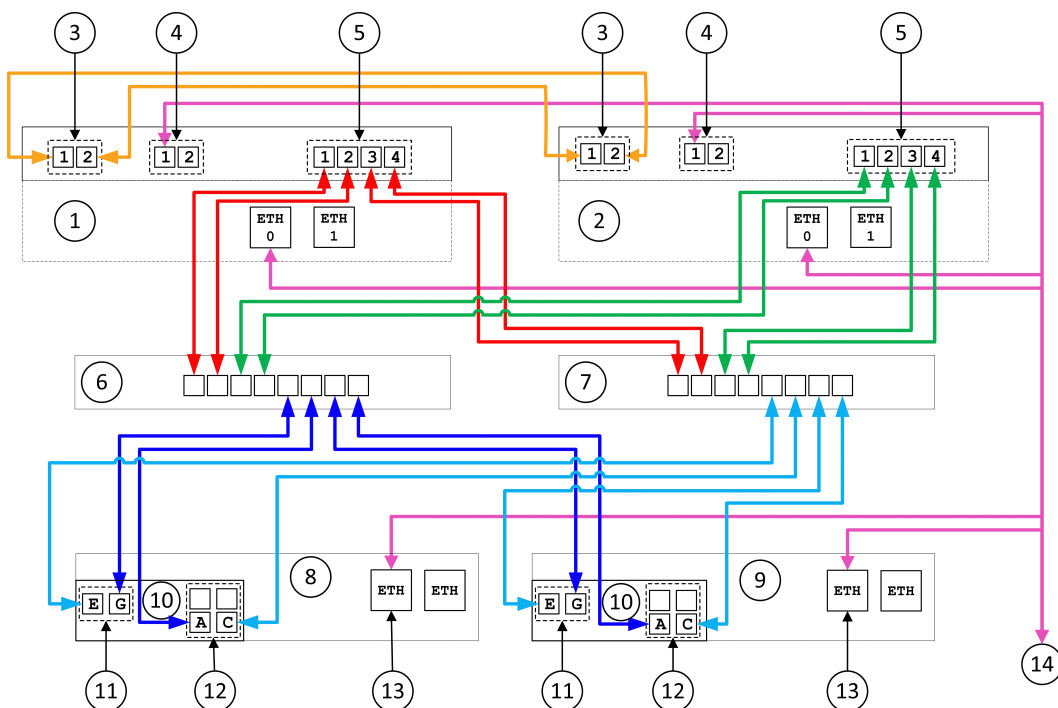
**Figure 33 Cabling a single HNAS 4060, 4080, or 4100 server direct-attach to two storage enclosures**

Item	Description
1	HNAS Server
2	10 GbE cluster interconnect (CI) ports
3	10 GbE public (data) network ports
4	2/4/8 G FC ports
5	RAID enclosure
6	Controller 0
7	Controller 1
8	FC ports
9	Controller Ethernet ports
10	Data network



**Figure 34 Cabling a cluster of HNAS 4060, 4080, or 4100 servers direct-attach to two storage enclosures**

Item	Description
1	HNAS Server
2	10 GbE cluster interconnect (CI) ports
3	10 GbE public (data) network ports
4	2/4/8 G FC ports
5	Ethernet switch (private management network)
6	RAID enclosure
7	Controller 0
8	Controller 1
9	FC ports
10	Controller Ethernet ports
11	Data network



**Figure 35 Cabling through Fibre Channel switches for a cluster of HNAS 4060, 4080, or 4100 servers attach to two storage enclosures**





Item	Description
1	HNAS Server 1
2	HNAS Server 2
3	10 GbE cluster interconnect (CI) ports
4	10 GbE public (data) network ports
5	4/8 G FC ports
6	FC switch 1
7	FC switch 2
8	RAID enclosure 1
9	RAID enclosure 2
10	RAID Controller
11	FC ports
12	FC ports
13	Ethernet maintenance port
14	Data network

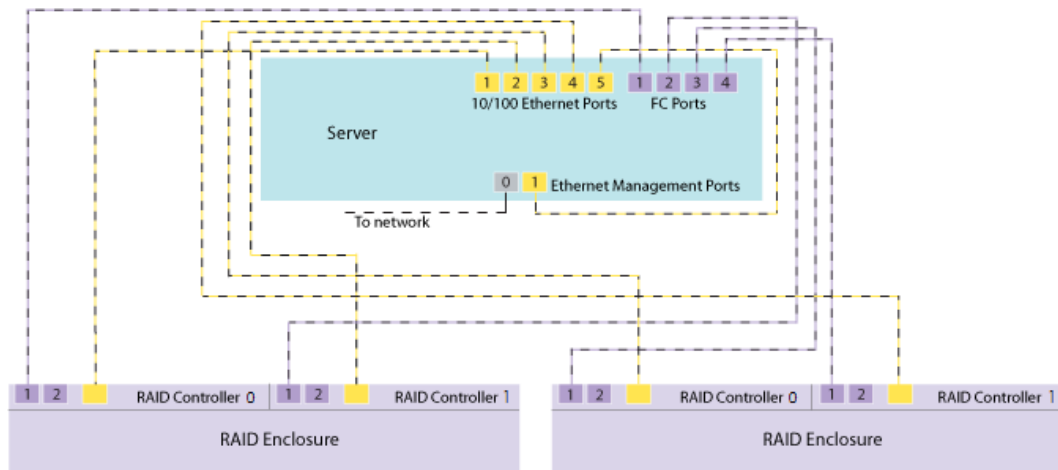
## Connecting to the server

This section provides recommendations for cabling the system. The final cabling layout will be specific to the design and needs of the system. Refer to your documentation wallet for more information, or contact customer support for guidance.

The following tables and diagrams are only for reference.


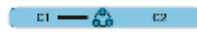
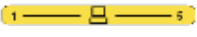
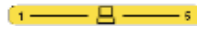
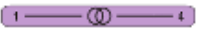
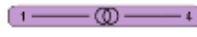




**Table 17 Connecting a single server to two storage enclosures**

Port	Connection	
	1	Controller 0 in enclosure 1
	2	Controller 1 in enclosure 1
	3	Controller 0 in enclosure 2
	4	Controller 1 in enclosure 2
	5	Eth1 on this server
	1	Host port 1 on controller 0 in enclosure 1
	2	Host port 1 on controller 1 in enclosure 1
	3	Host port 1 on controller 0 in enclosure 2
	4	Host port 1 on controller 1 in enclosure 2
	0	Public (customer data) network
	1	10/100 Ethernet port 5 on this server



**Figure 36 Connecting a single 4040 server to two storage enclosures diagram**

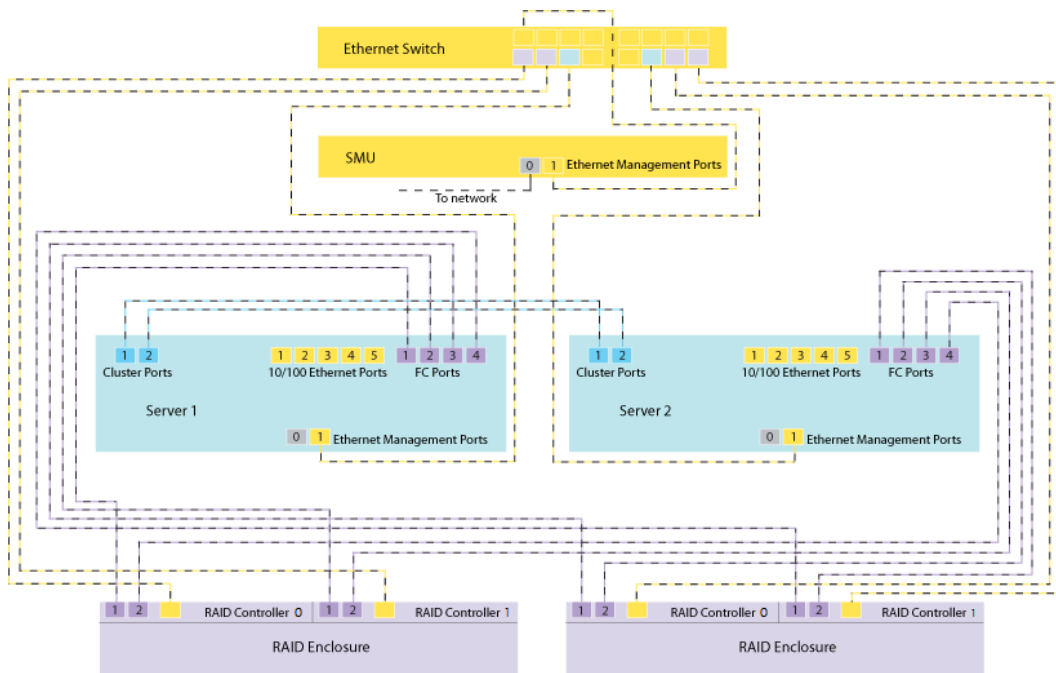
**Table 18 Connecting two nodes to two storage enclosures**

Node 1		Connection	Node 2		Connection
	1	Node 2 C1		1	Node 1 C1
	2	Node 2 C2		2	Node 1 C2
	1	Node 1 private management Ethernet network port 1		1	Node 2 private management Ethernet network port 1
	2	Controller 0 in enclosure 1		2	Controller 1 in enclosure 1
	3	Controller 1 in enclosure 2		3	None
	4	None		4	Controller 1 in enclosure 2
	5	Eth1 on node 1		5	Eth1 on node 2
	1	Host port 1 on controller 0 in enclosure 1		1	Host port 2 on controller 0 in enclosure 1
	2	Host port 1 on controller 1 in enclosure 1		2	Host port 2 on controller 1 in enclosure 1
	3	Host port 1 on controller 0 in enclosure 2		3	Host port 2 on controller 0 in enclosure 2
	4	Host port 1 on controller 1 in enclosure 2		4	Host port 2 on controller 1 in enclosure 2
	0	Public (customer data) network		0	Public (customer data) network
	1	Private management Ethernet network port 5 on node 1		1	Private management Ethernet network port 5 on node 2



**Attention:** The Ethernet ports on an SMU 400 are in the opposite order from those on the SMU 300. The follow figure shows an SMU 300.

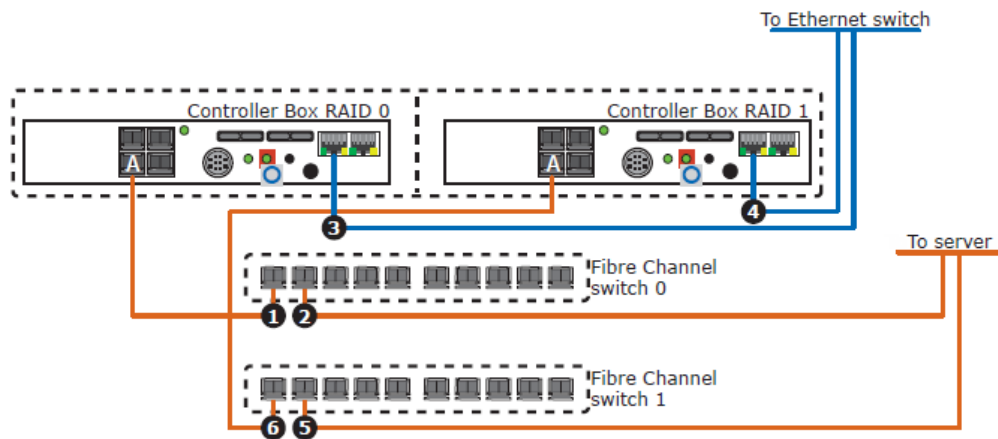
SMU model	Eth0 port location	Eth1 port location
300	Left	Right
400	Right	Left



**Figure 37 Connecting a 4040 two-node cluster with SMU to two storage enclosures**

## Connecting to the storage

This section provides recommendations for cabling the storage controller box and drive box. The final cabling layout will be specific to the design and needs of the system. Refer to your documentation wallet for more information, or contact customer support for guidance.



**Figure 38** Cabling one controller box

**Table 19** Cabling one controller box connection descriptions

Item	Description	Item	Description
1	Host I/O port A on Controller Box RAID 0 connects to Fibre Channel (FC) switch 0 using a fibre cable.	2	NAS server connects to FC switch 0 using a FC cable.
3	Management port on Controller Box RAID 0 connects to the Ethernet switch using an Ethernet cable.	4	Management port on Controller Box RAID 1 connects to the Ethernet switch using an Ethernet cable.
5	NAS server connects to FC switch 1 using a FC cable.	6	Host I/O port A on Controller Box RAID 1 connects to FC switch 1 using a FC cable.



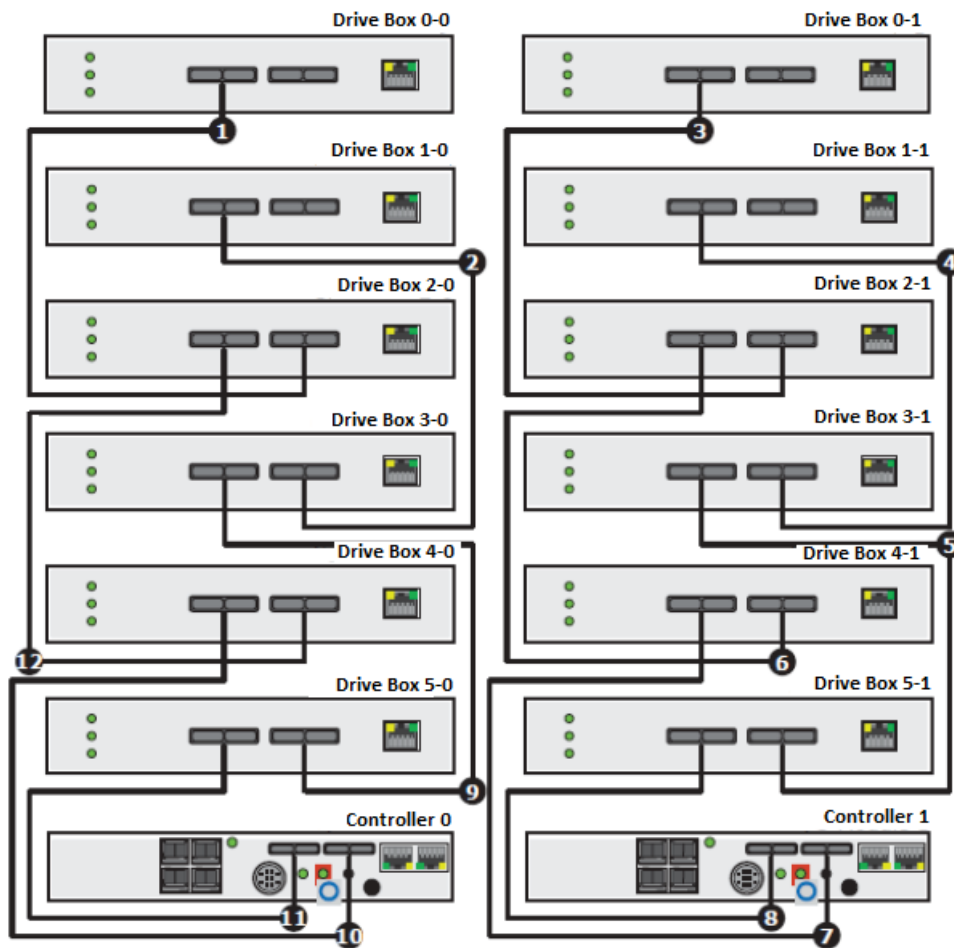


Figure 39 Cabling Drive Boxes

Table 20 Cabling drive boxes connection descriptions

Item	Description	Item	Description
1	IN port of Drive Box 0-0 connects to the OUT port of Drive Box 0-2.	2	IN port of Drive Box 1-0 connects to the OUT port of Drive Box 3-0.
3	IN port of Drive Box 0-0 connects to the OUT port of Drive Box 0-2.	4	IN port of Drive Box 1-1 connects to the OUT port of Drive Box 3-1.
5	IN port of Drive Box 3-1 connects to the OUT port of Drive Box 5-1.	6	IN port of Drive Box 4-1 connects to the OUT port of Drive Box 4-1.
7	IN port of Drive Box 4-1 connects to an I/O port on Controller 1.	8	IN port of Drive Box 5-1 connects to an I/O port on Controller 1.
9	IN port of Drive Box 4-0 connects to the OUT port of Drive Box 5-0.	10	IN port of Drive Box 4-0 connects to an I/O port on Controller 0.
11	IN port of Drive Box 5-0 connects to an I/O port on Controller 0.	12	IN port of Drive Box 2-0 connects to the OUT port of Drive Box 4-0.

## Connecting the power cables

The power cables from all of the system components must be connected to the power distribution unit (PDU). The PDU comes in two different amperages, 16 Amp and the new 32 Amp. Confirm that the PDU you received with your system has the correct amperage.


### Before you begin

Before you can connect the power cables to the PDU, you must have installed the rack cabling tray and mounted the PDU.

### Procedure

1. Route the power cables between the vertical rail and the outside skin of the rack. There is enough room to run the power leads between the power distribution unit (PDU) and the rack-side panel.
2. Secure power cables horizontally to the vertical side rail.
3. Position the tie-wraps, ensuring the cables do not overlap and remain parallel.
4. In redundant power supply systems in which both inlets are close together on one side of the system, secure power cables behind the vertical portion of the cable management panel.
5. Route power cables through the gaps in between the rails.
  - a. Power cables to be connected to the left side of the enclosure (from the rear of the rack) must be routed from under the rail.
  - b. Power cables to be connected to the right side of the enclosure must be routed over the top of the rail.
  - c. Server power cables should always be routed over the top of the rails.

## Checkpoint

 **Important:** Power on the components in the order given in the following steps.

### Procedure

1. Double check all power, Ethernet, and FC connections to ensure they are fully seated.
2. Confirm all power switches are in the off position, and plug the power distribution units (PDUs) into their dedicated receptacles.
3. Insert the disk drives into the trays while wearing a grounding strap.
 

Storage arrays come with a pre-configured volume group. Each drive chassis has a label with the serial number that correlates to a specific tray, and on the inside flap it indicates the drive order within the tray.

4. Power on all of the storage drive boxes (expansion trays), wait 30 seconds, and then power on all the controller modules.

The LEDs are green.

Refer to the OEM documentation for complete details on the LED states.

5. Power on the switches.
6. Power on the servers.  
The LEDs are green.
7. Power on the system management units (SMU).

The LEDs are green.

For complete details on the LED states, see one of the following as appropriate for your server model:

- *Hitachi NAS Platform 3080 and 3090 G2 Hardware Reference*
- *Hitachi Unified Storage File Module Hardware Reference*
- *Hitachi NAS Platform Series 4000 Hardware Reference*

For the server indicator information for the model 4040 server, see the *Hitachi NAS Platform 3080 and 3090 G2* or *Hitachi Unified Storage File Module Hardware Reference*.

### Next steps

Contact customer support for assistance if you do not pass this checkpoint.

---

## Chapter 5: Configuring the logical layer

The logical layer involves the software configuration for the system components. This installation phase includes the initial system configuration. After entering the commands from the CLI to set the IP addresses, run the configuration wizard to enter in all the relevant systems administration, site-specific, and customer information.

### Preparing for system configuration

To expedite the configuration of the system, consider the recommendations in this section.

The administration tool, called the Web Manager, is the graphical user interface (GUI) for the system management unit (SMU). This GUI provides a browser-based interface for managing standalone or clustered servers, and enables you to perform most administrative tasks from any client on the network using a supported web browser.

When configuring the HUS storage arrays, you must use the Hitachi Storage Navigator 2 (SNM2) software. Install the SNM2 software on the computer or laptop that will be used for making the configuration settings. The use of SNM2 software is called out when appropriate. When configuring a G1000 or Gx00 storage array, you must use the Hitachi Storage Navigator software from the SVP.

To successfully complete the configuration of the server, you will need the following:

Setting	Current configuration
Admin EVS public IP for Eth0	
File serving IP address	
DNS server IP, primary and secondary	
WINS, if any	
NIS, if any	
NTP server	
SMTP server	
Cluster name	
EVS1 and EVS2 names	
EVS1 and EVS2 IP addresses	

Setting	Current configuration
VLANs for management and data	

The server typically ships with any purchased licenses and the following pre-configuration:

Setting	Default/Example
Server root password	
Server manager password	
Server admin password	
Server admin EVS private IP address (Eth1)	Provided by customer
Server admin EVS public IP address (Eth0)	
SMU root and manager password	
SMU Eth0 IP	
SMU Eth0 subnet mask	
SMU Eth0 gateway	
SMU domain name	
SMU host name	



**Note:** Before connecting the server to your network, ensure that these IP addresses do not conflict with an existing network.

## Configuring the storage system

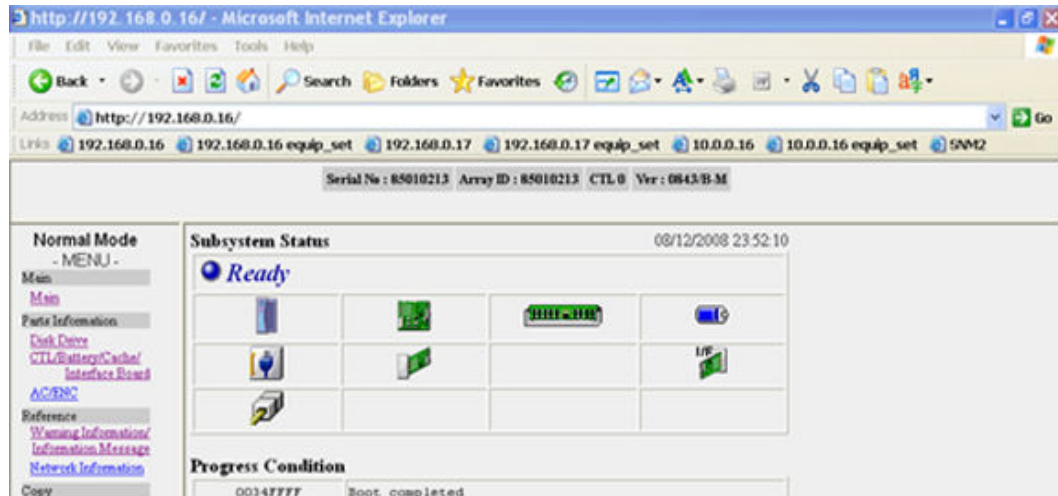
You can configure the storage system with the RAID+VOL set up. The storage system software is set up in the Storage Navigator Modular software graphical user interface (GUI).

To set up the storage system, you need to have available the customer information for the RAID+VOL setup. If this information is unavailable, create test RAID groups with at least one volume in each raid group of 20 GB for testing purposes.



**Note:** You must use all drives in a test RAID group.

When your system is ready, the storage system software GUI displays.



**Figure 40 Storage system GUI**

High-level steps required to set up a storage system. Use the Storage Navigator Modular GUI to perform the required steps.

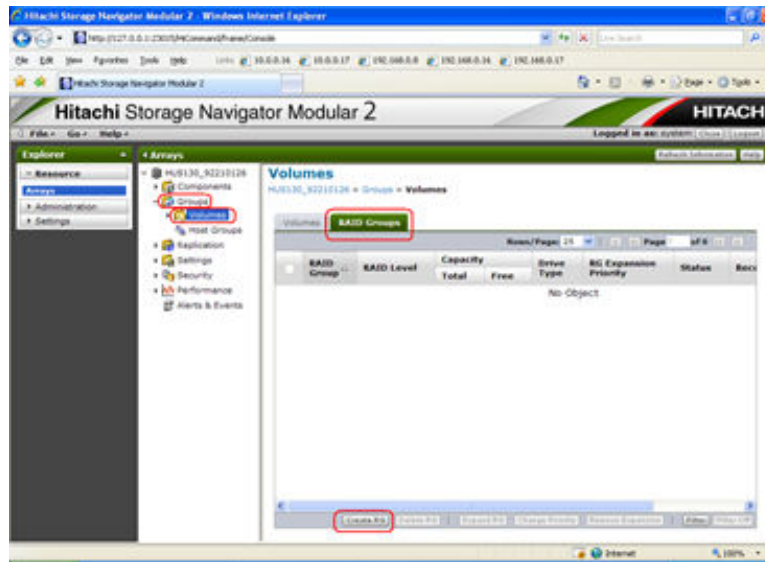
1. Connecting a laptop or desktop system to the HUS storage controller
2. Configuring the storage in the storage software GUI
3. Configuring the storage in the Storage Navigator Modular 2 (SNM2) software
4. Installing the license keys
5. Adding the storage arrays
6. Adding the spare drives
7. Creating the RAID groups
8. Creating the storage volumes
9. Configuring the host groups

## Creating the RAID groups

After you have added storage arrays and installed the license keys, you can create the RAID groups.

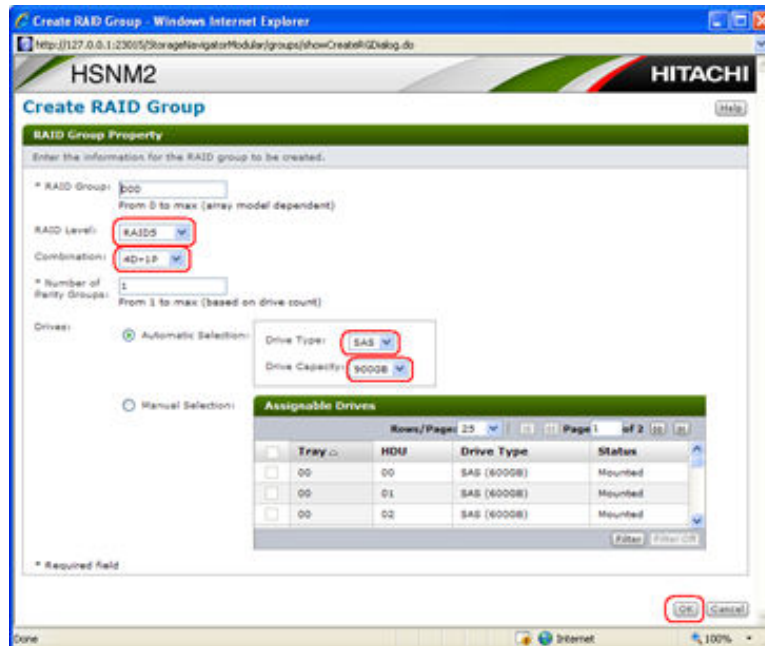
### Procedure

1. Open a browser and navigate to the Storage Navigator Modular 2 (SNM2) GUI at: <http://127.0.0.1:23015/StorageNavigatorModular/Login>
2. Log in with the user ID *system* and the password *manager*.
3. In the SNM2 GUI, select the following:
  - In the Arrays navigation tree (middle menu), select **Groups** and then **Volumes**.
  - In the Volumes pane (right side), select the **RAID Groups** tab, and then click **Create RG** at the bottom of the pane.



4. According to the customer specifications, perform the following steps:

- Choose the RAID Level.
- Choose the Combination.
- Choose the Drive Type.
- Choose the Drive Capacity.
- When finished, click OK.



5. In the confirmation window that displays, click **Close** in this screen.



- Repeat this procedure for the remaining drives for which you want to create RAID groups.  
When you have finished creating the RAID groups, you can create the necessary volumes.

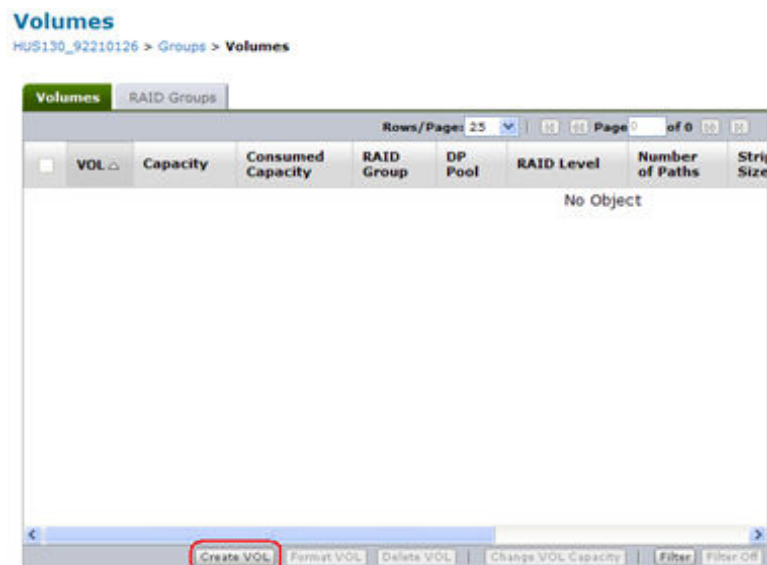
## Creating the storage volumes

After you have created RAID groups, you can create the volumes on the RAID groups.

**Note:** Before creating the storage volumes, see the *Hitachi NAS Platform HDP Best Practices* document for information about how best to configure HNAS with Hitachi Dynamic Provisioning (HDP).

### Procedure

- Open a browser and navigate to the Storage Navigator Modular 2 (SNM2) GUI at: <http://127.0.0.1:23015/StorageNavigatorModular/Login>
- Log in with the user ID *system* and the password *manager*.
- In the SNM2 GUI, in the Arrays navigation tree (middle menu), perform the following steps:
  - Select **Groups**.
  - Select the **Volumes** tab.
  - Click **Create VOL** in the bottom of the pane.



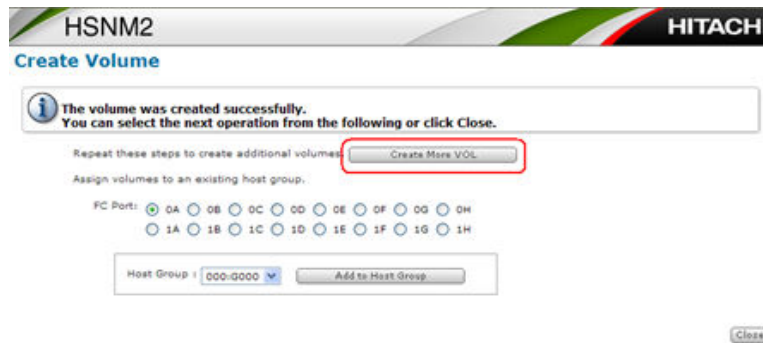


4. In the Basic tab window, perform the following steps:
  - From the **Capacity** list, select the capacity according to the customer specifications.

Usually, select **RG ALL**, unless this is FMD/SSD.



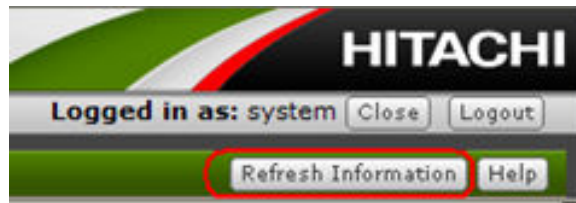
5. In the Advanced tab window, perform the following steps:
  - Set the Stripe size to 64K.
  - When finished with settings, click **OK**.
6. In the Create Volume window, click **Create More VOL** to create your other volumes. Repeat this step until you have created all of the volumes required by the customer specifications.



7. After creating your last volume, click **Close**, and you are returned to the Volume tab.

Number of Paths	Stripe Size	Cache Partition	Pair Cache Partition	Drive Type	Status
0	64KB	01	Auto	SAS	Normal
0	64KB	00	Auto	SAS	Normal(Waiting Quick Format{1}{0%})

8. In the Volumes window, click **Refresh Information** to check on the progress of the format.



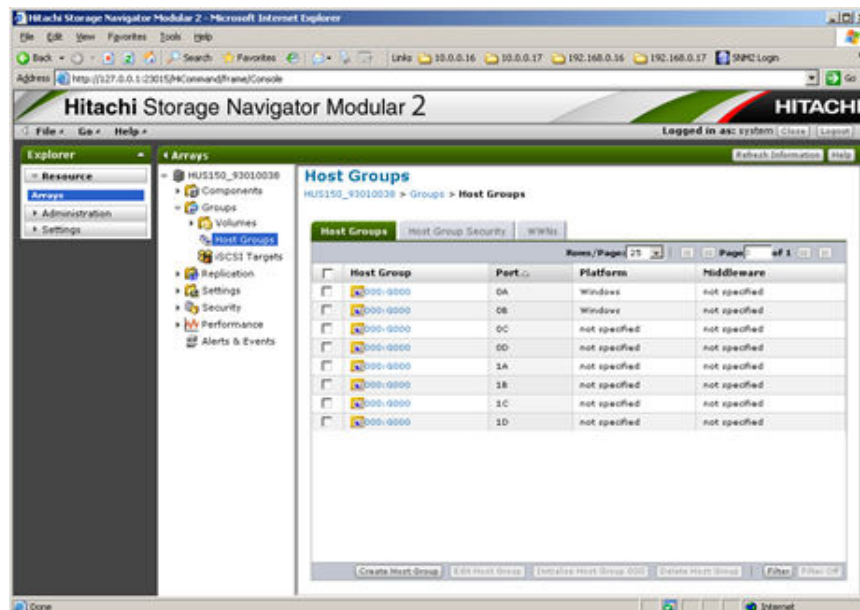
After you have created the necessary storage volumes, you can configure the host groups.

## Configuring the host groups

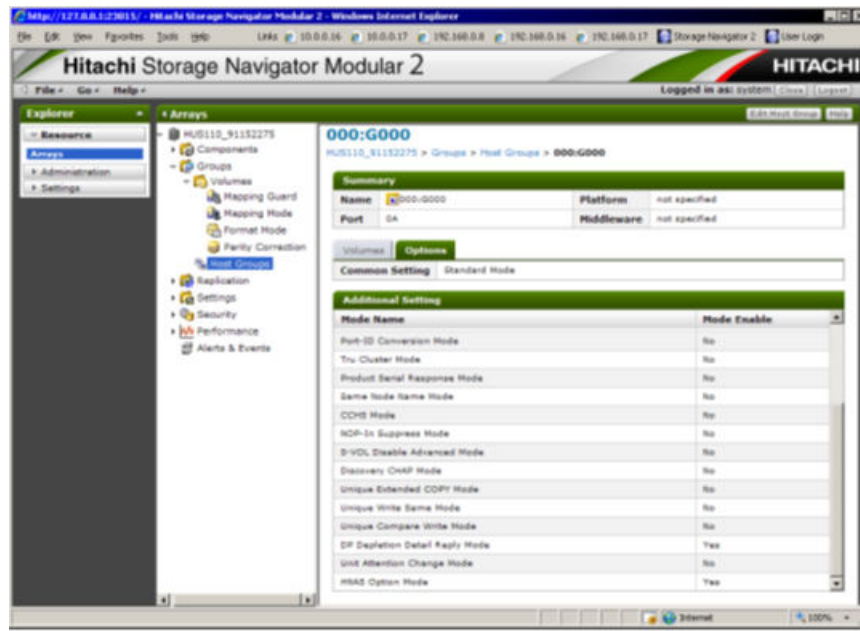
After you have created the RAID groups and volumes, you can configure the host groups. Host groups can help you monitor and manage host machines.

### Procedure

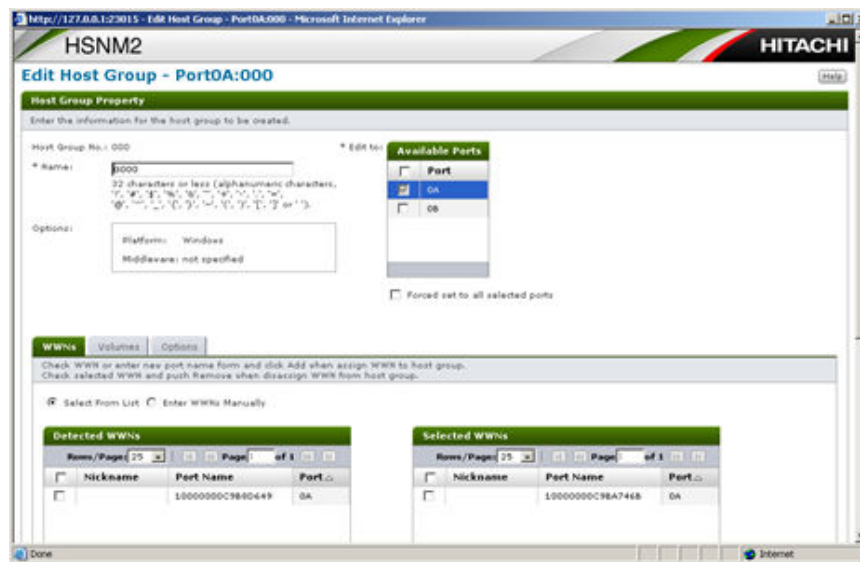
1. Open a browser and navigate to the Storage Navigator Modular 2 (SNM2) GUI at: <http://127.0.0.1:23015/StorageNavigatorModular/Login>
2. Log in with the user ID *system* and the password *manager*.
3. In the SNM2 GUI, in the Arrays navigation tree (middle menu), navigate to **Groups > Volumes > Host Groups**.



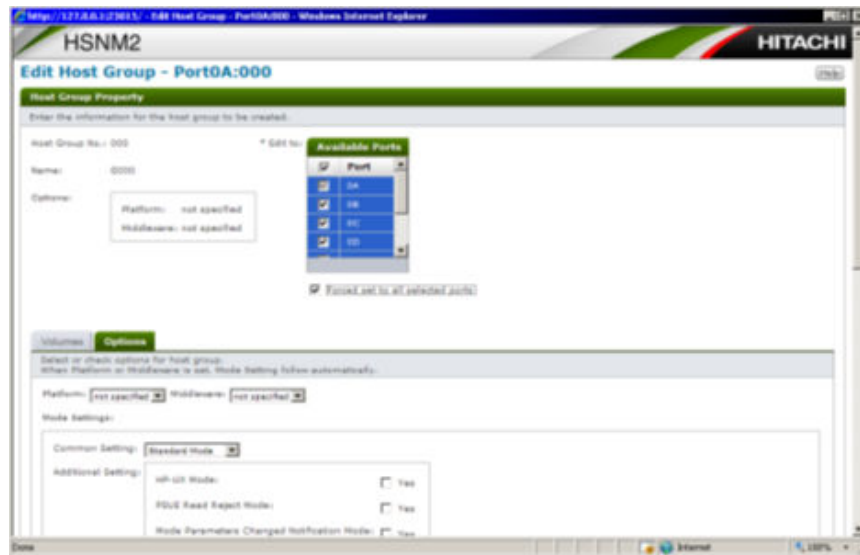
4. Under the Host Group column, click the group **000:G000 with 0A**, and then select **Edit Host Group** at the top of the pane.



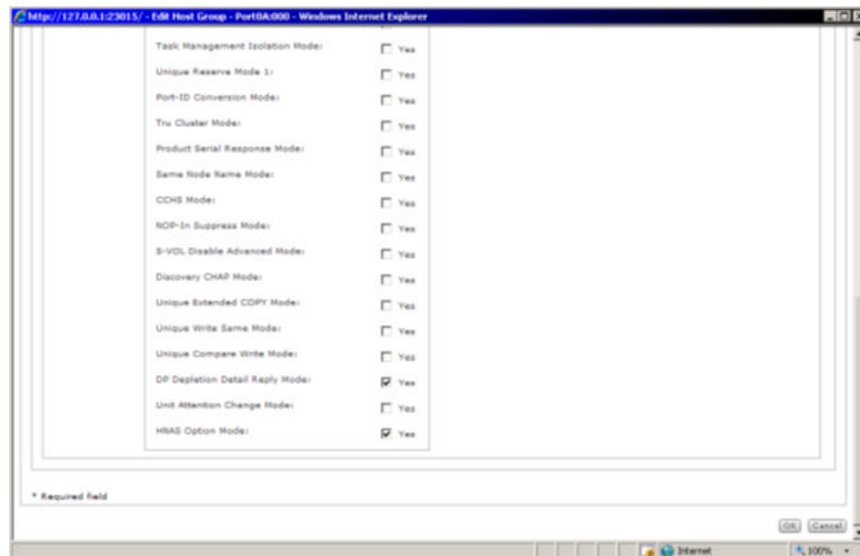
- In the Edit Host Group window, click the **Volumes** tab.



- Click the **Port** checkbox to select all ports and check the **Forced set to all selected ports**.  
Leave **Platform** and **Middleware** set to **not specified**.



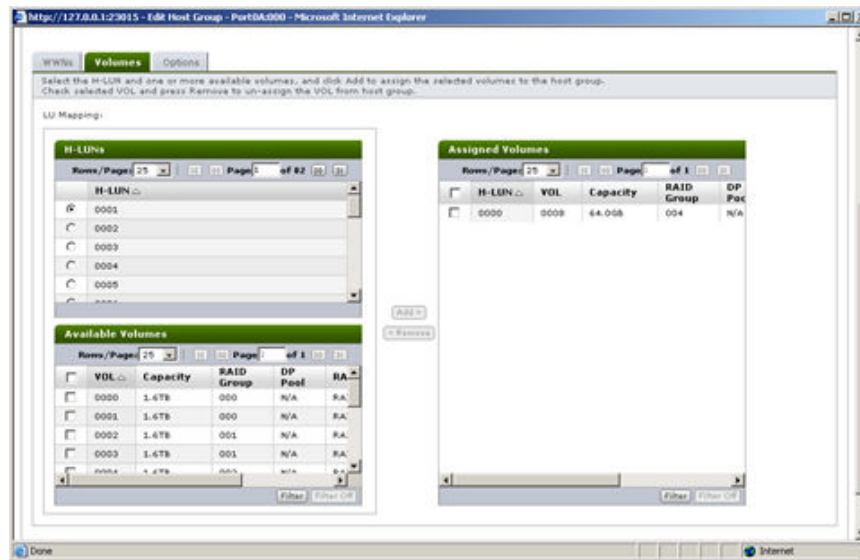
7. In the lower half of the window, select the HNAS Option Mode to **Yes**, and then click **OK** at the bottom of the window.



8. Add the required volumes to this host group.



**Important:** Map all of the LUNs that are created to *all array host ports* that will be connected to either the server or the SAN.



9. After the volumes are added, select the **Options** tab.
10. Set the **Platform** and **Middleware** lists to **not specified**, and then click **OK**.



11. Repeat this procedure for each host group that you want to edit.

### Next steps

Depending on the firmware code version you are using on the server and storage, you can configure additional settings in the storage software to improve performance. After you complete the additional configurations, you can set up the first server to be added.

## Configuring additional storage settings based on firmware

After making your initial configurations for host groups, you can set some additional configurations in the storage software to increase performance of both the storage and the server. The configurations are appropriate depending on the firmware code versions in use.

The configurations relate to the following firmware versions:

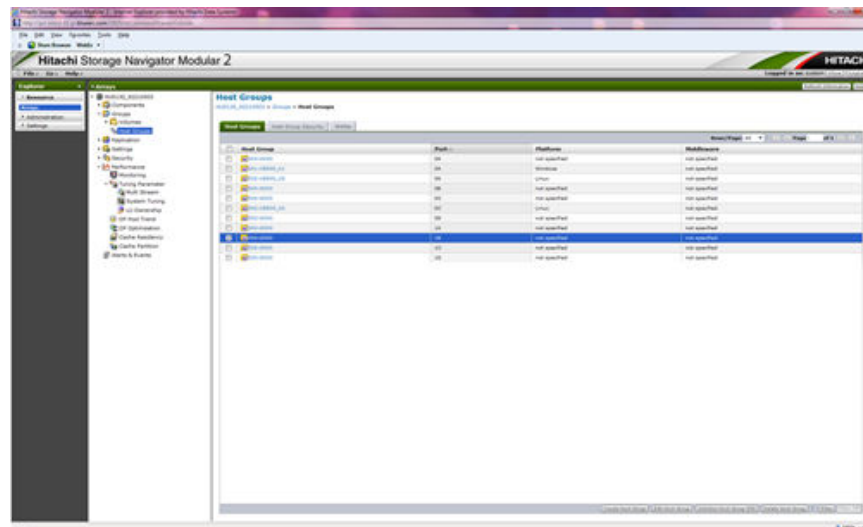
- Storage module HUS1x0 firmware code base version 0935A or later
- Server SU firmware code version 11. 2.33xx or later

Make these configuration settings immediately following the configuration of the host groups.

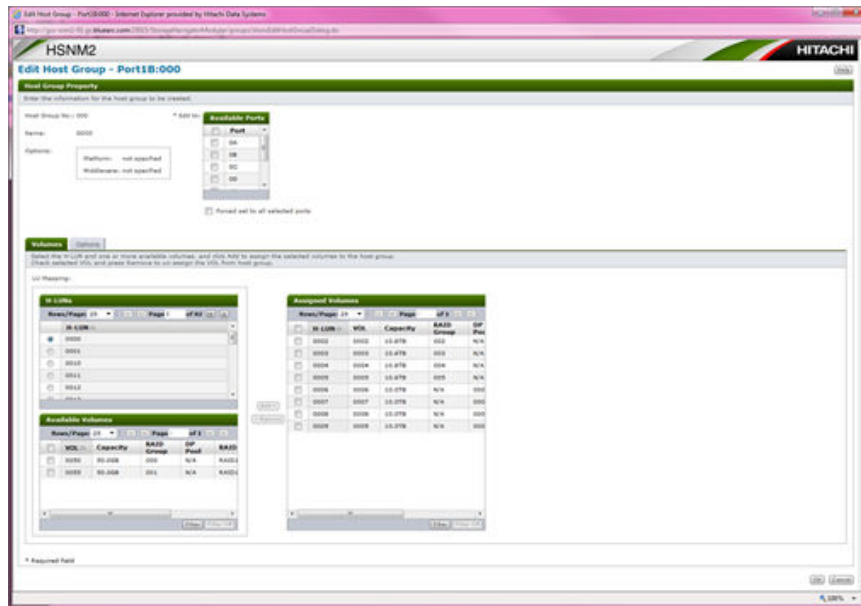
The configuration setting you make to the storage results in an array performance increase. You must then make the configuration settings on the server as well. Those changes enable the server to recognize the firmware version that is running on the storage arrays. After you configure the server, its firmware can then take advantage of the performance increase that resulted from the configuration setting you made in the storage. The change in per-port Q depth on the server depends upon the change you are making.

### Procedure

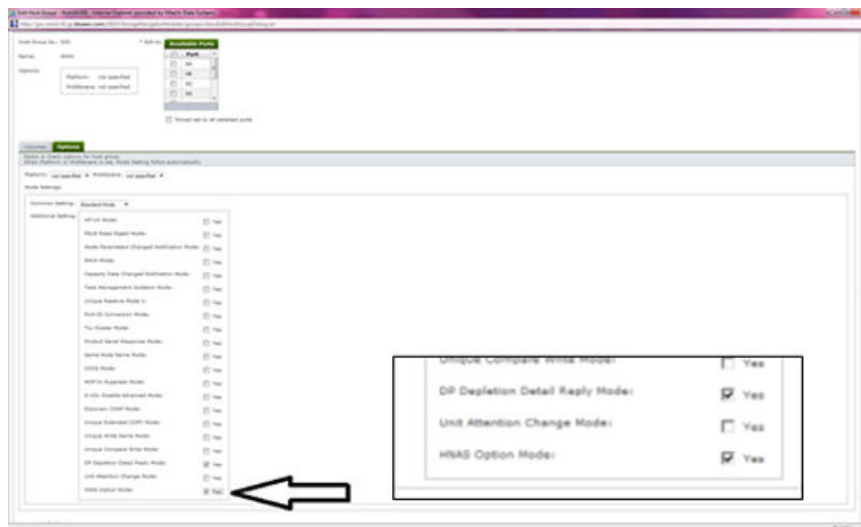
1. If the HUS Storage Module firmware code is base 0935A or greater, you must enable the **HNAS Option Mode** option.
  - a. In the SNM2 GUI, in the Arrays navigation tree (middle menu), navigate to **Groups > Host Groups** tab.
  - b. In the **Host Groups** window, under the **Host Group** column, click the host group that you are configuring.



The **Edit Host Group** window displays, and the **Volumes** tab is shown by default:



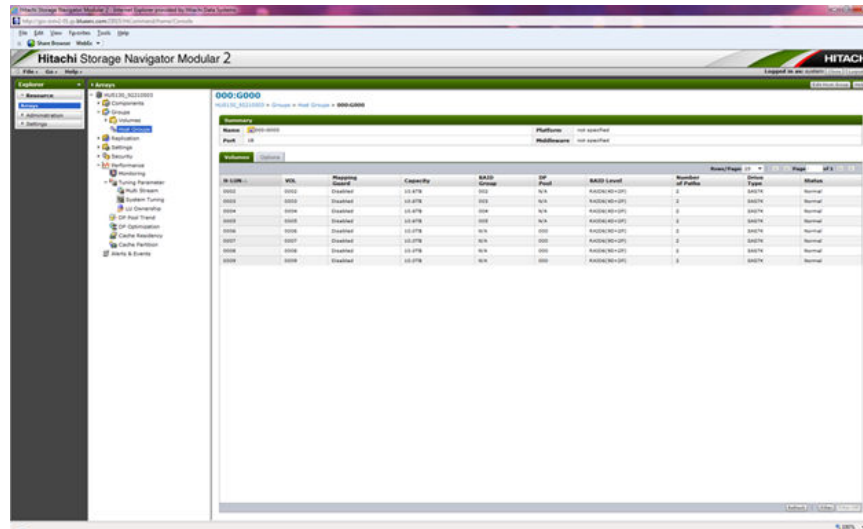
- c. In the **Edit Host Group** window, select the **Options** tab, and then select the **Yes** check box for **HNAS Option Mode**.



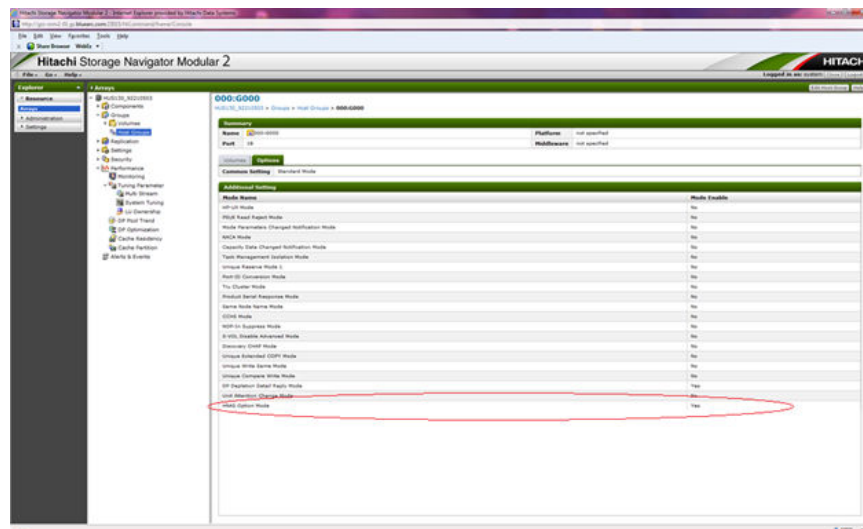
- d. Click **OK**.  
You are returned back to the SNM2 GUI.

e. Verify the setting by performing the following steps:

- Select **Host Groups**.



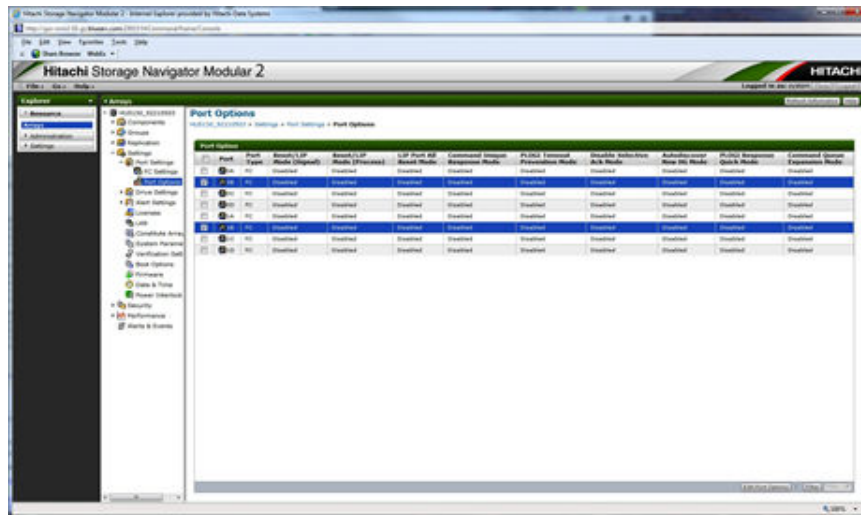
- Select the **Options** tab, and then verify that the **HNAS Option Mode** is set to **Yes**.



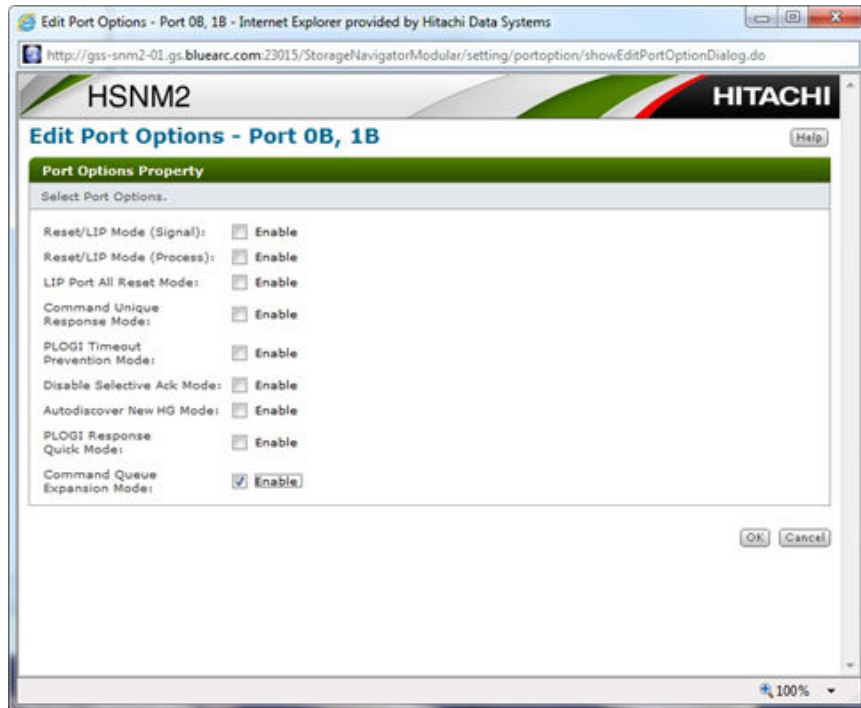
The storage configuration is complete.

2. If the server SU code is version 11. 2.33xx or later, perform the following steps:
  - a. From the SNM2 GUI, select **Settings > Port Settings > Port Options**.
  - b. In the **Port Options** window, select the check boxes for the associated ports.

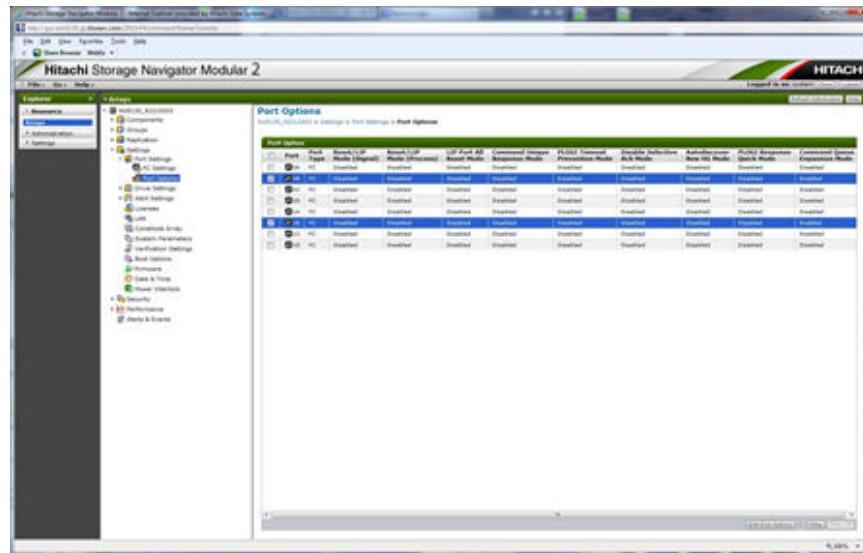




- c. Click **Edit Port Options** at the bottom of the window.
- d. In the **Edit Port Options** window, select the check box for **Command Queue Expansion Mode**, then click **OK**.



- e. In the **Port Options** dialog, under the **Command Queue Expansion Mode** column at the right side, confirm that the ports you configured now display **Enabled**.



The server firmware can now take advantage of the performance increase that resulted from the configuration setting you made in the storage. The change in per-port Q depth on the server depends upon the change you just made.

To take advantage of the increase on the storage array, you must perform the described two-pronged implementation on the server.

The server must be able to recognize that the array is running firmware version 09.35A. Before making this change, the server was not aware of the version of the code running on the array.

## Setting up the OS and software on an SMU

The Hitachi NAS Platform Series 4000 or Series 4000 system management unit (SMU) supports the following:

- CentOS version 6.2
- SMU software version 11

You must install the OS before installing the SMU software.

An external SMU is required for clustered server systems.

If you are running a single server, the SMU can be either external or embedded in the server. An embedded SMU does not have its own OS.

## Configuring a server administrative IP to access embedded SMUs

This command configures the administrative EVS public IP address of Eth0 on the server, which is used to access the system using Web Manager.

### Before you begin

Allow the server up to 10 minutes after powering on to ensure it fully starts all processes.

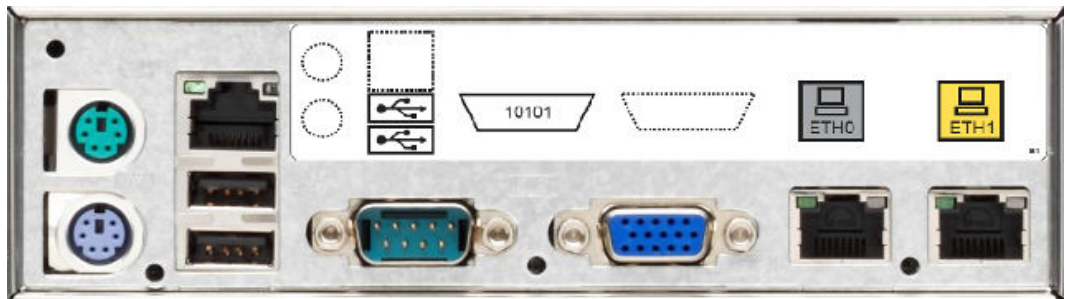
## Procedure

1. Either connect using KVM or attach an RS-232 null-modem cable (DB-9 female to DB-9 female) from your laptop to the serial port.

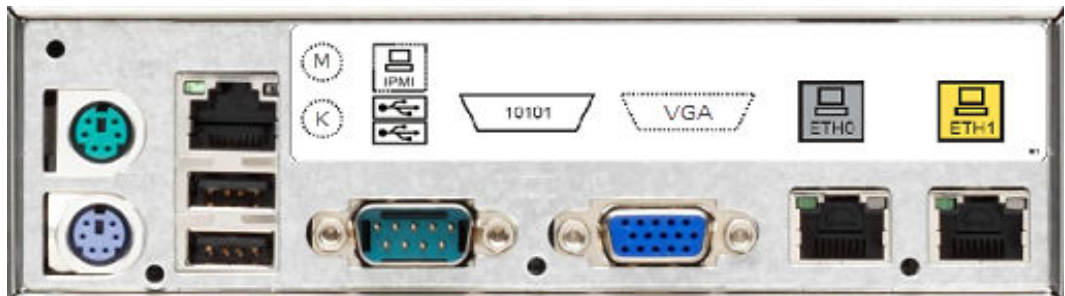
If using a serial connection, start a console session using your terminal emulation with the following settings:

- 115,200 bps
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control
- VT100 emulation

You may want to enable the logging feature in your terminal program to capture the session.



**Figure 41 NAS Platform 4040 rear panel Main Motherboard (MMB) port layout**



**Figure 42 NAS Platform 4060, 4080, and 4100 rear panel MMB rear port layout**

2. Log in to the server as `manager`.  
These credentials provide access to the Bali console. If you receive a `Failed to connect: Connection refused` error, wait a few moments and enter `ssc localhost`.
3. Enter `evsipaddr -l` to display the default IP addresses.

4. Enter `evsipaddr -e 0 -a -i admin_public_IP -m netmask -p eth0` to customize the administrative EVS public IP address for your local network.

This command configures the administrative EVS public IP address of Eth0 on the server, which is used to access the system using Web Manager.

5. Now that the administrative service is configured, connect the local network Ethernet cable to the Eth0 port.

## Installing the CentOS operating system

This section describes installing the CentOS version 6.2 operating system.

### Procedure

1. Switch on the connected external SMU using the power button on the front of the SMU.
2. Place the DVD containing the CentOS software in to the CD/DVD reader device. The SMU boots from the DVD.
3. Connect to the SMU by using either a KVM or a serial connection.

After the DVD software has booted up, the following screen displays with instructions.



**Note:** The installation examples are based on a KVM installation.

```

Welcome to SMU OS Installation
(CentOS 6.0)
Type the option and press <ENTER> to begin installing.

Clean installation, destroying all data in the hard drive:
clean-kvm   - Clean SMU OS install (erases entire HD) using KVM.
clean-serial - Clean SMU OS install (erases entire HD) using serial console.

For a second installation (only one installation already present):
second-kvm  - Second SMU OS install using KVM.
second-serial - Second SMU OS install using serial console.

For a virtual machine installation (only one partition):
virtual-smu -Virtual SMU OS install using KVM

- To boot the existing kernel press <ENTER>

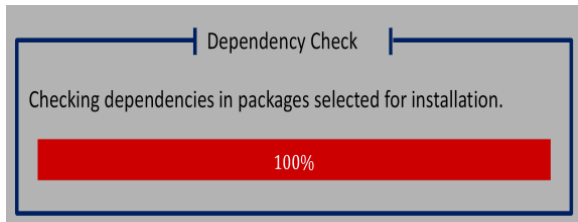
- Use the function keys listed below for more information.

[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: clean-kvm

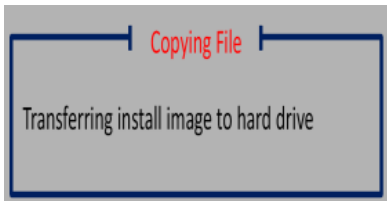
```

4. Type the command `clean-kvm` (or `clean-serial` when using serial connection), and then press `Enter`.

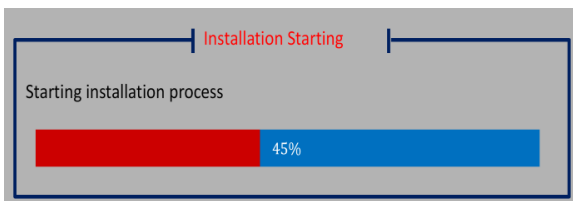
The systems runs a Dependency Check.



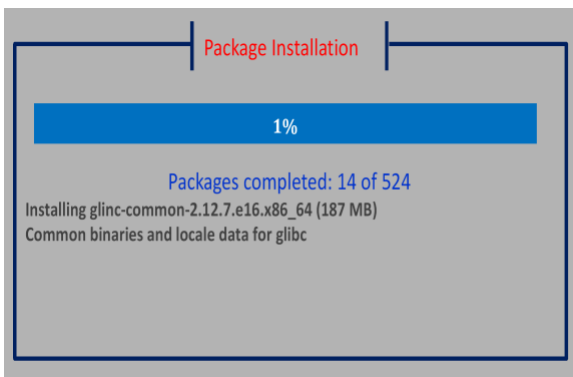
- When you choose the option to install, the system unpacks the needed packages from the DVD.



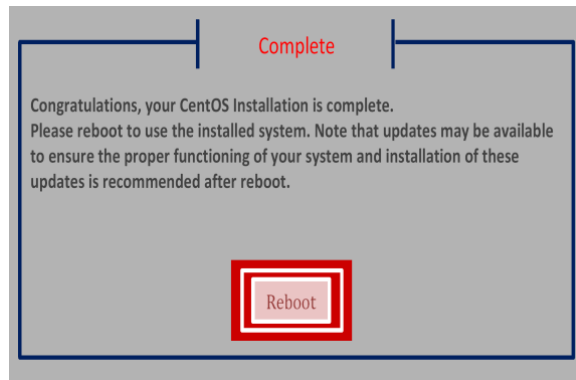
- After the packages are unpacked, the system copies the new files to the internal hard disk drives (HDDs) on the SMU, and then installs the files.



- The entire CentOS installation (using KVM) takes approximately 10 to 15 minutes.



5. After the installation completes, press `Enter` or click **Reboot** with the mouse to reboot the system.



6. Remove the DVD from the drive and store it safely.

### Next steps

After you complete the CentOS installation, you can install the SMU software.

## Initially configuring an external SMU

### Before you begin

Allow the server up to 10 minutes after powering on to ensure it fully starts all processes.

There are several options for console access:

- Monitor and keyboard connection
- IPMI network access to console sessions (PROVIDED AS-IS; neither supported nor maintained by HNAS engineering or HDS Support.)
- Serial cable from PCs with DB-9 serial ports
- USB-to-serial cable from PCs with USB, but without DB-9 serial ports

The SMU 400 has two serial DB-9 ports, one on the rear, and one on the front. These two serial ports are *not* equivalent. Both ports can be used with direct serial cables or with USB-to-serial cables, and both ports can be used to access BIOS screens. However, only the rear port can be used for a Linux login session after boot.

DB-9 serial port	Identity in BIOS	Availability
Rear	COM1	Boot time and after boot
Front	COM2	Boot time only; blank after boot

### Procedure

1. Either connect the KVM or attach a null-modem cable from your laptop to the serial port of the system management unit (SMU).

If using a serial connection, start a console session using your terminal emulation with the following settings:

- 115,200 b/s,
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control
- VT100 emulation

You may want to enable the logging feature in your terminal program to capture the session.

2. Log in as root and run `smu-config`.

### Result

The SMU completes the configuration, and reboots.

## Installing and configuring the SMU software

After you have installed the CentOS operating system (OS), you can set up the system management unit (SMU) software.

### Procedure

1. Either make a serial connection or a KVM connection to the SMU.
  - For a KVM connection, connect a monitor, keyboard, and mouse to the appropriate ports on the back of the SMU .
  - For a serial connection, start a console session using your terminal emulation program. Use the following settings:
    - 115,200 b/s
    - 8 data bits
    - 1 stop bit
    - No parity
    - No hardware control flow
    - VT100 emulation

You may want to enable the logging feature in your terminal program to capture the session.

2. Place the SMU Setup DVD into the SMU DVD tray.
3. To mount the DVD, issue the command: `mount /media/cdrecorder`

4. To run the `autorun` script, issue the command: `/media/cdrecorder/autorun`

```
CentOS Linux release 6.2 (Final)
Kernel 2.6.32-220.el6.x86_64 on N X86_64

Localhost login : root
Password:
[toot@localhost ~]# mount /media/cdrecorder
mount: block device /dev/sr0 is write-protected, mounting read-only
[toot@localhost ~]# /media/cdrecorder/autorun
Logging to /var/opt/smu/log/installer/smu_inst_100003867.201007021245
===== Running /media.cdrecorder/Packages/Installer-
1.3/app
Copying the packages onto the system
```

The installation of the SMU update process starts. The SMU reboots when the installation is complete.

5. When the installation is complete, remove the DVD from the drive and store it safely.
6. After the reboot, log in to the SMU using the root user.
7. To begin the SMU configuration, issue the command: `smu-config`

Use the settings in the following table to configure the SMU:

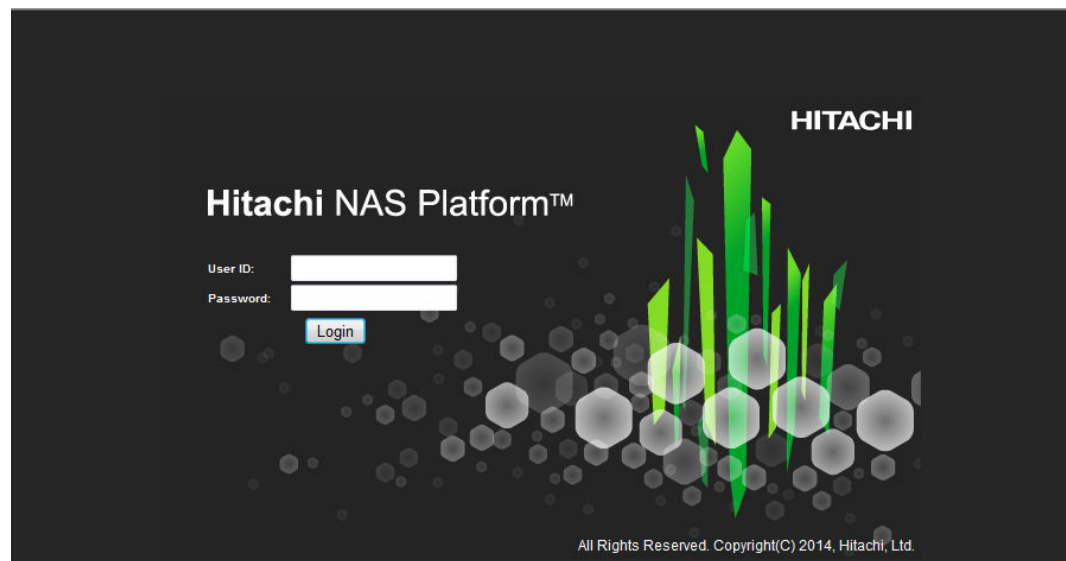
Setting	Default	Customer Setting
Root password		Provided by customer
Manager password		Provided by customer
SMU public IPv4 address (eth0)	xxx.xxx.xxx.xxx	Provided by customer
SMU public IPv4 netmask (eth0)	xxx.xxx.xxx.xxx	Provided by customer
IPv4 gateway	xxx.xxx.xxx.xxx	Provided by customer
Standby SMU		n (if primary SMU)
SMU private IPv4 address (eth1)	192.0.2.1	192.0.2.1
Configure IPv6 address		n (unless required by customer)
Use stateless auto-configuration (SLAAC)		n (unless required by customer and IPv6 address is configured)
SMU public IPv6 address (eth0)		Provided by customer (if IPv6 address is configured)



Setting	Default	Customer Setting
IPv6 gateway		Provided by customer (if IPv6 address is configured)
SMU domain (fully qualified)		Provided by customer
SMU host name (without the domain name)	smu1	Provided by customer

For more details about running the smu-config script, see [Running the SMU-CONFIG script \(on page 140\)](#).

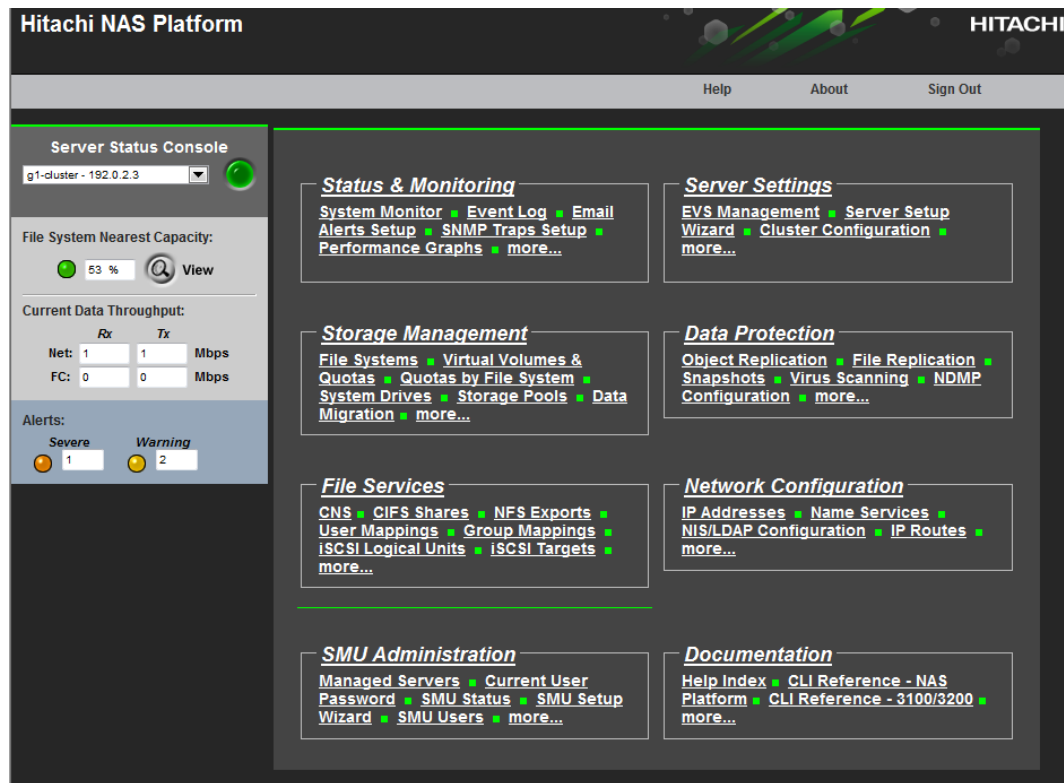
8. Review all of the settings you have made, and then enter `Y` if they are correct. The script sets up the network interfaces and default properties, and then the SMU reboots.
9. Connect your laptop or workstation browser to one of the SMU IP addresses.



10. Log in to the SMU using the `admin` User ID.



**Note:** The user ID here (`admin`) is *not* the same as that used by the SMU CLI (`manager`).



When the SMU GUI opens, the SMU configuration has been verified.

- When you have finished installing the SMU, and before setting up the server, navigate to **Home > SMU Administration > SMU Setup Wizard** to configure the SMU settings.

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

## Configuring an HNAS Platform or HUS File Module server

Servers can be used in a single Hitachi NAS Platform or Hitachi Unified Storage File Module server configuration, but using two servers is more common. When you use a clustered server configuration, you configure first one server, then the other server.



**Note:** For the purposes of this document, when you use two servers, the servers are referred to as a cluster, and then the servers are referred to as nodes.

When you are using two servers, you must determine which node is node 1 and which node is node 2. HDS only licenses one of the nodes completely. The node that is licensed completely is node 1, or the first node in a cluster. Look at the paper or CD license keys, cross reference the node serial numbers, and perform the work on the node that is licensed as node 1.

## Configuring the first HNAS or HUS File Module server

Perform the software configurations steps for the server. If you have installed a second server, you can configure its software after you finish the first server.

### Before you begin

Be aware that when the server starts, it makes a significant amount of noise. When the login prompt appears, wait for the noise to subside before logging in. When the fans stop blowing loudly (not entirely), you can log in.



**Note:** The screen output may vary slightly depending on the server model that you are configuring.

### Procedure

1. Connect to the server with a serial or KVM connection.
2. Power on the server.  
The system boots.
3. Log in with the `root` user.  
If the login is successful, the Linux prompt for the unit is displayed.
4. Identify whether the server has already had the `nas-preconfig` script run on it by issuing the command: `ssc localhost`
  - If the server displays the server name and MAC address as shown, the script has already been run, and the server has booted fully. Skip to [step 8 \(on page 96\)](#).

```
HDS NAS OS Console
Server name : testhost
MAC ID :4D-7F-DD-BC-D0-06
```

- If the server refuses the connection, the script needs to be executed. See [Running the NAS-PRECONFIG script \(on page 126\)](#).
5. Enter `reboot`, and when prompted, log in to Linux with the `root` user.
  6. View the status LEDs on the rear of the unit.  
When the power LED is flashing quickly, the server is booting.  
Once the server is fully booted, the power and server status flashes slowly green.
  7. To be sure that the `nas-preconfig` script ran successfully, issue the command: `ssc localhost`

The server name and MAC address are displayed if the execution was successful.

```
HDS NAS OS Console
Server name : testhost
MAC ID :4D-7F-DD-BC-D0-06
```

8. Set the server to the correct IP address by using the following steps:



**Note:** The correct IP address is 192.0.2.200.

- To check the current IP address, issue the command: **ipaddr**

```
testhost :$ ipaddr
Cluster node ID = 1
##      IP Address      Mask          Port
--      -
1      192.0.2.200      255.255.255.0 eth1
```

- To reset the IP address, issue the command: **ipaddr -i 192.0.2.200 -m 255.255.255.0**

9. Set the server to the correct admin IP address for eth1 by using the following steps:



**Note:** The correct admin IP address for eth1 is 192.0.2.2.

- Check the admin IP address for the unit by issuing the command: **evs list**

```
testhost :$ evs list
Node  EVS ID  Type      label      Enabled  Status      IP Address      Port
----  -
1      0          Cluster   testhost   Yes      Online      192.0.2.200     eth1
1      0          Admin     testhost   Yes      Online      192.0.2.2       eth1
                                           192.168.31.191  eth0
```

- Remove any additional addresses that exist on eth1, other than 192.0.2.2, by issuing the command: **evsipaddr -e 0 -r -i <IP address to remove>**
- If the Admin IP address is not 192.0.2.2, change it by issuing the command: **evsipaddr -e 0 -u -i 192.0.2.2 -m 255.255.255.0 -p eth1**



**Note:** If you need to change the admin address, you must first remove the address present on eth0. After you remove the address on eth0, you can use the change command for the admin address on eth1.

10. If your storage configuration includes Fibre Channel (FC) switches, issue the following command: **fc-link-type -t N**

```
testhost:$ fc-link-type -t N
Cluster node 1
Set interface link type OK
FC 1: N
FC 2: N
FC 3: N
FC 4: N
```

11. If your storage configuration is direct-attached, issue the following command: **fc-link-type -t NL**

```
testhost:$ fc-link-type -t N
Cluster node 1
Set interface link type OK
FC 1: NL
FC 2: NL
FC 3: NL
FC 4: NL
```

12. Confirm that all of the FC ports are operating at the correct speed by issuing the command appropriate for the server model:

Model	Speed	Command
HNAS 4040	4 GB	<code>fc-link-speed -s 4</code>
HNAS 4060, 4080, and 4100	8 GB	<code>fc-link-speed -s 8</code>

- HNAS 4040 command: `fc-link-speed -s 4`

```
testhost:$ cn all fc-link-speed -s 4
Cluster node 1
Set interface link speed OK
FC 1: 4
FC 2: 4
FC 3: 4
FC 4: 4
```

- HNAS 4060, 4080, and 4100 command: `fc-link-speed -s 8`

```
testhost:$ cn all fc-link-speed -s 8
Cluster node 1
Set interface link speed OK
FC 1: 8
FC 2: 8
FC 3: 8
FC 4: 8
```

13. Confirm that all FC ports are correctly enabled by issuing the following commands:

```
cn all fc-link 1 enable
cn all fc-link 2 enable
cn all fc-link 3 enable
cn all fc-link 4 enable
```

```

testhost:$ cn all fc-link 1 enable
Cluster node 1
FC 1: Enabled
testhost:$ cn all fc-link 2 enable
Cluster node 1
FC 2: Enabled
testhost:$ cn all fc-link 3 enable
Cluster node 1
FC 3: Enabled
testhost:$ cn all fc-link 4 enable
Cluster node 1
FC 4: Enabled

```

All of the FC ports are enabled, and set for the correct speed and the correct topology.

14. Confirm that the installed software is the current GA code by issuing the command: **ver**



**Note:** The following example shows the certified version of the server software as 10.2.3072.08, but a newer version may be available.

```

testhost:$ ver

Model: 3080-G2

Software: 10.2.3072.08

Hardware: NAS Platform (M2SEKW1213163)

board      MMB1
mmb        10.2.3072.08

```

Here you can see the model type and serial number.

15. Check the MAC ID by issuing the command: **getmacid**

```

testhost:$ getmacid
MAC ID is 4D-7F-DD-BC-D0-06
testhost:$

```

16. Leave this server in its current state while you configure the second server. If you are not using a second server, leave this server in its current state while you update the firmware on the server.

## Configuring the second HNAS or HUS File Module server

After you have set up the first HNAS or Hitachi Unified Storage File Module server, you can set up the second server. The configuration steps are the same for both servers, but the system responses to some commands are different.

### Before you begin

Be aware that when the server starts, it makes a significant amount of noise. When the login prompt appears, wait for the noise to subside before logging in. When the fans stop blowing loudly (not entirely), you can log in.



**Note:** The screen output may vary slightly depending on the server model that you are configuring.

### Procedure


1. Connect to the server with a serial or KVM connection.
2. Power on the server.  
The system boots.
3. Log in with the `root` user.  
If the login is successful, the Linux prompt for the unit is displayed.
4. Identify whether the server has already had the `nas-preconfig` script run on it by issuing the command: `ssc localhost`
  - If the server displays the server name and MAC address as shown, the script has already been run, and the server has booted fully. Skip to [step 8 \(on page 96\)](#).

```
HDS NAS OS Console
Server name : testhost
MAC ID :4D-7F-DD-BC-D0-06
```

- If the server refuses the connection, the script needs to be executed. See [Running the NAS-PRECONFIG script \(on page 126\)](#).
5. Enter `reboot`, and when prompted, log in to Linux with the `root` user.
  6. View the status LEDs on the rear of the unit.  
When the power LED is flashing quickly, the server is booting.  
Once the server is fully booted, the power and server status flashes slowly green.
  7. To be sure the `nas-preconfig` script ran successfully, issue the command: `ssc localhost`  
The server name and MAC address are displayed if the execution was successful.

```
HDS NAS OS Console
Server name : testhost
MAC ID :4D-7F-DD-BC-D0-06
```

8. Set the server to the correct IP address by using the following steps:


 **Note:** The correct IP address is 192.0.2.201.

- To check the current IP address, issue the command: **ipaddr**

```
testhost :$ ipaddr
Cluster node ID = 1
##      IP Address      Mask      Port
--      -
1      192.0.2.201      255.255.255.0      eth1
```

- To reset the IP address, issue the command: **ipaddr -i 192.0.2.201 -m 255.255.255.0**


9. Set the server to the correct admin IP address for eth1 by using the following steps:

 **Note:** The correct admin IP address for eth1 is 192.0.2.3.

- Check the admin IP address for the unit by issuing the command: **evs list**

```
testhost :$ evs list
Node  EVS ID  Type      label      Enabled  Status      IP Address      Port
----  -
1      0      Cluster   testhost   Yes      Online      192.0.2.200     eth1
1      0      Admin     testhost   Yes      Online      192.0.2.2       eth1
                                           192.168.31.191  eth0
```

- Remove any additional addresses that exist on eth1, other than 192.0.2.3, by issuing the command: **evsipaddr -e 0 -r -i <IP address to remove>**
- If the Admin IP address is not 192.0.2.3, change it by issuing the command: **evsipaddr -e 0 -u -i 192.0.2.3 -m 255.255.255.0 -p eth1**

 **Note:** If you need to change the admin address, you must first remove the address present on eth0. After you remove the address on eth0, you can use the change command for the admin address on eth1.

10. If your storage configuration includes Fibre Channel (FC) switches, issue the following command: **fc-link-type -t N**



```
testhost:$ fc-link-type -t N
Cluster node 1
Set interface link type OK
FC 1: N
FC 2: N
FC 3: N
FC 4: N
```

11. If your storage configuration is direct-attached, issue the following command: **fc-link-type -t NL**

```
testhost:$ fc-link-type -t NL
Cluster node 1
Set interface link type OK
FC 1: NL
FC 2: NL
FC 3: NL
FC 4: NL
```

12. Confirm that all of the FC ports are operating at the correct speed by issuing the command appropriate for the server model:

Model	Speed	Command
HNAS 4040	4 GB	<b>fc-link-speed -s 4</b>
HNAS 4060, 4080, and 4100	8 GB	<b>fc-link-speed -s 8</b>

- HNAS 4040 command: **fc-link-speed -s 4**

```
testhost:$ cn all fc-link-speed -s 4
Cluster node 1
Set interface link speed OK
FC 1: 4
FC 2: 4
FC 3: 4
FC 4: 4
```

- HNAS 4060, 4080, and 4100 command: **fc-link-speed -s 8**

```
testhost:$ cn all fc-link-speed -s 8
Cluster node 1
Set interface link speed OK
FC 1: 8
FC 2: 8
FC 3: 8
FC 4: 8
```

13. Confirm that all FC ports are correctly enabled by Issue the following commands:

```
cn all fc-link 1 enable
cn all fc-link 2 enable
```

```
cn all fc-link 3 enable
cn all fc-link 4 enable
```

```
testhost:$ cn all fc-link 1 enable
Cluster node 1
FC 1: Enabled
testhost:$ cn all fc-link 2 enable
Cluster node 1
FC 2: Enabled
testhost:$ cn all fc-link 3 enable
Cluster node 1
FC 3: Enabled
testhost:$ cn all fc-link 4 enable
Cluster node 1
FC 4: Enabled
```

All of the FC ports are enabled, and set for the correct speed and the correct topology.

14. Confirm that the installed software is the current GA code by issuing the command: **ver**



**Note:** The latest certified version of the server software is 10.2.3072.08.

```
testhost:$ ver

Model: 3080-G2

Software: 10.2.3072.08

Hardware: NAS Platform (M2SEKW1213163)

board      MMB1
mmb        10.2.3072.08
```

Here you can see the model type and serial number.

15. Check the MAC ID by issuing the command: **getmacid**

```
testhost:$ getmacid
MAC ID is 4D-7F-DD-BC-D0-06
testhost:$
```

16. Confirm that the SMU service is running by performing the following steps:
  - a. Issue the command: **smu-service-status**

```
testhost:~$ smu-service-status
The SMU status is: running
testhost:~$
```

- b. If the status is not `running`, activate the embedded SMU.



**Note:** See the steps in the section about updating the firmware of the HNAS servers.

17. Leave this server in its current state while you update the firmware on the servers.

## Adding the servers as managed servers in the SMU

After you have set up the servers and configured them, you can add them as managed servers in the system management unit (SMU). That way, the system recognizes the new servers right away. Having the new servers recognized by the SMU makes it easier for you to determine which server is to be considered server one. This determination is especially important if you are building a server cluster.

## Building a two-node cluster

When you are using an external SMU, you can build and configure a two-node server cluster.

### Before you begin

All servers you intend to add to the cluster must already be managed by the SMU. For information on configuring the SMU to manage a server, see the *Hitachi NAS Platform Server and Cluster Administration Guide*.



**Note:** Clusters of two or more nodes require an external SMU.

### Procedure

1. Log in to the SMU.
2. Navigate to **Home > SMU Administration > Managed Servers**, and then click **Add**.

SMU Administration [Home](#) > [SMU Administration](#) > Managed Servers

### Managed Servers

IP	Server Username	Model	Cluster Type	Status	
<input type="checkbox"/> 172.31.60.59 - gizmo1	supervisor	Unknown Model	Unknown Type	<span style="color:red">●</span>	<a href="#">details</a> <a href="#">Set as Current</a>
<input type="checkbox"/> 192.0.2.3 - g1-cluster	supervisor	3090-G2	Clustered	<span style="color:green">●</span>	<a href="#">details</a> <a href="#">Set as Current</a>

[Check All](#) | [Clear All](#)

**Actions:** [add](#) [remove](#)

**Shortcuts:** [Server Upgrade Utility](#) [Server Setup Wizard](#)

- Fill out the IP address information and credentials to be able to reach your first server.

The server IP address is the Admin EVS address that is set on the server. The user name and password are both `supervisor`.

If the following message appears, update your server firmware before continuing.



- Be sure to disable the embedded SMU when prompted.
- Confirm that your first server is displayed in the list of servers in the cluster.
- Repeat the previous steps to add the second server.
- Confirm that the second server is also displayed in the list of managed servers.
- Navigate to **Home > Server Settings > License Keys**, and then click **Add**.

MAC ID	Cluster	EVS	Storage Capacity	Universal NAS Virtual Capacity	Model Type	Expires	details
<input type="checkbox"/> D404-28EC-D341-E8F0-67B9-209D-83B1		0 EVS					details
<input type="checkbox"/> D405-38E1-5A41-E8F0-679B-209D-E487		0 EVS					details
<input type="checkbox"/> D405-B23B-0941-E8F0-67AD-209D-859F		0 EVS					details
<input type="checkbox"/> D406-1628-F741-E8F0-6787-209D-6148		0 EVS					details
<input type="checkbox"/> D406-B041-A841-E8F0-6784-209D-E35F-DE98-1B1C		0 EVS		100 TB			details
<input type="checkbox"/> D406-B059-8E41-E8F0-6784-209D-E35F-DE98-636C		0 EVS		100 TB			details
<input type="checkbox"/> D407-7950-3F41-E8F0-6799-209D-6B6A		0 EVS					details
<input type="checkbox"/> D419-8820-FE41-E8F0-67B8...B68-5B6B-51BD-912D-BFD7	Max 4 Nodes	64 EVS	256 TB				details
<input type="checkbox"/> D41B-521E-1041-E8F0-679C-209D-6AE3		0 EVS					details
<input type="checkbox"/> D41B-7FEE-A441-E8F0-679D-209D-F95F-DE03-B2BE		0 EVS					details

**Total Licensed on All Unexpired Keys**

CIFS	NFS	SFM
WORM	ISCSI	Data Migrator
FS Roll Back	Snapshot Restore	CNS
Read Cache	HDS	DDN
EVS Security	SyncDR	Replication
XVL	FSRS	File Clone
BlueArcRS	Performance Accelerator	Data Migrator Cloud
Premium Deduplication	Extension Pack Secure FTP	

- In the License Key Add dialog, either import the license key file or import the separate key copied from the file.

10. Navigate to **Home > Server Settings > License Keys** and confirm that your license key has been added.
11. Navigate to **Home > Server Settings > Add Cluster Node**.

12. Complete the fields in the Cluster Wizard for the first server by performing the following steps:



**Note:** After the wizard reboots the node, the Cluster Node IP Address and Subnet Mask displays the cluster node IP address that is in effect. The IP address may be changed here.

- a. Give the cluster a name.
- b. Change the IP address if required. If the field is blank, enter a suitable free IP address from the private management network to which your SMU is attached.
- c. Select the SMU as your quorum device.
- d. Click **OK**.

The server reboots.

13. Watch to confirm that the server is added successfully.
14. You can add your second server now, or do it later.
15. To switch from first server to the managed server you want to add to the cluster, navigate to **Home**, and choose the managed server from those listed in the **Server Status Console** drop down list.  
For more details, see the *Hitachi NAS Platform Server and Cluster Administration Guide*.
16. Install the license key for this second server so you can add the server to the cluster.
17. Go back to the first server before you add another node.

18. If you are adding a second server later, navigate to **Home > Server Settings > Add Cluster Node**.
19. In the Cluster Wizard, enter the credentials of your second server. The user name and password are usually `supervisor`.
  - The Cluster Node IP Address shown is in effect after the node joins the cluster. You can change the IP address here if needed.
  - Entering the IP is not necessary to reach your second server.
20. Navigate to **Home > SMU Administration > Managed Servers**, and confirm that a server is displayed and shows the status of `Clustered`.



**Note:** Only a single cluster entry can be visible.

Your dual-server cluster had been successfully built.

## Configuring the Ethernet switch as a cluster switch

This section describes the configuration of the 10 Gigabit Ethernet (10 GbE) switch that is required when you have three or more servers in your system. After you have set up the servers, storage, and system management units (SMU), and configured the Fibre Channel switches, you can configure the 10 GbE switch.

Use this procedure to configure the Ethernet switch (a Brocade VDX 6740) for use as an ICC (intra-cluster communication) switch.



**Note:** The Brocade VDX 6740 Ethernet switch is *not* suitable for shipment loaded in the rack. At the distribution center, after the VDX 6740 Ethernet switch is tested in the enclosure, it is removed from the enclosure and is packed separately (brown box) and shipped separately.

### Procedure

1. Connect to the switch's serial port using the serial cable supplied with the switch, 9600 8N1 no flow control. Log in with user name `admin`, password `password`.
2. Set passwords (optional).

```
sw0# configure terminal
Entering configuration mode terminal
sw0(config)# username user password
(<WORD>): *****
sw0(config)# username admin password
(<WORD>): *****
```

3. Set IP settings.

```
configure terminal
interface Management 1/0
no ip address dhcp
ip address IPv4-address/length
ipv6 address IPv6-address/length
rbridge-id 1
ip route 0.0.0.0/0 gateway
```

**Example:**

```
sw0# configure terminal
Entering configuration mode terminal
sw0(config)# interface Management 1/0
sw0(config-Management-1/0)# no ip address dhcp
sw0(config-Management-1/0)# ip address 192.0.2.123/24
sw0(config-Management-1/0)# ipv6 address 2001:db8:1234::5678/64
sw0(config-Management-1/0)# rbridge-id 1
sw0(config-rbridge-id-1)# ip route 0.0.0.0/0 192.0.2.1
```

**4. Priority mapping.**

Trusting priority tags is more complicated than on previous models. One must define a mapping that can then be applied to each interface.

The mapping output must avoid both 3 and 7, as these are reserved (this is not mentioned in Brocade's documentation). The shuffling of 0-2 is purely to allow for pre-7.0 software releases' use of an older standard (some customer systems are still running affected versions; it is conceivable that one of these may need a replacement cluster switch.) This map is applied to each port as part of the per-port configuration below.

```
sw0(config)# qos map cos-mutation hnas 2 1 0 4 4 5 6 6
```

**5. Configure ports (cluster-specific configuration).** Most other configuration is per port. It is necessary to increase the MTU to allow large enough jumbo frames. The port should be set to trust priority tags on inbound frames. Each port must also be explicitly enabled.

```
sw0(config)# interface TenGigabitEthernet 1/0/1
sw0(conf-if-te-1/0/1)# mtu 9216
sw0(conf-if-te-1/0/1)# switchport
sw0(conf-if-te-1/0/1)# qos cos-mutation hnas
sw0(conf-if-te-1/0/1)# interface TenGigabitEthernet 1/0/2
sw0(conf-if-te-1/0/2)#
```

Repeat these steps for all ports required. Unused ports could be left disabled to guard against accidental mis-connection.

**6. Configuring VLANs for multiple clusters.**

Where cluster switches are shared by multiple clusters, or for cluster and non-cluster connections, each cluster must have its own VLAN. In this case, no cluster should be assigned to VLAN 1. No per-VLAN configuration is required, but a VLAN must be (trivially) configured before ports can be added to it:

```
sw0(config)# interface Vlan 2
sw0(config-Vlan-2)# exit
sw0(config)# interface TenGigabitEthernet 1/0/1
sw0(conf-if-te-1/0/1)# switchport access vlan 2
sw0(conf-if-te-1/0/1)# interface TenGigabitEthernet 1/0/2
sw0(conf-if-te-1/0/2)# switchport access vlan 2
```

**7. In cases where an inter-switch link is needed, provided the switch at the other end is a compatible model, no special configuration should be needed.** Brocade's VCS system should do everything automatically.**8. To save the configuration:**

```
sw0(config)# exit
sw0# copy running-config startup-config
This operation will modify your startup configuration. Do you
want to continue? [y/n]:y
```

## Configuring the Ethernet switch to the storage system

After the switches are racked, see the *Brocade VDX 6740 Switch Configuration for use in an HNAS Cluster Configuration Guide* for information about switch configuration.

## Configuring HyperTerminal for the Ethernet switch configuration

You can use the HyperTerminal software to access the switch for configuration.

### Procedure

1. Start the HyperTerminal software.  
The Connection Description dialog displays.
2. In the Name field, type `TX24 Switch`, and then click **OK**.  
The Connect To dialog box displays.
3. From the **Connect using** drop down menu, select **COM1**, and then click **OK**.
4. Enter the following values in the COM1 properties dialog:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
5. Click **OK**.
6. Choose **File** and then **Save** to save the HyperTerminal configuration.

## Recovering from a lost password during switch configuration

By default, the CLI does not require passwords. However, if someone has configured a password for the device and the password has been lost, you can regain super-user access to the device using the following procedure.

### Procedure

1. Connect the null modem cable between COM1 of the Test Set PC to the switch's management serial port.
2. Start the HyperTerminal software.
3. While the system is booting, before the initial system prompt appears, type `b` to enter the boot monitor.
4. At the boot monitor prompt, issue the command: `no password`





**Note:** You cannot abbreviate the `no password` command.

The system displays: `OK! Skip password check when the system is up.`

5. At the boot monitor prompt, issue the command: `boot system flash primary`  
The device bypasses the system password check.
6. When the console prompt reappears, assign a new password.

## Configuring a system with an embedded SMU

### Customizing the server administrative IP address

#### Before you begin

Allow the server up to 10 minutes after powering on to ensure it fully starts all processes.

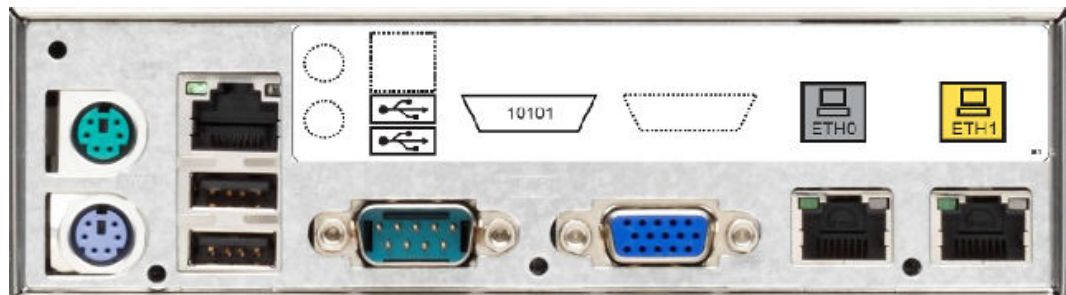
#### Procedure

1. Either connect using KVM or attach an RS-232 null-modem cable (DB-9 female to DB-9 female) from your laptop to the serial port.

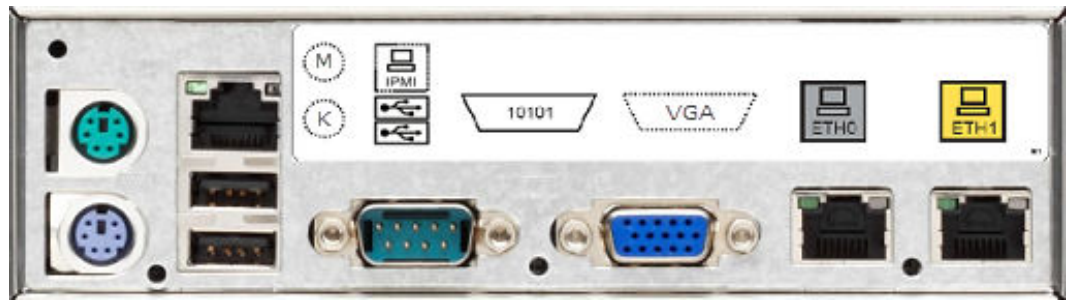
If using a serial connection, start a console session using your terminal emulation with the following settings:

- 115,200 bps
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control
- VT100 emulation

You may want to enable the logging feature in your terminal program to capture the session.



**Figure 43** NAS Platform 4040 rear panel Main Motherboard (MMB) port layout



**Figure 44 NAS Platform 4060, 4080, and 4100 rear panel MMB rear port layout**

2. Log in to the server as `manager`.  
These credentials provide access to the Bali console. If you receive a `Failed to connect: Connection refused` error, wait a few moments and enter `ssc localhost`.
3. Enter `evsipaddr -l` to display the default IP addresses.
4. Enter `evsipaddr -e 0 -a -i admin_public_IP -m netmask -p eth0` to customize the administrative EVS public IP address for your local network.  
This command configures the administrative EVS public IP address of `Eth0` on the server, which is used to access the system using Web Manager.
5. Now that the administrative service is configured, connect the local network Ethernet cable to the `Eth0` port.

## Using the server setup wizard

### Procedure

1. From a browser, enter `http://admin_public_IP` to launch Web Manager.
2. Navigate to **Server Settings > Server Setup Wizard**.  
When accessing the system for the first time, it might prompt you for the following:
  - New licenses. Contact customer support for assistance if none are present.
  - Allow access to system drives. If none are configured; select **Yes** when prompted.
3. Enter the server information, and click **apply**.

Server Settings [Home](#) > [Server Settings](#) > Server Setup Wizard

## Server Setup Wizard

### Server Information

Description: My Wizard

Company Name: HDS Identifies this site to your support provider.

Department: IP

**First Contact**

First Name: Santos

Last Name: Domingo

Phone Number: 408.777.7777

Email: email@customer.com

**Location**

Address 1: 300 High Plains Drive

Address 2:

City: San Jose

ZIP / Postal Code: 95134

State / Province: CA

Country: USA



**Note:** It is important that this information is accurate and complete as it is used in event notifications and Call-Home.

- Modify the administrative EVS name, cluster node, and EVS settings, as needed, leave Port set to **ag1**, and then click **apply**.



**Note:** It is not possible for the wizard to change the IP address being used to manage the server.

- Enter DNS server IP addresses, domain search order, WINS server, NIS domain, and name services ordering, as needed, and then click **apply**.

For CIFS (Windows) or NFS file serving functioning you need to specify the DNS servers and the domain search order.

- Specify the time zone, NTP server, time and date, and then click **apply**.
- Optional:* modify CIFS settings (register the EVS with a domain controller by entering its IP address), and then click **apply**.
- Specify the email server to which the server can send and relay event notification emails, check the `Enable the Support Profile` option, enter the contact's email address (*critical to receive proper system support*), and then click **apply**.
- Change the supervisor password (default: `supervisor`), and then click **apply**.
- Click **apply** to create a test file system, share, and export.
  - Check the `Create a NFS` option if this will be a NFS file server.
  - Check the `Create a CIFS` option if this will be a CIFS file server.
  - Check both options if this will be a mixed environment.

- After successfully navigating all pages of the wizard, a configuration summary is displayed, if restarting the file serving service and internal SMU are not required.

If a restart is required, the browser navigates to a wait page, and then reloads the home page.

- If the system uses a different subnet for management, set the default route by navigating to **Home** > **Network Configuration** > **IP Routes**.

## Configuring a system with an external SMU

### Initially configuring an external SMU

#### Before you begin

Allow the server up to 10 minutes after powering on to ensure it fully starts all processes.

There are several options for console access:

- Monitor and keyboard connection
- IPMI network access to console sessions (PROVIDED AS-IS; neither supported nor maintained by HNAS engineering or HDS Support.)
- Serial cable from PCs with DB-9 serial ports
- USB-to-serial cable from PCs with USB, but without DB-9 serial ports

The SMU 400 has two serial DB-9 ports, one on the rear, and one on the front. These two serial ports are *not* equivalent. Both ports can be used with direct serial cables or with USB-to-serial cables, and both ports can be used to access BIOS screens. However, only the rear port can be used for a Linux login session after boot.

DB-9 serial port	Identity in BIOS	Availability
Rear	COM1	Boot time and after boot
Front	COM2	Boot time only; blank after boot

#### Procedure

1. Either connect the KVM or attach a null-modem cable from your laptop to the serial port of the system management unit (SMU).

If using a serial connection, start a console session using your terminal emulation with the following settings:

- 115,200 b/s,
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control
- VT100 emulation

You may want to enable the logging feature in your terminal program to capture the session.

2. Log in as root and run `smu-config`.

## Result

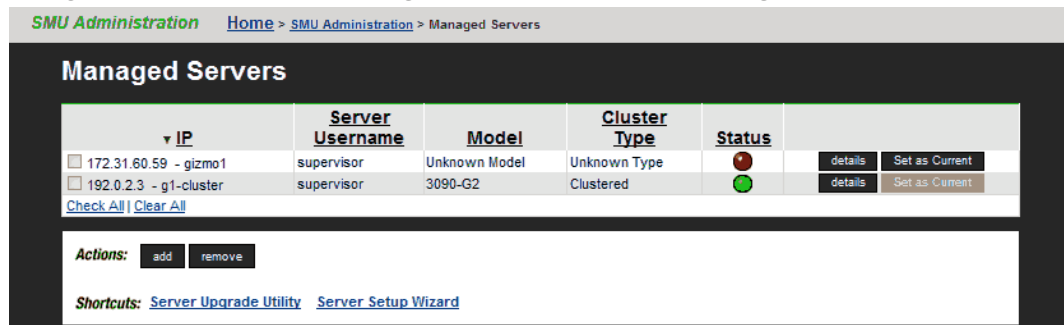
The SMU completes the configuration, and reboots.

## Selecting external NAS Manager-managed servers

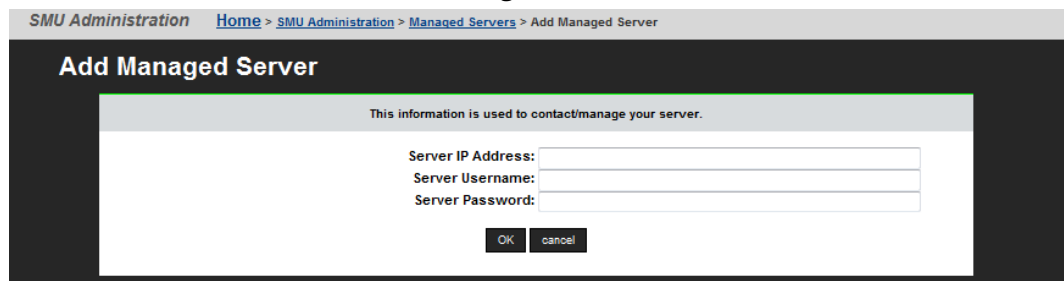
The external NAS Manager manages multiple servers or clusters and their associated storage subsystems. Use the Managed Servers page to add information about the server to be managed; specifically, the IP address and user name/password.

## Procedure

1. From a browser, enter the public IP address (Eth0) to launch Web Manager.
2. Navigate to **Home > NAS Manager Administration > Managed Servers**.



3. Click **add** to add the server to the Managed Servers list.



4. Enter the administrative EVS IP address for the server (user name and password are `supervisor` by default) and then click **OK**.

After adding a server, it displays in the Managed Servers list.

Status indicates the following states:

- *Green*: Operating normally
- *Amber*: Warning condition (server operational but action should be taken to maintain normal operation)
- *Red*: Critical condition (check the cables and hardware)

## Result

When the NAS Manager adds a managed server, the following actions occur:

- The NAS Manager Eth1 IP address is added to the server's list of NTP servers, and is configured as the server's primary SMTP server. If the server was already configured to use a mail server, this server will automatically become the backup SMTP server.
- The server's user name and password are preserved on the NAS Manager. This ensures that when selecting this server as the current managed server, or when connecting to the server's CLI using SSH, the server does not prompt for an additional authentication of its user name and password.

## Using the server setup wizard with a single-node configuration

### Procedure

1. From a browser, enter `http://Web_Manager_IP` to launch Web Manager.
2. Navigate to **Server Settings > Server Setup Wizard**.

When accessing the system for the first time, it might prompt you for the following:

- New licenses, contact Hitachi Vantara for assistance if none are present.
- Allow access to system drives, if none are configured; select **Yes** when prompted.

3. Enter the server information, and click **apply**.



**Note:** It is important that this information is accurate and complete as it is used in event notifications and Call-Home.

4. Modify the administrative EVS name, cluster node, and EVS settings, as needed, leave Port set to **ag1**, and then click **apply**.



**Note:** It is not possible for the wizard to change the IP address being used to manage the server.

5. Enter DNS server IP addresses, domain search order, WINS server, NIS domain, and name services ordering, as needed, and then click **apply**.

For CIFS (Windows) or NFS file serving functioning you need to specify the DNS servers and the domain search order.

6. Specify the time zone, NTP server, time and date, and then click **apply**.
7. *Optional:* modify CIFS settings (register the EVS with a domain controller), and then click **apply**.
8. Specify the email server to which the server can send and relay event notification emails, check the `Enable the Support Profile` option, enter the contact's email address (*critical to receive proper system support*), and then click **apply**.
9. Change the supervisor password (default: `supervisor`), and then click **apply**.

10. Click **apply** to create a test file system, share, and export.
  - Check the `Create a NFS` option if this will be a NFS file server.
  - Check the `Create a CIFS` option if this will be a CIFS file server.
  - Check both options if this will be a mixed environment.
11. After successfully navigating all pages of the wizard, a configuration summary is displayed, if restarting the file serving service and external SMU are not required.  
If a restart is required, the browser navigates to a wait page, and then reloads the home page.
12. If the system uses a different subnet for management, set the default route by navigating to **Home > Network Configuration > IP Routes**.

## Backing up configuration files

Before upgrading or making configurations changes to the system, it is highly recommended that you back up the configurations and save them in a safe, external location.

When using embedded SMU to backup configurations, the SMU configuration is included as a combined (server plus SMU) backup file. If an external SMU is used to manage the system, it is necessary to back up the server registry and SMU configuration independently, as they are archived separately.

## Backing up the server registry

### Procedure

1. From a browser, enter `http://Web_Manager_IP` to launch Web Manager.
2. Navigate to **Home > Server Settings > Configuration Backup & Restore**.
3. Click **backup**.
4. When prompted, save a copy of the registry to a safe location.

## Backing up the external SMU configuration

### Procedure

1. Navigate to **Home > SMU Administration > SMU Backup**.
2. Click **Backup**, choose a location (on your PC or workstation) to store/archive the configuration, and then click **OK**. A copy of the backup is stored on the SMU.

## Chapter 6: Accepting your system

The last phase ensures the customer is receiving system events to monitor ongoing system health and establish external connectivity to Call-Home service. This step informs the customer support and service organization to begin monitoring and assure support entitlement is accepted and activated.

### Checkpoint

#### Procedure

1. Navigate to **Home > Server Settings > Server Status > Cluster Configuration** to verify all components are functioning properly.

Server Settings [Home](#) > [Server Settings](#) > [Cluster Configuration](#) > Cluster Node

### Cluster Node Group1-node1

Cluster Node Name:  [rename](#)

Cluster Node ID: 1  
Status: Online

#### Network & Storage

File Systems: ● [OK](#)  
Ethernet Aggregations: ● [OK](#)  
Management Network: ● [OK](#)  
Fibre Channel Connections: ● [OK](#)

#### Cluster Communication

Cluster Interconnect: ● [OK](#)  
Management Network: ● [OK](#)  
Quorum Device: ● [OK](#)

#### Chassis

Power Supply Status: ● [OK](#)  
Temperature: ● [OK \(41 C\)](#)  
Chassis Disks: ● [OK \( Maximum Used: 9 % \)](#)  
Chassis Battery Status: ● [OK \(7.87V\)](#)  
Fan Speed: ● [OK \(4400 rpm\)](#)  
System Uptime: 8 days 21 hours 19 minutes 52 seconds

#### EVS

● [Group1-admin](#) ● [q1-evs3](#)  
● [q1-evs1](#) ● [LNAS](#)  
● [q1-evs2](#) ● [EVS1](#)

[remove](#)

Complete the following table as you verify each of the areas are installed correctly.

Problem Resolution	Area	Checked
File systems	Call support	



Problem Resolution	Area	Checked
Ethernet aggregations	Check cables	
Management network	Check cables	
Fibre Channel connections	Check cables	
Power supply status	Check power cables	
Temperature	Call support	
Disk RAID	Check cables and call support	
Chassis battery status	Call support	
Fan speed	Call support	
EVS	Call support	

2. Depending on your configuration:
  - If you modified the CIFS settings, and a test file system and share were created, connect to the share from a CIFS client on the same domain
  - If you selected the NFS option, mount the export from an NFS client.
3. Navigate to **Home > Server Settings > License Keys** to verify all services are enabled.
4. Navigate to **Home > Storage Management > System Drives** to verify the health of all the system drives (SD) presented to the server.
5. Navigate to **Home > Status & Monitoring > Self Test Event** and click **test** to send a test email to the profile you created.

6. If you receive the test event, congratulations, you are finished! Otherwise, verify your settings, and contact Hitachi Vantara for assistance if you are unable to pass this checkpoint.

Use the `trouble` command to perform a health check on the system. If you are unable to account for the event or resolve it, contact support.

## **Additional system verification tests**

This section includes any additional test that may be required when configuring a new system.

### **Verifying the SD superflush settings**

If you set the SD superflush settings during your install, you can verify the settings now. If you have not yet set the superflush settings, you can set them now.

Use the Hitachi Storage Navigator Modular 2 (SNM2) software to verify and enable SD superflush settings.

---

## Appendix A: Upgrading storage firmware

Upgrade the firmware on the storage arrays to take advantage of the changes in the newest version.

### Upgrading storage array firmware

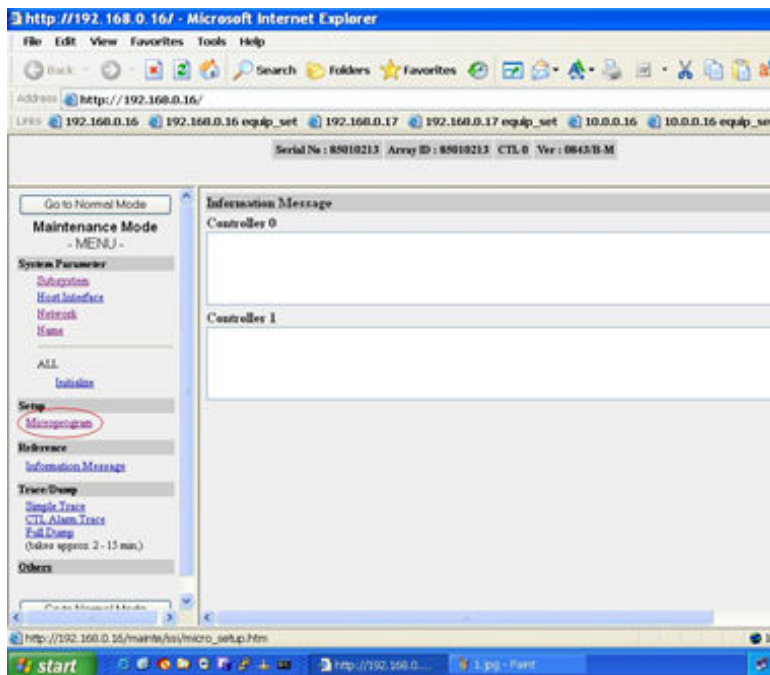
This task describes the procedure for upgrading the firmware on the storage arrays. The steps are performed in the system graphical user interface (GUI).

#### Procedure

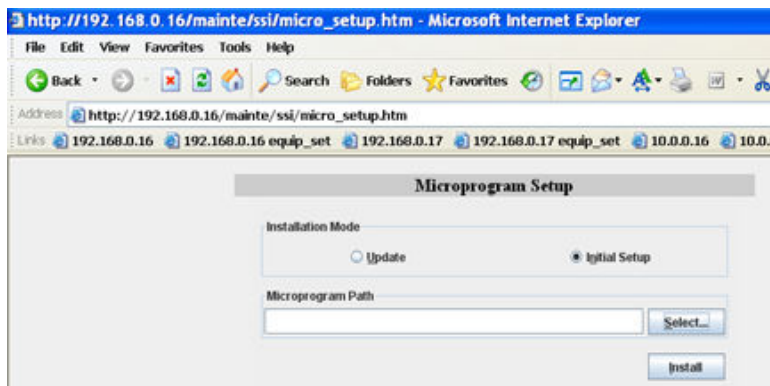
1. Open Internet Explorer and access the storage system using <http://10.0.0.16>  
The 10.0.0.x address is only accessible if you connect the LAN cable to the maintenance port.
2. Log in to the system with username `maintenance` and password `hosyu9500`, and click **OK**.



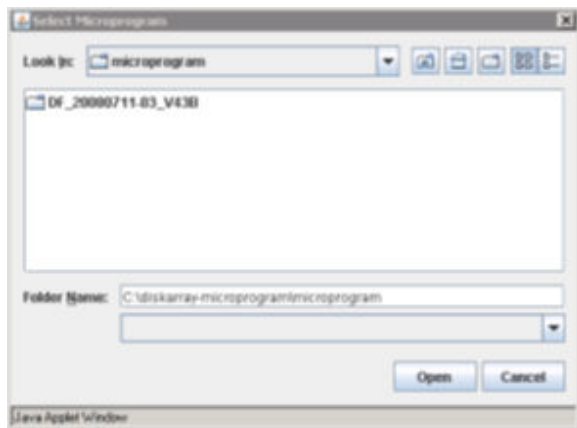
3. In the navigation pane, under Setup, click **Microprogram**.



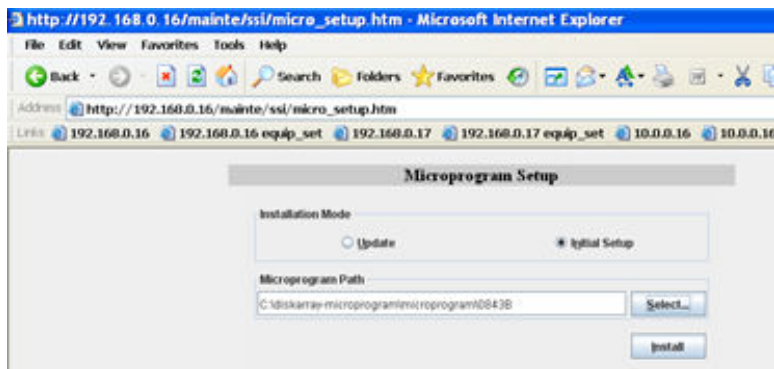
4. In the Microprograms Setup window, select **Initial Setup**, and then click **Select**.



5. In the Select Microprogram dialog, select the microprogram folder for the current GA release code, and click **Open**.



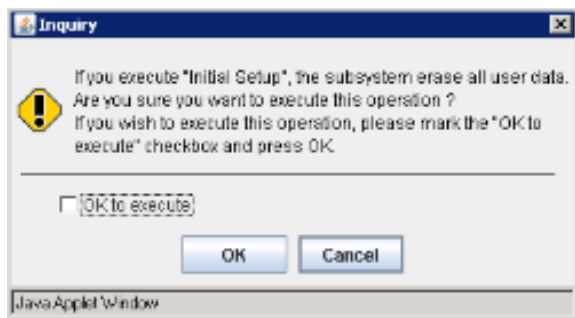
6. Back in the Microprograms Setup window, click **Install**.



- In the Inquiry dialog, click **OK**.



- In the Inquiry dialog, select the **OK to execute** checkbox, and then click **OK**.



- In the Information dialog, click **OK**.



- In the next window, click **To Maintenance Mode Top** to go back to the main menu.

## Appendix B: Configuring superflush settings

The superflush feature gives you the ability to force the write cache to hold a full stripe update, so you can turn random writes into a streaming write. Configure the superflush settings to maximize the workload of the storage array.

### Configuring the superflush settings

After creating volumes on the storage, configure the superflush settings.

#### Procedure

1. Use the SSH command in the SMU CLI to select the managing server.
2. Run the following command:

```
sd-set -w 0 -s 0
```

This command allows the system to dynamically set the superflush to the type of storage attached. Leaving `--width` and `--stripesize` at zero, which is the default value, causes the server to use the following values, which are always recommended, regardless of RAID level, media type, or the use of HDP or HDT:

- **Hitachi Module Storage** - `sd-set --width 1 --stripesize 256 ...`
- **Hitachi Enterprise Storage and Unified systems** - `sd-set --width 1 --stripesize 384 ...`

3. Run the following command to display the new settings:

```
sd-list -p
```

For example:

```
clus-1:$ sd-list -p
Device  Status  Alw  GiByte  Mirror  In span  S'flush
-----  -
0       OK      Yes  837     Pri     span1   ....
1       OK      Yes  837     Pri     span1   ....
2       OK      Yes  2793    Pri     span2   ....
3       OK      Yes  2793    Pri     span2   ....
```


Superflush is now enabled.


---

## Appendix C: Upgrading HNAS or HUS File Module server software

This section covers procedures for how you upgrade the operating system (OS) and firmware on a server. The procedures apply to both the Hitachi NAS Platform server and the Hitachi Unified Storage File Module server.

### Upgrading operating systems

 **Important:** When updating the NAS File OS, always refer to the release notes that are specific to the firmware you are installing for the most up-to-date upgrade instructions.

 **Remember:** Always capture system diagnostics *before* and *after* an upgrade. The diagnostics information will expedite support's ability to assist you if the system behaves unexpectedly.

### Upgrading the server software

#### Procedure

1. Open a supported browser and enter the SMU IP address to launch Web Manager.
2. Log in as `admin`.
3. Click **Home > Server Settings > Firmware Package Management**.
4. Ensure there are less than three existing packages (excluding any “patch” `.tar.gz` files). If there are more than three `.tar` files, remove the oldest files by selecting the check box next to its name and clicking **delete** in the Package View section.
5. In the Node View section, select **upload package**.
6. Select a managed server, and then click **OK**.
7. Click the **Browse** button, and then select the new software package. Ensure that the **Set as default package and Restart file serving** and **Reboot the server if necessary** options are enabled, click **Apply**, and then click **OK** when the confirmation is displayed to start the install.

The **Package Upload Progress page** is displayed. At the end of the process, the file server restarts. This takes approximately 20 minutes. After the page refreshes, “Upgrade completed successfully” is displayed.



**Note:** The status indicator might appear red and display the message `Server is not responding to management protocol. Connection refused.` If so, refresh the page to resolve the issue.

## Upgrading server firmware



**Note:** You must install each major release in order when upgrading a system from earlier releases. For example: If the system is running SU 7.x, you must first install 8.1.2312.09, or later, before upgrading to 10.x.

## Upgrading firmware on servers not usually managed by the SMU

You may need to upgrade the firmware on the server to the latest version.

The firmware upgrade process takes about 45 minutes. If you have two servers installed, you must repeat the process for both servers.

### Procedure

1. Log in to the SMU using the `admin` user.
2. Navigate to **Server Settings > Server Upgrade Selection**.
3. Choose the option **Not a Managed Server** and enter the credentials.

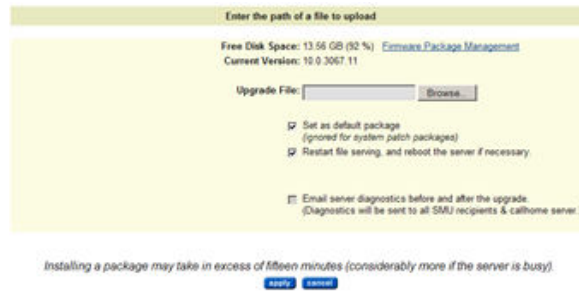
The credentials are the same as those used for your initial log-in to the servers, `supervisor` and `supervisor`. The IP address is the management address of the first server.

4. Browse to the location of the update file, the HNAS folder on the DVD.

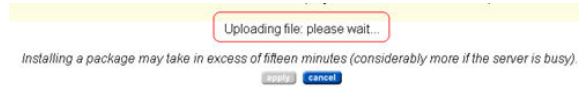


**Note:** The unit can only read \*.TAR files, not \*.ISO files.





5. Click **Apply** when the selection is made.



### Next steps

After the server firmware has been upgraded, you can run checks on the servers.

---

## Appendix D: Running the NAS-PRECONFIG script

Use the `nas-preconfig` script to automate the execution of common commands required for server configuration.

### Running the NAS-PRECONFIG script


This section describes the procedure for running the `nas-preconfig` script. This script automates some required configuration steps.

To run the `nas-preconfig` script, perform the following:

#### Procedure

1. At the Linux prompt, issue the command: `nas-preconfig`
2. Enter your network and server information using the information in the following table:

<b>nas-preconfig prompt</b>	<b>Sample value</b>
Admin Service Private (eth1) IP address	192.0.2.2
Admin Service Private (eth1) Netmask	255.255.255.0
Optional Admin Service Public (eth0) IP address	
Admin Service Public (eth0) Netmask	
Optional Physical Node (eth1) IP address	192.0.2.200
Physical Node (eth1) Netmask	255.255.255.0
Gateway	192.0.2.1
Domain name (without the host name)	CustDomain.com

nas-preconfig prompt	Sample value
Hostname (without the domain name)	hnas1   <b>Note:</b> The host (node) name may be up to a maximum of 15 characters. Spaces and special characters are not allowed in host/node names.

### Next steps

After running the script, you can proceed with the rest of the server configuration.

---

## Appendix E: Using a virtual SMU

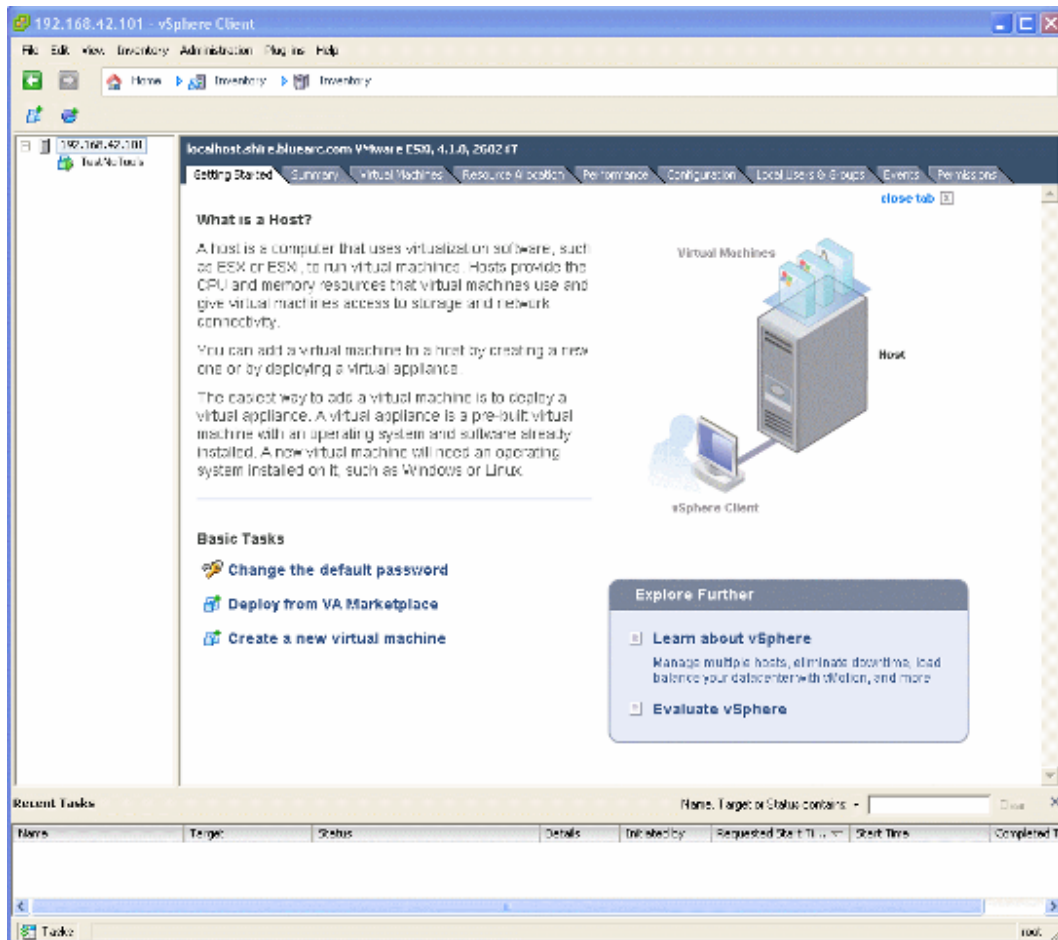
This section describes virtual SMUs and covers procedures for how you install, upgrade, and configure the software.

### About configuring a virtual SMU

Configuring a system to use a virtual SMU is nearly identical to the steps required for establishing an external SMU, with the exceptions that follow in this section.

Notes:

- A minimum amount of resources must be reserved for each VM. For details, see [Configuring VM resource allocations \(on page 134\)](#).
- Limited support for up to two managed servers/clusters.
- Open virtual appliance/application (OVA) is the standard distribution format for the virtual SMU, which is a compressed archive (tarball) of open virtualization format (OVF) files, including configuration and sparse disk image files.



## Installation requirements

Requirements include:

- Either of the following:
  - ESXi host hardware equivalent to an SMU300, or better. A dedicated server is highly recommended. Minimum specifications are:
    - 64-bit CPU with dual 2-GHz cores
    - 4GB RAM
    - 500 GB hard drive space
    - Two network adapters, one dedicated to the SMU private network
    - DVD drive
  - VMware enterprise-class software, installed and operational.

For details, see the documentation provided with your VMware solution, as the subject is beyond the scope of this document.
- IP addresses for access to the ESXi installation and for connecting to the SMU.  
Each SMU VM you deploy requires at least one IP address for management UI access.
- An ESXi installation CD.
- A configured OVA package.
- An SMU install image on CD.



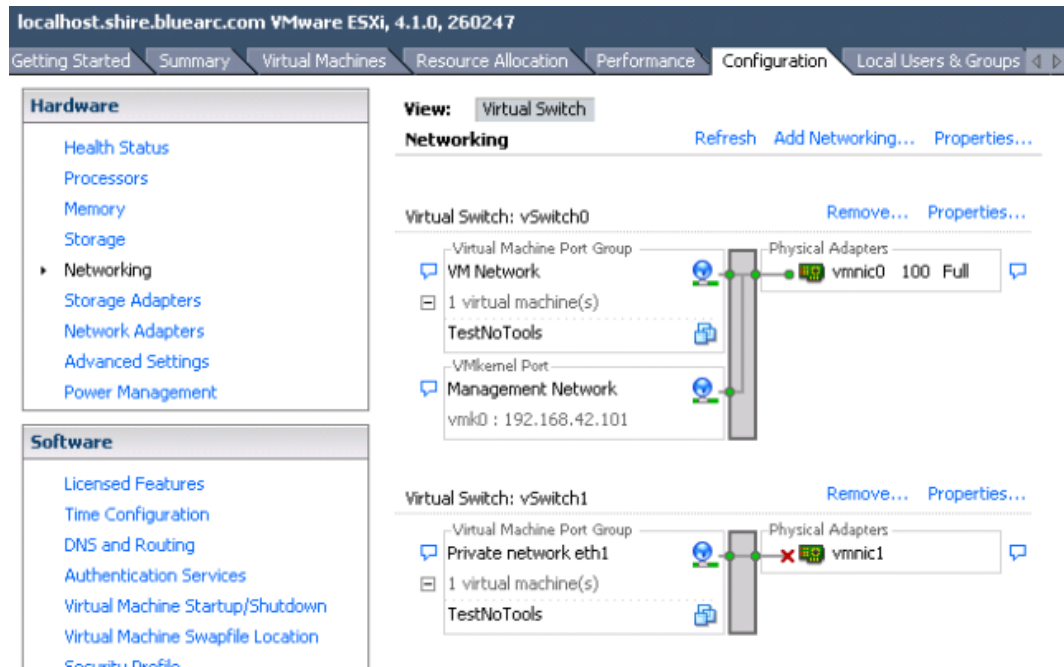
**Note:** If you have any questions, please contact your Support organization for assistance with these procedures.

## Configuring vSwitches

Configure a virtual switch (vSwitch) to avoid accidentally placing the private network for the SMU on the public NIC. The second network adaptor to be used for the private management LAN should reside in a separate vSwitch.

### Procedure

1. From the vSphere client, navigate to the server **Configuration** tab.
2. In the **Hardware** pane, select **Networking**.



3. Click **Add Networking** to launch the wizard.
4. Select the “Virtual Machine” default for the **Connection Type**, and then click **Next**.
5. Select **Create a virtual switch** and **vmnic1** (also known as eth1), and then click **Next**.
6. In the **Network Label** field, type `Private network eth1`.
7. Click **Next**, and then click **Finish**.

## Deploying CentOS SMU VMs

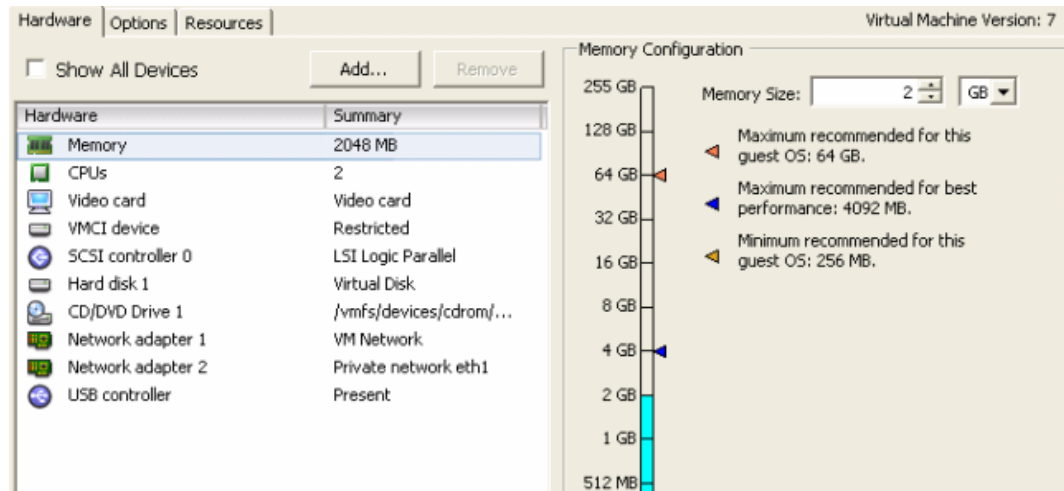
Deploy and map the CentOS eth1 to the physical eth1 to avoid placing the IP address on the public Ethernet port.

### Procedure

1. Navigate to **File > Deploy OVF Template** to launch the deployment wizard.
2. Click **Browse**, and then locate the `SMU-OS-2.1.ova` file.
3. Click **Next** to select the defaults, and then verify that the **Thick Provisioned Format** option is selected in the disk format dialog box. This option allocates disk space resources immediately to ensure it is available for an optimum running environment.
4. Click **Finish** to deploy the OVA.

Note that this process might take a few moments.

5. After the SMU OS OVA deploys, right-click the VM and select **Editing Settings** to open the **SMU OS Virtual Machine Properties** dialog box.



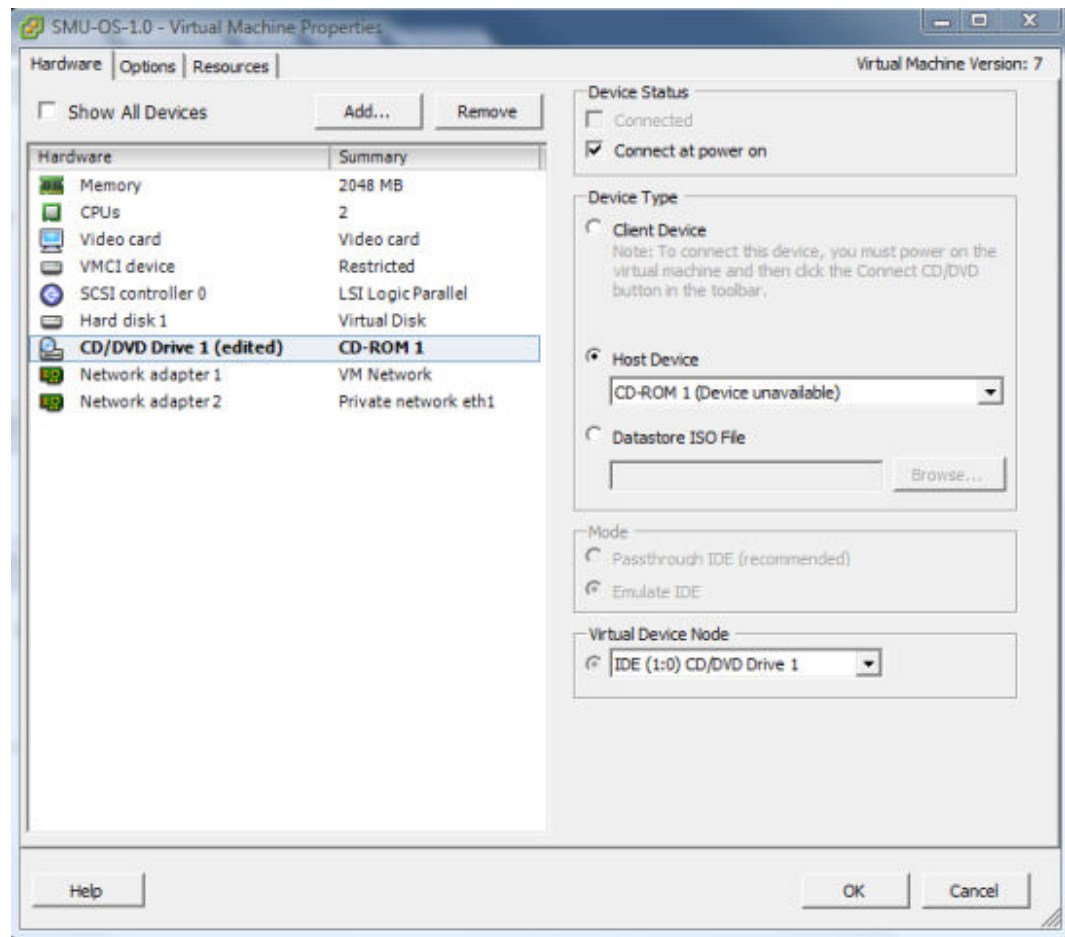
6. Under **Hardware**, select **Network adapter 2**.
7. From the **Network Connection** list, select **Private network eth1**, and then click **OK**.

## Installing SMU software in a VM

### Procedure

1. Insert the media into the DVD drive.
2. Right-click the virtual machine (VM) and select **Edit Settings**.
3. Under **Hardware**, select the CD/DVD drive.





4. Click **Host Device**, ensure that the **Connect at power on** check box is selected, and then click **OK**.
5. Click the green play button to power on the VM, and then click the **Console** tab.



6. Log in as root.



**Note:** Press **Ctrl+Alt** whenever you want to release focus from the console and return to other windows.

7. Enter `mount /media/cdrecorder`.
8. Enter `/media/cdrecorder/autorun` to start the installation. The installation takes a few minutes to complete.

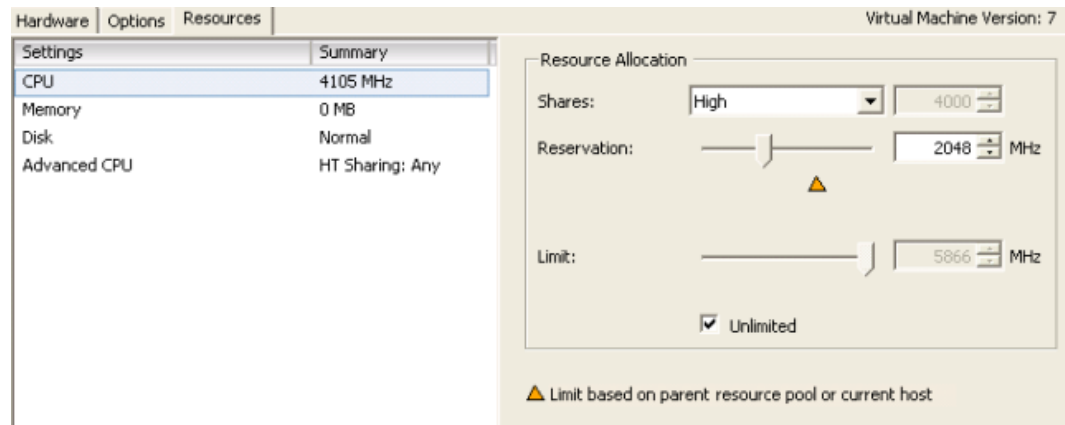
## Configuring VM resource allocations

### Before you begin

A minimum amount of resources must be reserved for each VM. After configuring the reservations, VMware allows the VM to start only if the resources can be guaranteed. The *VMware Resource Management Guide* calls this mechanism *admission control*.

### Procedure

1. In the **Virtual Machine Properties** dialog box, click the **Resources** tab.



2. Under **Settings**, select **CPU**.
3. From the **Shares** list, select **High**, and then set **Reservation** to **1500 MHz**.
4. Under **Settings**, select **Memory**.
5. From the **Shares** list, select **High**, and then set **Reservation** to **2048 MB**.
6. Under **Settings**, select **Disk**.
7. From the **Shares** list, select **High**, and then click **OK**.

## Installing VMware tools

VMware tools provide useful options when managing the virtual SMU. For instance, without the tools, the Power Off option is equivalent to removing the power cords from the outlet. However, with the tools installed, Power Off provides a healthier shutdown. As an alternative, you can enter the `shutdown -h` command from a console session, or from Web Manager, navigate to Home > SMU Administration > SMU Shutdown / Restart, and then click shut down.



**Note:** It is necessary to reinstall the VMware tools every time the SMU software is updated.

### Procedure

1. Power on the VM.
2. Right-click the VM, and then navigate to **Guest > Install/Upgrade VMware Tools**.

3. When the **VMware Tools** installation dialog box opens, enter `mount /media/cdrecorder`  
The volume mounts as read-only.
4. Copy the distribution file to `/tmp`, and expand it. For example, enter `cd /tmp; tar xvfz VMwareTools.8.3.2-257589.tar.gz`
5. Enter `cd /tmp/vmware-tools-distrib; ./vmware-install.pl` to run the installer.  
Follow the prompts, confirming the default settings. Run any commands, if instructed to do so.
6. Reboot, and then review the installation on the **VM Summary** page. **VMware Tools** should display "OK" in the **General** pane.

## Upgrading the OS for a virtual SMU

Use this alternate virtual machine (VM) upgrade procedure if you want to upgrade the operating system (OS) on an embedded or virtual SMU.



**Note:** This section applies only to virtual SMUs. It does *not* apply to external SMUs. For information on external SMUs, see [Upgrading the SMU OS \(on page 136\)](#).

To perform an alternate VM upgrade:

### Procedure

1. Back up the SMU configuration, and power down the VM.
2. Deploy a second open virtual appliance (OVA), and do a fresh installation of the new SMU version.
3. Restore the SMU configuration from the original.
4. Proceed to upgrading any other SMUs needed.  
You can switch between versions by shutting down one VM, and then powering up the other.

---

## Appendix F: Upgrading an external SMU

This section covers procedures for how you upgrade the operating system (OS) and system management unit (SMU) software for an external SMU.

### About upgrading an external SMU

You can upgrade the software for an external System Management Unit (SMU), but you cannot upgrade the external SMU hardware.

The SMU installation and upgrade methods include:

- *Fresh installation:* Erases and partitions the entire hard drive; performs a full OS installation followed by the SMU software.



**Note:** New SMUs are preinstalled with the latest OS. It may be necessary to perform a fresh installation to downgrade a replacement SMU so that the unit is compatible with the system in which its being installed. For instance: An SMU running 10.0 must have a fresh OS installed to downgrade it to NAS File OS 8.x.

- *Alternate partition upgrade:* Installs the SMU OS and software on the second partition of the SMU. This allows for downgrading the SMU by booting into the older installation.
- *In-place upgrade:* SMU point builds can be installed over a previous installation (for instance, within the active partition) without having to reinstall the OS. However, this means the SMU cannot be downgraded to its previous version.

### Upgrading the SMU OS

Use this OS upgrade procedure only when you have an external SMU.

This procedure does not apply to embedded or virtual SMUs.

CentOS 6.x is only supported on SMU200 and later models.

#### Procedure

1. Either connect the KVM or attach a null-modem cable from your laptop to the serial port of the SMU.

If you are using a serial connection, start a console session using your terminal emulation with the following settings:

- 115,200 b/s
- 8 data bits (bps)
- 1 stop bit
- No parity
- VT100 emulation

You may want to enable the logging feature in your terminal program to capture the session.

2. Log in as `root`.
3. Enter `smu-remove-alt-partition`.

This checks for an SMU installation on the alternate partition. If one is not found, the command reports the error and exits, which is the expected behavior. In essence, this prepares the alternate partition for an upgrade.

If another installation is found, you are prompted to confirm the deletion. Ignore any IO error messages that are displayed.

```
***** WARNING *****
This action will irreversibly delete
SMU 10.1.3070 on hda3
from the SMU.
The SMU will then have space available to set up a new
installation in
the freed space.
Continue? [y/n]
```

4. Boot the SMU with the installation OS DVD.

```
Welcome to SMU OS Installation
(CentOS 6.2)
Type the option and press <ENTER> to begin installing.

Clean installation, destroying all data in the hard drive:
clean-kvm - Clean SMU OS install (erases entire HD) using KVM.
clean-serial - Clean SMU OS install (erases entire HD) using
serial
console.

For a second installation (only one installation already
present):
second-kvm - Second SMU OS install using KVM.
second-serial - Second SMU OS install using serial console.

For a virtual machine installation (only one partition):
virtual-smu - Virtual SMU install using KVM.

- To boot the existing kernel press <ENTER>
- Use the function keys listed below for more information.

[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot:
```

5. Enter the appropriate option based on the type of installation required:

- a. *Fresh installation:* Choose fresh installation when you want to completely wipe out the SMU hard drive and start fresh. This means that it will not be possible to downgrade to the alternate partition. All SMU configuration (if present) will be destroyed. If this is a fresh install, not an SMU upgrade, this is the proper selection. Based on your connection to the SMU, enter `clean-kvm` or `clean-serial`.



**Important:** This step destroys the previously installed SMU software; ensure you have backed up the SMU before proceeding.

The installation takes approximately 12 minutes from DVD.

- b. *Alternate partition installation:* Choose alternate partition installation if you are upgrading an SMU. This option preserves the existing SMU configuration and allows the SMU to be downgraded. This option is only valid for SMU upgrades, not fresh installs. Based on your connection to the SMU, enter `second-kvm` or `second-serial`.

The installation takes approximately 12 minutes from DVD.

6. Click `Reboot` when the installation finishes, and remove the installation medium from the SMU drive.

## Upgrading the NAS Manager software

### Before you begin

If you are upgrading from NAS File OS 7.x, you must upgrade to CentOS 4.8.1 and then NAS Manager 8.1.2312.09 before installing NAS File OS 10.x. This is only necessary with external NAS Managers, and not embedded NAS Manager configurations.



**Note:** During the upgrade, NAS Manager processes are not running, which results in it temporarily not collecting performance statistics, running replication jobs, and so forth.

### Procedure

1. Insert the NAS Manager Software CD into the DVD drive.
2. Log in as `root`.
3. Enter `mount /media/cdrecorder`, and then `/media/cdrecorder/autorun`.



**Note:** On the NAS Manager 200, the path is `/media/cdrom`, instead of `/media/cdrecorder`.

If you are installing from an ISO image (for example, `SMUsetup_uplands_3067_hds.iso`) versus a physical DVD, use `scp` to copy `SMUsetup_uplands_3067_hds.iso` to `/tmp` on the NAS Manager, and then issue the following commands:

```
su - root
cd /tmp
```

```
mount -o loop /tmp/SMUsetup_uplands_3067_hds.iso /media/cdrom  
/media/cdrom/autorun
```

4. If a fresh install was performed, log in as `root`, and run the `smu-config` script.

This step is not necessary for alt-partition upgrades.

For details about running the `smu-config` script, see [Running the SMU-CONFIG script \(on page 140\)](#).

After the Upgrading the NAS Manager software has restarted, the Upgrading the NAS Manager software upgrade is complete.

5. If a fresh install was performed, restore the Upgrading the NAS Manager software configuration from your most recent backup file.

This step is not necessary for alt-partition upgrades.

The Upgrading the NAS Manager software reboots.

---

## Appendix G: Running the SMU-CONFIG script

Use the `smu-config` script to automate the execution of common commands required for system management unit (SMU) configuration.

### Running the SMU-CONFIG script

#### Before you begin

- Allow the server up to 10 minutes after powering on to ensure that it fully starts all processes.
- Make sure you have the information in the following table available to complete the `smu-config` setup. Obtain the customer setting from the Account Team based upon the pre-engagement checklist, SAD, and/or the PTC.

Setting	Customer Setting
Root password	Provided by customer
Manager password	Provided by customer
SMU public IPv4 address (eth0)	Provided by customer
SMU public IPv4 netmask (eth0)	Provided by customer
IPv4 gateway	Provided by customer
Standby SMU	n (if primary SMU)
SMU private IPv4 address (eth1)	192.0.2.1
Configure IPv6 address	n
Use stateless auto-configuration (SLAAC)	n
SMU public IPv6 address (eth0)	Provided by customer
IPv6 gateway	Provided by customer
SMU domain (fully qualified)	Provided by customer
SMU host name (without the domain name)	Provided by customer



## Procedure

1. Either make a serial connection or a KVM connection to the SMU.
  - For a KVM connection, connect a monitor, keyboard, and mouse to the appropriate ports on the back of the SMU .
  - For a serial connection, start a console session using your terminal emulation program. Use the following settings:
    - 115,200 b/s
    - 8 data bits
    - 1 stop bit
    - No parity
    - No hardware control flow
    - VT100 emulation

You may want to enable the logging feature in your terminal program to capture the session.

2. Press the red button on the front of the SMU to power on the unit.
3. Log in as `root`.
4. Run the command `smu-config`
5. Enter the appropriate configuration information.



**Note:** If an item is incorrect, the script can be re-run until you save it.

6. Review all the settings you have made, and then enter `Y` if they are correct.

The following shows an example configuration:

```
[root@group5-smu manager]# smu-config
***** WARNING *****
This script will configure the SMU's network settings and
system passwords.
If the SMU is used as a Quorum Device and the SMU IP address
is changed, the cluster(s) using it will be left in a
Degraded State until the SMU can notify them of the changes.
Any custom SSL certificates will need to be re-applied.
The script will interrupt existing ssh and browser connections,
and be followed by an immediate reboot of the SMU.

Proceed with changing the SMU settings? [y/n]: y

Configures the Management Unit's system passwords.
You will need to provide:
- Management Unit's root password, and
- manager account password

Changing password for user root.
New password: xxxxxxxx
BAD PASSWORD: it is based on a dictionary word
Retype new password: xxxxxx
passwd: all authentication tokens updated successfully.

Changing password for user manager.
New password: xxxxxx
BAD PASSWORD: it is based on a dictionary word
Retype new password: xxxxxx
passwd: all authentication tokens updated successfully.

Configure the management unit's basic networking.
- IPv4 addresses
- IPv4 netmask
- IPv4 gateway
- Enable IPv6
- Enable stateless IPv6 address configuration
- IPv6 address for eth0 in CIDR format
- IPv6 address gateway
- domain name
- host name

Any further configuration may be carried out via a web browser.

An IPv4 address, and optionally an IPv6 address, are required
for the SMU public (eth0) interface.
Enter the SMU public IPv4 address (eth0) [172.31.60.80]

Enter the IPv4 netmask [255.255.255.0]

Enter the IPv4 gateway [172.31.60.254]

Is this a standby SMU? [y/n]
n
Recommended eth1 IP for non-standby SMUs is 192.0.2.1.
The netmask is 255.255.255.0.
Enter the SMU private IP address (eth1) [192.0.2.1]

Configure IPv6 address? [y/n] [yes]
```

```
y
Use stateless autoconfiguration (SLAAC)? [y/n] [yes]
y
Enter the SMU public (eth0) IPv6 address. Use CIDR format
or "none" [face::3/64]

Enter the SMU IPv6 gateway address or "none". [face::254]

Enter the Domain name for the management unit (without the
host name) [example.com]

Enter the Host name for the management unit (without the domain
name)
[smu]

SMU public IP (eth0) = 172.31.60.80
Netmask = 255.255.255.0
Gateway = 172.31.60.254
SMU private IPv4 (eth1) = 192.0.2.1
Enable IPv6 = yes
IPv6 stateless auto-configuration = yes
SMU static IPv6 (eth0) = face::3/64
SMU static IPv6 gateway = face::254
Domain = example.com
Unit hostname = smu
Are the above settings correct? [y/n] y
```

When you save the configuration, the script sets up the network interfaces and default properties, and then the SMU reboots.

---

## Appendix H: Adding nodes to an N-way cluster (three-plus nodes)

The system design allows you to create an N-way cluster. An N-way cluster is a cluster that contains three or more nodes. You can create an N-way cluster or upgrade a two-node cluster to an N-way cluster. This section also includes the configuration of the 10 GbE cluster interconnect switches that are used to connect the nodes.

### Maximum number of nodes supported

The maximum number of nodes in a cluster is controlled by several factors, including hardware model of the server nodes, HNAS server firmware version, and maximum number of cluster nodes allowed by the cluster licenses.



**Note:**

The maximum licensed number of nodes in a cluster will never exceed the maximum number of nodes supported by the hardware and software of the nodes making up the cluster.

For each HNAS server model, the maximum supported number of nodes allowed in a single cluster is:

HNAS server model being used as nodes	Maximum number of nodes supported
3080	2
3090	4
4040	2
4060	2
4080	4
4100	8



**Note:**

All nodes in a cluster must be of the same model of server.

## Adding nodes to an N-way cluster

This section provides information on how to create or upgrade a two-node cluster to an N-way cluster. An N-way cluster has three or more nodes. A server becomes a node when it is added to a cluster.

### Before you begin

Before you add any nodes to an N-way cluster, make certain of the following:

- The server is running the same NAS File OS release.
- You have the following available:
  - A laptop or other client system to connect to the server serial console and management network ports, and necessary cables.
  - License keys that enable the appropriate number of cluster nodes.
  - Wiring diagrams for the cluster interconnect.
  - Plan for the intended cluster node IP addresses to use for the nodes. These are the physical IP addresses to be used for the cluster communication. The addresses will reside on the private management network.

Refer to the configuration guide for the switch, or contact customer support for more information.

### Procedure

1. Mount the new servers and 10 GbE intercluster switches into the intended rack locations.
2. Connect the cables for the intercluster switches.  
Do *not* connect the cables for the servers at this time.
3. Configure the intercluster switches.
4. Install the license keys to enable the new nodes.
5. Disconnect the C1 port connections on both existing servers, and connect those ports to the first switch.
6. Confirm that the links to the first switch are up before disconnecting the C2 port connections.
7. Disconnect the C2 port connections on both existing servers.
8. Connect the C1 port on the third node to the first switch.
9. Use a serial cable to connect your laptop to the new server, and connect with a terminal emulation program.
10. Join the new node to the cluster in the software.  
See the *Server and Cluster Administration Guide* for details.
11. Connect C2 ports on all nodes to the second switch.
12. Additional nodes may now be added.

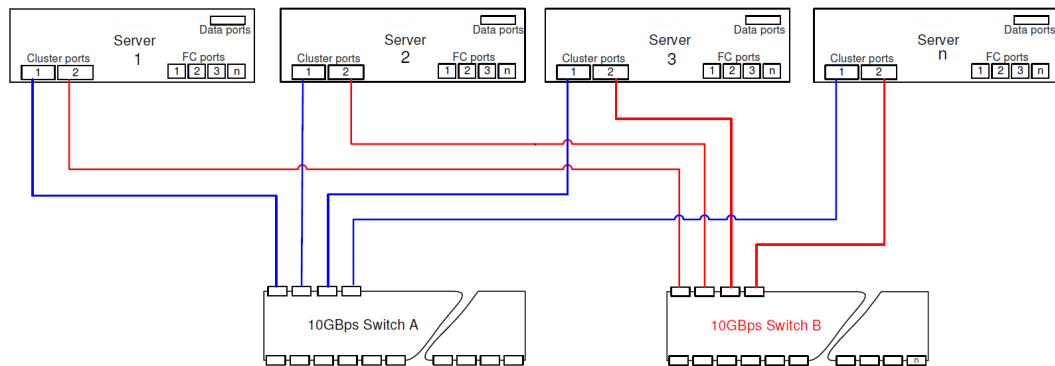
For each node you add, ensure that only the C1 port is connected until the node has completely joined the cluster, and then you can connect the C2 port.

13. After the cluster seems to be properly installed, issue the command: `cluster-show -a`

This command ensures that the cluster health is robust and that no links or interfaces are degraded or failed.

## Cluster cable configurations

The cabling configurations provided in this section are only for reference. See the documentation wallet that shipped with your system for its specific configuration, or contact Hitachi Data Systems Support Center for assistance.



**Figure 45** Cabling servers to 10 GbE switches



**Note:** See *SX515176-02* for complete details.

**Hitachi Vantara**



Corporate Headquarters  
2535 Augustine Drive  
Santa Clara, CA 95054 USA  
[HitachiVantara.com](http://HitachiVantara.com) | [community.HitachiVantara.com](http://community.HitachiVantara.com)

Contact Information  
USA: 1-800-446-0744  
Global: 1-858-547-4526  
[HitachiVantara.com/contact](http://HitachiVantara.com/contact)