

Hitachi NAS Platform and Hitachi Unified Storage Series 4000 Hardware Reference

Release 14.2

© 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.

AI/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, Edge, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft corporate logo, the Microsoft Edge 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

Preface	7
Related Documentation.....	7
Accessing product documentation.....	10
Getting help.....	10
Comments.....	10
Chapter 1: About this manual.....	12
Applicable products.....	12
Audience.....	13
Conventions.....	13
Chapter 2: Safety information.....	18
Electrostatic discharge precautions.....	18
Safety and handling precautions.....	18
Electrical precautions.....	19
Battery precautions.....	19
Data protection precautions.....	20
Chapter 3: Mandatory regulations.....	22
International standards.....	22
Federal Communications Commission (FCC).....	23
European Union (EU) Statement.....	23
Canadian Department of Communication Compliance Statement.....	24
Avis de conformité aux normes du ministère des Communications du Canada.....	24
Radio Protection for Germany.....	24
Food and Drug Administration (FDA).....	24
Chinese RoHS Compliance Statement.....	25
Taiwan RoHS Compliance Statement.....	25
South Africa: ICASA.....	26
Chapter 4: Hitachi NAS Platform server components.....	28
System components.....	28
Server components.....	30
Server specifications.....	31
Ventilation.....	34

Server front panel.....	34
LED status indicators.....	36
NVRAM backup battery pack.....	39
Hard disk drives.....	42
Fans.....	43
Server rear panel - model 4040	45
Rear panel server LED and button locations.....	46
GE Ethernet network ports	47
Rear panel LED state descriptions	48
10/100 private Ethernet ports.....	49
Server rear panel - models 4060, 4080, and 4100.....	50
Rear panel server LED and button locations.....	52
Rear panel LED state descriptions.....	52
10 Gigabit Ethernet cluster interconnect ports.....	54
10 Gigabit Ethernet cluster interconnect ports.....	54
Server rear panel - all models.....	55
Power button (PWR).....	55
Reset button (RST).....	56
Fibre channel storage ports.....	56
10 Gigabit Ethernet customer data network ports.....	57
Power supply units	58
Ethernet management ports 0 and 1.....	60
Serial port	60
USB ports.....	60
Management interfaces.....	61
RS-232 serial management port	62
10/100/1000 Ethernet management ports.....	63
Ethernet cables	63
Chapter 5: Replacing server components.....	65
Field-replaceable units.....	65
Hot-swappable components.....	65
Removing and replacing the front bezel.....	66
Bezel removal.....	66
Bezel replacement.....	67
Replacing a fan.....	67
Replacing the NVRAM backup battery pack.....	68
Checking battery pack status.....	69
Identifying a cluster node that requires battery replacement	70
Replacing the NVRAM battery module.....	70
Collecting system backups and diagnostics.....	72
Resetting the battery age and restarting the chassis monitor	73

Collecting a final diagnostic	74
Recovering or replacing a hard disk.....	75
Replacing a power supply unit.....	76
Chapter 6: Rebooting, shutting down, and powering off.....	78
Rebooting or shutting down a server.....	78
Rebooting or shutting down a server or cluster.....	79
Restarting an unresponsive server.....	80
Powering down the server.....	82
Powering on the server or cluster.....	82
Recovering from power stand-by.....	83
Appendix A: Server replacement procedures.....	84
Replacement procedure overview.....	84
Server replacement requirements.....	84
Swapping components.....	85
Model selection.....	85
MAC ID and license keys.....	85
Previous backups.....	86
Upgrades.....	86
Manually installing an embedded SMU (if necessary)	86
Replacing a single server with an embedded SMU.....	87
Obtaining backups, diagnostics, firmware levels, and license keys.....	87
Shutting down the server you are replacing.....	89
Configuring the replacement server.....	93
Finalizing and verifying the replacement server configuration.....	94
Replacing a single server with an external SMU.....	96
Obtaining backups, diagnostics, firmware levels, and license keys.....	97
Shutting down the server you are replacing.....	98
Configuring the replacement server.....	102
Finalizing and verifying the replacement server configuration.....	103
Replacing a node within a cluster.....	105
Capturing information from the existing node.....	106
Preparing the new node.....	106
Preparing the old node for removal.....	107
Installing the new node.....	107
Finalizing and verifying the server configuration.....	108
Replacing all servers within a cluster.....	111
Obtaining backups, diagnostics, firmware levels, and license keys.....	111
Shutting down the servers you are replacing.....	113
Configuring the replacement servers.....	116
Finalizing and verifying the system configuration.....	117

Appendix B: Accessing the server CLI.....	119
Accessing the command line interface.....	119
Using the serial (console) port	119
Using an SSH connection.....	120
Appendix C: Parts list for Series 4000 servers.....	121

Preface

This manual provides an overview of the Hitachi NAS Platform and the Hitachi Unified Storage File Module hardware. The manual explains how to install and configure the hardware and software, and how to replace faulty components.

The following server models are covered: 4040, 4060, 4080, and 4100

For assistance with storage arrays connected to the server, refer to the *Storage Subsystem Administration Guide*.

Related Documentation

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

Command Line References

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

- *NAS Module Server Command Line Reference*
- *Command Line Reference for models 4060, 4080, and 4100*
- *Command Line Reference for models 3080, 3090 and 4040*
- *Command Line Reference for models 5200 and 5300*

Administration Guides

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



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

Hardware References

- *Hitachi NAS Platform 3080 and 3090 G2 Hardware Reference* (MK-92HNAS017) — 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 Series 4000 Hardware Reference* (MK-92HNAS030)—Provides an overview of the Hitachi NAS Platform Series 4000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components
- *Hitachi NAS 5000 Series Hardware Reference* MK-92HNAS089—Provides an overview of the Hitachi NAS Platform Series 5000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.
- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.

Best Practices

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

- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.
- *NAS Platform ICC with Cisco Nexus Reference Guide* (MK-92HNAS085)—This document describes how to configure Cisco Nexus series switches for use as an ICC (intra-cluster communication) switch.
- *File System Snapshots Operational Best Practice* (MK-92HNAS068)—This document provides operational guidance on file system snapshots.
- *Virtual Infrastructure Integrator for Hitachi Storage Platforms Operational Best Practice* (MK-92HNAS069)—This document provides operational guidance on Hitachi Virtual Infrastructure Integrator for the HNAS platform.
- *Hitachi NAS Platform Replication Best Practices Guide* (MK-92HNAS070)—This document details the best practices for configuring and using HNAS Replication and related features.
- *Hitachi NAS Platform to Hitachi Virtual Storage Platform Unified Gx00 Models Migration Guide* (MK-92HNAS075)—This best practice guide describes how to perform a data-in-place migration of the Hitachi NAS Platform and Virtual Storage Platform (VSP) Gx00 File solution to the VSP Gx00 platform.

Accessing product documentation

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

Getting help

The [Hitachi Vantara Support Website](https://support.hitachivantara.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: 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, register, and complete your profile.

Comments

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

Thank you!

Chapter 1: About this manual

This manual provides an overview of the NAS Platform and the Hitachi Unified Storage File Module hardware. The manual explains how to install and configure the hardware and software, and how to replace faulty components.

The following server models are covered: 4040, 4060, 4080, and 4100.

For assistance with storage arrays connected to the server, refer to the *Storage Subsystem Administration Guide*.

Applicable products

Applicable products include:

- Hitachi NAS Platform, which includes the hardware and software for:
 - Hitachi NAS Platform 4040
 - Hitachi NAS Platform 4060
 - Hitachi NAS Platform 4080
 - Hitachi NAS Platform 4100
- Hitachi Unified Storage File Module (all models)
- Hitachi Virtual Storage Platform G1000

Server Series	Server Model	Currently Supported Offerings	Discontinued, but Still Supported
▪ NAS Platform Series 4000 ▪ NAS Platform Series 5000	For the NAS Platform Series 4000: ▪ 4060 ▪ 4080 ▪ 4100 For the NAS Platform	VSP G200, VSP G350, VSP G370, VSP G400, VSP G600, VSP G700, VSP G800, VSP G900, VSP G1000, VSP G1500, VSP F1500, VSP F200, VSP F350, VSP F370, VSP F400, VSP F600, VSP F700, VSP F800, VSP F900, VSP 5100, VSP 5200,	HUS VM, HUS 110, HUS 130, HUS 150

Server Series	Server Model	Currently Supported Offerings	Discontinued, but Still Supported
	Series 5000: 5200 5300	VSP 5500, VSP 5600, VSP 5100H, VSP 5200H, VSP 5500H, VSP 5600H, VSP E590, VSP E790, VSP E590H, VSP E790H, and VSP E990	
NAS Platform Series 4000	4040	VSP G200, VSP G400, VSP G600, VSP G800, VSP G1000, VSP G1500, VSP F1500, VSP F200, VSP F400, VSP F600, VSP F800	HUS VM, HUS 110, HUS 130, HUS 150
NAS Platform Series 3000	3080 and 3090	VSP G200, VSP G400, VSP G600, VSP G800, VSP G1000, VSP G1500, VSP F1500, VSP F200, VSP F400, VSP F600, VSP F800	HUS VM, HUS 110, HUS 130, HUS 150

Audience

This guide provides reference information for anyone who repairs the system hardware and has a good working knowledge of computer systems and part replacement.

Conventions

The following conventions are used throughout this document:

Convention	Meaning
Command	This fixed-space font denotes literal items such as commands, files, routines, path names, signals, messages, and programming language structures.

Convention	Meaning
<i>variable</i>	The italic typeface denotes variable entries and words or concepts being defined. Italic typeface is also used for book titles.
<code>user input</code>	This bold fixed-space font denotes literal items that the user enters in interactive sessions. Output is shown in nonbold, fixed-space font.
[and]	Brackets enclose optional portions of a command or directive line.
...	Ellipses indicate that a preceding element can be repeated.
GUI element	This font denotes the names of graphical user interface (GUI) elements such as windows, screens, dialog boxes, menus, toolbars, icons, buttons, boxes, fields, and lists.

The following types of icons are used throughout this manual. It is recommended that these icons and messages are read and clearly understood before proceeding:

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Før du starter (DANSK)

Følgende ikoner anvendes i hele guiden til at anføre sikkerhedsrisici. Det anbefales, at du læser og sætter dig ind i, og har forstået alle procedurer, der er markeret med disse ikoner, inden du fortsætter.

Bemærk: “Bemærk” indikerer informationer, som skal bemærkes.

FORSIGTIG: “Forsigtig” angiver en mulig risiko for beskadigelse af data eller udstyr. Det anbefales, at du ikke fortsætter længere end det afsnit, der er mærket med dette ord, før du helt har sat dig ind i og forstået proceduren.

ADVARSEL: “Advarsel” angiver en mulig risiko for den personlige sikkerhed.

Vorbereitung (DEUTSCH)

Die folgenden Symbole werden in diesem Handbuch zur Anzeige von Sicherheitshinweisen verwendet. Lesen Sie die so gekennzeichneten Informationen durch, um die erforderlichen Maßnahmen zu ergreifen.

Anmerkung: Mit einer Anmerkung wird auf Informationen verwiesen, die Sie beachten sollten.

VORSICHT: Das Wort "Vorsicht" weist auf mögliche Schäden für Daten oder Ihre Ausrüstung hin. Sie sollten erst dann fortfahren, wenn Sie die durch dieses Wort gekennzeichneten Informationen gelesen und verstanden haben.

WARNUNG: Mit einer Warnung wird auf mögliche Gefahren für Ihre persönliche Sicherheit verwiesen.

Antes de comenzar (ESPAÑOL)

Los siguientes iconos se utilizan a lo largo de la guía con fines de seguridad. Se le aconseja leer, y entender en su totalidad, cualquier procedimiento marcado con estos iconos antes de proceder.

Sugerencia: Una sugerencia indica información adicional que puede serle de utilidad en la finalización de una tarea.

PRECAUCIÓN: Una precaución indica la posibilidad de daños a los datos o equipo. Se le aconseja no continuar más allá de una sección marcada con este mensaje, a menos que entienda el procedimiento por completo.

ADVERTENCIA: Una advertencia indica la posibilidad de un riesgo a la seguridad personal.

Avant de commencer (FRANÇAIS)

Les icônes ci-dessous sont utilisées dans le manuel pour mettre en évidence des procédures de sécurité. Nous vous invitons à les lire et à bien comprendre toutes les procédures signalées par ces icônes avant de poursuivre.

Conseil : "Conseil" signale les informations complémentaires que vous pouvez trouver utiles pour mener à bien une tâche.

ATTENTION : "Attention" signale qu'il existe une possibilité d'endommager des données ou de l'équipement. Nous vous recommandons de ne pas poursuivre après une section comportant ce message avant que vous ayez pleinement assimilé la procédure.

AVERTISSEMENT : "Avertissement" signale une menace potentielle pour la sécurité personnelle.

Operazioni preliminari (ITALIANO)

Le seguenti icone vengono utilizzate nella guida a scopo cautelativo. Prima di procedere Vi viene richiesta un'attenta lettura di tutte le procedure, contrassegnate dalle suddette icone, affinché vengano applicate correttamente.

Suggerimento: "Suggerimento" fornisce indicazioni supplementari, comunque utili allo scopo.

ATTENZIONE: “Attenzione” indica il potenziale danneggiamento dei dati o delle attrezzature in dotazione. Vi raccomandiamo di non procedere con le operazioni, prima di aver ben letto e compreso la sezione contrassegnata da questo messaggio, onde evitare di compromettere il corretto svolgimento dell'operazione stessa.

PERICOLO: “Pericolo” indica l'eventuale pericolo di danno provocato alle persone, mettendo a rischio la vostra incolumità personale.

Vóór u aan de slag gaat (NEDERLANDS)

De volgende pictogrammen worden in de hele handleiding gebruikt in het belang van de veiligheid. We raden u aan alle procedure-informatie die door deze pictogrammen wordt gemarkeerd, aandachtig te lezen en ervoor te zorgen dat u de betreffende procedure goed begrijpt vóór u verder gaat.

VOORZICHTIG: “Voorzichtig” geeft aan dat er risico op schade aan data of apparatuur bestaat. We raden u aan even halt te houden bij de sectie die door dit woord wordt gemarkeerd, tot u de procedure volledig begrijpt.

WAARSCHUWING: Een waarschuwing wijst op een mogelijk gevaar voor de persoonlijke veiligheid.

Antes de começar (PORTUGUÊS)

Os ícones mostrados abaixo são utilizados ao longo do manual para assinalar assuntos relacionados como a segurança. Deverá ler e entender claramente todos os procedimentos marcados com estes ícones ande de prosseguir.

Sugestão: Uma sugestão assinala informações adicionais que lhe poderão ser úteis para executar uma tarefa.

CUIDADO: “Cuidado” indica que existe a possibilidade de serem causados danos aos dados ou ao equipamento. Não deverá avançar para lá de uma secção marcada por esta mensagem sem ter primeiro entendido totalmente o procedimento.

AVISO: Um aviso indica que existe um possível risco para a segurança pessoal.

Ennen kuin aloitat (SUOMI)

Seuraavilla kuvakkeilla kiinnitetään tässä oppaassa huomiota turvallisuusseikkoihin. Näillä kuvakkeilla merkityt menettelytavat tulee lukea ja ymmärtää ennen jatkamista.

Huomautus: Huomautus sisältää tietoja, jotka tulee ottaa huomioon.

VAROITUS: Varoitus varoittaa tietojen tai laitteiden vahingoittumisen mahdollisuudesta. Tällä merkillä merkitystä kohdasta ei tule jatkaa eteenpäin ennen kuin täysin ymmärtää kuvatus menettelyn.

VAARA: Vaara varoittaa henkilövahingon mahdollisuudesta.

Innan du startar (SVENSKA)

Följande ikoner används i hela handboken för att markera säkerhetsaspekter. Läs igenom handboken ordentligt så att du förstår steg som har markerats med dessa ikoner innan du fortsätter.

Obs: “Obs” anger vad du ska observera.

FÖRSIKT: “Försikt” anger vad som kan leda till data eller utrustningsskador. Fortsätt inte till nästa avsnitt innan du förstår det steg som har markerats med detta meddelande.

VARNING: “Varning” anger vad som kan leda till personskador.

Chapter 2: Safety information

This section lists important safety guidelines to follow when working with the equipment.

Electrostatic discharge precautions

To ensure proper handling of system components and to prevent hardware faults caused by electrostatic discharge, follow these safety precautions:

- Wear an anti-static wrist or ankle strap.
- Observe all standard electrostatic discharge precautions when handling plug-in modules or components that have been removed from any anti-static packaging.
- Avoid contact with backplane components and module connectors.

Safety and handling precautions

To ensure your safety and the safe handling and correct operation of the equipment, follow all safety precautions and instructions.



Caution: Observe safe lifting practices. Each server or each storage system can weigh 51 lb. (23 kg) or more. At least two people are required to handle and position a server in a rack.



Caution: There is a risk that a cabinet could fall over suddenly. To prevent this from occurring:

- If your system comes with a rack stabilizer plate, install it.
- Fill all expansion cabinets including all storage enclosures from the bottom to the top.
- Do not remove more than one unit from the rack at a time.

Electrical precautions

Follow these guidelines to ensure your safety and the safe handling of equipment:

- Provide a suitable power source with electrical overload protection to meet the power requirements of the entire system (the server/cluster and all storage systems and switches).
- Provide a power cord suitable for the country of installation (if a power cord is not supplied).
- Power cords supplied with this server or system may be less than 1.5m in length. These cords are for use with a power distribution unit (PDU), which is mounted inside the 19-inch rack. If you require longer cables, contact your Hitachi representative.
- Provide a safe electrical ground connection to the power cord. Check the grounding of an enclosure before applying power.
- Only operate the equipment from nominal mains input voltages in the range 100 - 240Vac, 6A max, 50/60Hz.



Caution: Turn off all power supplies or remove all power cords before undertaking servicing of the system.

- Unplug a system component if it must be moved or if it is damaged.



Note: For additional data protection, use an external UPS to power the server. Also, each of the redundant power supplies in the server and in the storage systems must be operated from a different main power circuit to provide a degree of protection from main power supply failures. If one circuit fails, the other continues to power the server and the storage system.

Battery precautions

To ensure your safety and the safe handling of batteries, follow these handling guidelines.



Caution: Ensure that batteries are replaced in accordance with the instructions in the manual or their relevant manual.

- Only replace a battery with one of the prescribed type. Use of the wrong battery type or incorrect replacement may result in an explosion.
- Dispose of batteries according to the laws and regulations of your region.
- French:
 - Seulement remplacer une batterie avec le type recommandé. L'utilisation du mauvais type de batterie ou une mauvaise installation peut entraîner une explosion.
 - Jetez les batteries conformément aux lois et règlements de votre région.
- Chinese:

注意
用错误型号电池更换会有爆炸危险
务必按照说明处置用完的电池
- Japanese:

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると
電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を
講ずるよう要求されることがあります。 VCCI- A

Data protection precautions

To help ensure the protection of data and safe handling of equipment, follow these guidelines:

- Each storage enclosure contains multiple removable hard disk drive (HDD) modules. These units are fragile so handle them with care and keep them away from strong magnetic fields.
- All supplied plug-in modules and blanking plates must be in place to complete the internal circuitry and enable air to flow correctly around an enclosure.
- Using the system for more than a few minutes with modules or blanking plates missing can cause an enclosure to overheat, leading to power failure and data loss. Such use may invalidate the warranty.
- A loss of data can occur if a hard drive module is removed. Immediately replace any modules that are removed. If a module is faulty, replace it with one of the same type, of at least the same capacity and speed.
- Always shut down the system before it is moved, switched off, or reset.

- All storage enclosures are fitted with optical SFP transceivers. The transceivers that are approved for use with supported storage enclosures vary depending on the unit. The transceivers qualified for older systems might not be approved for use with the most current storage systems. To ensure proper operation of the server and the storage subsystems, use only the approved replacement parts for each system. See Hitachi Vantara Support Connect for technical details about replacement parts.
- Maintain backup routines and do not abandon backup routines.

Chapter 3: Mandatory regulations

The sections that follow outline the mandatory regulations governing the installation and operation of the system. Adhere to these instructions to ensure that regulatory compliance requirements are met.

International standards

The equipment described in this manual complies with the requirements of the following agencies and standards.

Safety

- Worldwide: IEC60950-1: 2nd edition
- EU: EN60950-1: 2nd edition
- North America: UL60950-1: 2nd edition; CAN/CSA-C22.2 No.60950-1-07 2nd edition

EMC

- USA: FCC Part 15 Subpart B class A
- Canada: ICES-003 Issue No 4 class A
- EU: EN55022 class A; EN61000-3-2; EN61000-3-3; EN55024
- Australia & New Zealand: C-Tick – AS/NZS CISPR22 class A
- South Korea: KCC class A
- Japan: VCCI class A

Certification for the following approvals marks have been granted:

- European Union CE mark, including RoHS and WEEE
- China: CCC
- CU (including Russia): EAC
- Taiwan: BSMI
- Argentina: IRAM
- Australia & New Zealand: C-Tick
- Mexico: NOM and CONUEE
- South Africa: ICASA
- India: BIS

Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if it is not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Neither the provider nor the manufacturer is responsible for any radio or television interference caused by using non-recommended cables and connectors, or by unauthorized changes or modifications to this equipment.

Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. The device can not cause harmful interference.
2. The device must accept any interference received, including interference that might cause undesired operation.

European Union (EU) Statement

This product conforms to the protection requirements of the following EU Council Directives:

- 89/336/EEC Electromagnetic Compatibility Directive
- 73/23/EEC Low Voltage Directive
- 93/68/EEC CE Marking Directive
- 2015/863/EU amending Annex II of Directive 2011/65/EU Restriction in the use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) - This product is 10/10 (fully) compliant.

The manufacturer cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.



Caution: This is a Class A product and as such, in a domestic environment, might cause radio interference.

Canadian Department of Communication Compliance Statement

This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité aux normes du ministère des Communications du Canada

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Radio Protection for Germany

Dieses Gerät erfüllt die Bedingungen der EN 55022 Klasse A.

Food and Drug Administration (FDA)

The product complies with FDA 21 CFR 1040.10 and 1040.11 regulations, which govern the safe use of lasers.

Chinese RoHS Compliance Statement

有毒有害物质名称标识

Toxic and Hazardous Substances Table

部件名称 Part Name	有毒有害物质或元素 Toxic and Hazardous Substances and Elements					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
机箱 Chassis	O	O	O	O	O	O
电源 Power Supply Module	O	O	O	O	O	O
风扇模块 Fan Module	O	O	O	O	O	O
硬盘 Hard Disk Drive	O	O	O	O	O	O

O：表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 规定的限量要求以下

O：Indicates that the toxic or hazardous substances contained in all of the homogeneous materials for this part is below this limit requirement in SJ/T 11363-2006.

X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 规定的限量要求

X：Indicates that the toxic or hazardous substances contained in at least one of the homogeneous materials used for this part is above the limit requirement in SJ/T 11363-2006.



Note: The Hard Disk Drive is a solid state disk (SSD) device.

Figure 1 Chinese RoHS Compliance Statement

Taiwan RoHS Compliance Statement

設備名稱：存儲陣列服務器，型號（型式）：HNAS 4100 Equipment name 系列型號：HNAS 4060, HNAS 4080 Type designation (Type)						
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻Hexavalent chromium (Cr ⁺⁶)	多溴聯苯Polybrominated biphenyls (PBB)	多溴二苯醚Polybrominated diphenyl ethers (PBDE)
產品內外殼 (含框架)	☐	☐	☐	☐	☐	☐
電路板	☐	☐	☐	☐	☐	☐
主機板	☐	☐	☐	☐	☐	☐
記憶卡	☐	☐	☐	☐	☐	☐
散熱模組(風扇)	☐	☐	☐	☐	☐	☐
配件(電源線、排線)	☐	☐	☐	☐	☐	☐
其它固定組件(螺絲、夾具)	☐	☐	☐	☐	☐	☐
備考1. “超出0.1 wt %”及“超出0.01 wt %”係指限用物質之百分比含量超出百分比含量基準值。 Note 1 : “Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition. 備考2. “○”係指該項限用物質之百分比含量未超出百分比含量基準值。 Note 2 : “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence. 備考3. “—”係指該項限用物質為排除項目。 Note 3 : The “—” indicates that the restricted substance corresponds to the exemption.						

South Africa: ICASA

TA 2016-211 Approved



Chapter 4: Hitachi NAS Platform server components

This section describes the components included in the server chassis.

A Hitachi Unified Storage File Module system can contain single Hitachi NAS Platform server or several servers that operate as a cluster. Clusters of more than two servers include two 10 Gbps Ethernet switches. Hitachi Vantara only requires two switches for redundancy.

For information about the physical configuration of a cluster configuration, see the *Hitachi NAS Platform and Hitachi Unified Storage File Module System Installation Guide*.

The Hitachi NAS Platform server chassis consists of

- A removable fascia
- MMB (Motherboard)
- MFB (FPGA Board)
- Two hot-swappable fan assemblies
- Dual power supplies
- NVRAM backup battery pack
- Dual 2.5 inch disk drives

System components

The system contains many components and is housed in a rack or cabinet. This section describes the main system components.

Component	Description
Hitachi NAS Platform or Hitachi Unified Storage File Module server	The system can contain a single server or several servers that operate as a cluster. Clusters that use more than two servers include two 10 Gbps Ethernet switches. Hitachi Vantara supports two switches for redundancy. For information about the physical configuration of a cluster configuration, see the <i>Hitachi NAS Platform and Hitachi Unified Storage File Module System Installation Guide</i>.
System management unit (SMU)	The SMU is the management component for the other components in a system. An 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. In a single-server configuration, typically an embedded SMU manages the system. In clustered systems and some single-node systems, an external SMU provides the management functionality. In some cases, multiple SMUs are advisable.
Storage subsystems	A Hitachi NAS Platform system or a Hitachi Unified Storage File Module system can control several storage enclosures. The maximum number of storage enclosures in a rack depends on the model of storage enclosures being installed. Refer to the <i>Storage Subsystem Administration Guide</i> for more information on supported storage subsystems.
Fibre Channel (FC) switches	The server supports FC switches that connect multiple servers and storage subsystems. See Hitachi Vantara Support Connect for information about which FC switches are supported.
External Fast Ethernet (10/100) or Gigabit Ethernet switches	(HNAS 4040 model only) A standalone server can operate without an external Ethernet switch, as long it uses the embedded SMU and there are fewer than three RAID subsystems attached. A standalone server requires an external Ethernet switch if there are more than two RAID subsystems attached or if there are two RAID subsystems attached and an external SMU is used. All cluster configurations require an external Ethernet switch.
External 10 Gigabit Ethernet (10 GbE) switches	A single node server can operate without an external Ethernet switch if the server uses the embedded SMU. This is also true if fewer than three RAID subsystems are attached to the server. If an external SMU is used, a single node server requires a cable from the SMU to Eth1.

Component	Description
	With the HNAS 4040 model, the switch is also required if there are more than two RAID subsystems attached or if there are two RAID subsystems attached. All cluster configurations require an external Ethernet switch. See Hitachi Vantara Support Connect for information about the 10 GbE switches that have been qualified for use with the system, and to find out about the availability of those switches.
10 GbE switches	The server connects to a 10 GbE switch for connection with the public data network (customer data network). Also, a 10 GbE switch is required for internal cluster communications for clusters of three or more nodes. See Hitachi Vantara Support Connect for information about the 10 GbE switches that have been qualified for use with the server, and to find out about the availability of those switches. Hitachi Vantara requires dual 10 GbE switches for redundancy. In a dual-switch configuration, if one switch fails, the cluster nodes remain connected through the second switch.

Server components

The Series 4000 server comes in four models: Hitachi NAS Platform 4040, Hitachi NAS Platform 4060, Hitachi NAS Platform 4080, and Hitachi NAS Platform 4100.

Physically, models HNAS 4060 and HNAS 4080 are identical. To upgrade a model HNAS 4060 to a model HNAS 4080 requires the addition of a software license. From outside of the chassis, model HNAS 4100 is identical to the other models--it shares the same ports and connectivity.

All server models have a chassis that is 3U (5.25 inches) high, 480 millimeters (19 inches) wide, rack mountable, and a maximum of 686 millimeters (27 inches) deep, excluding the bezel. The chassis contains:

- Front bezel
- MMB (Main Motherboard)
- MFB (Main FPGA Board)
 - Model 4040 uses an MFB
 - Models 4060 and 4080 use an MFB2
 - Model 4100 uses an MFB2E
- Hot-swappable fan assemblies
 - Model 4040 has two fans
 - Models 4060, 4080, and 4100 have dual fans
- Dual power supplies
- NVRAM backup battery pack
- Dual 2.5 inch disk drives

If there is an issue with the motherboard (MMB) or field programmable gate array (MFB), the server must be returned for repair. MMBs are not field replaceable and, typically, MFBs are not field replaceable. Many of the other components can be replaced in the field, and some are hot-swappable (they can be changed without shutting down the server). Field replaceable units (FRUs) include power supplies, an NVRAM backup battery pack, fan assemblies, and disk drives.

Server specifications

The following specifications are for the server. Except for the power and cooling values, these specifications do not reflect differences among models; they are the maximum for all server models. For more detailed specifications of a particular model or configuration, contact your representative.

Physical:

- Weight: 25 kg (55 lb.) with plastic bezel or 26 kg (57 lb.) with metal bezel
- Height: 132 mm. (5 in.)
- Depth (including handles and bezel): 725 mm. (28.6 in.)
- Width: 440 mm. (17.3 in.)
- Rack space required: 3U (5.25 in.)



Note: A rack unit, or U, is a unit of measure that is used to describe the height of equipment intended to be mounted in a rack. One rack unit is equivalent to 1.75 inches or 44.45 millimeters.

Power and cooling:



Note: The power supplies and cooling fans noted in the following table are hot-swappable.

Item	Model 4040	Models 4060, 4080, and 4100
Power supplies	2	2
Cooling fans	2	2
Current drawn:	110 VAC: 2.6A to 3.1A 208 VAC: 1.3A to 1.7A 230 VAC: 1.2A to 1.5A	110 VAC: 2.9A to 3.5A 208 VAC: 1.5A to 1.9A 230 VAC: 1.4A to 1.7A
Power supply rating	450W	550W
Average thermal (BTU per hour)	853	938
Max thermal (BTU per hour)	1057	1194
Max power usage	310W	350W

Other thermal:

- Temperature range (operational): 10° to 35° C (50° to 95° F)
- Maximum rate of temperature change per hour (operational) 10° C (18° F)
- Temperature range (storage): -10° to 45° C (14° to 113° F)
- Maximum rate of temperature change per hour (storage) 15° C (27° F)
- Temperature range (transit): -20° to 60° C (-4° to 140° F)
- Maximum rate of temperature change per hour (transit) 20° C (36° F)

Airflow:

Fan speed	Single fan in free air		Single fan at 33% perforation	Two fans at 33% perforation		
	m ³ /min	CFM	m ³ /min	m ³ /min	CFM	
@ 100%	7.40	261.22	2.96	5.92	208.98	Not used
@ 2/3	4.93	174.15	1.97	3.95	139.32	Fan failure or over temperature
@ 1/3	2.47	87.07	0.99	1.97	69.66	Normal operation

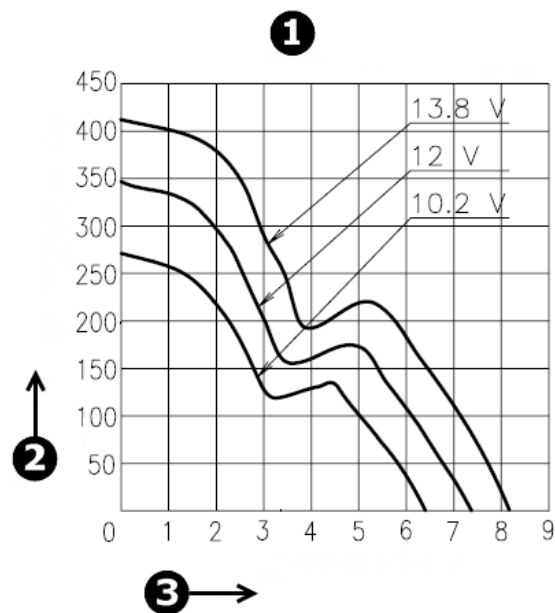


Figure 2 Airflow performance curves

Item	Description
1	Performance curves, pulse width modulation (PWM) = 100%
2	Static pressure (Pa)
3	Airflow (m ³ /minute)

Humidity:

- Operational: 20-80%
- Storage: 10-90%
- Transit: 5-95%

Noise: A-weighted Sound Power Level, Lwa (db re 1pW):

- Typical: 71
- Max: 81

Shock and vibration:

- Optional random vibration: 10 to 350 Hz @ 0.18 Grms
- Non-operational sinusoidal vibration: 60 to 350 Hz: @ 1g
- Non-operational shock: 3g 11ms, half sine

Packaged transport specification:

- Drops from 356mm and 508mm as per ASTM D5276
- Vibration at up to 0.53 Grms as per ASTM D4728

Altitude:

- Maximum of 2000 meters

Ventilation

There are vents and fan openings on the front and the rear of the server. These openings are designed to allow airflow, which prevents the server from overheating.



Note: At least four inches of clearance must be present at the rear of the server rack so that airflow is unrestricted.



Caution:

- Do not place the server in a built-in installation unless proper ventilation is provided.
- Do not operate the server in a cabinet with an internal ambient temperature that exceeds 35° C (95° F).

Server front panel

The front of these servers feature a removable bezel that shields the front-facing server components.

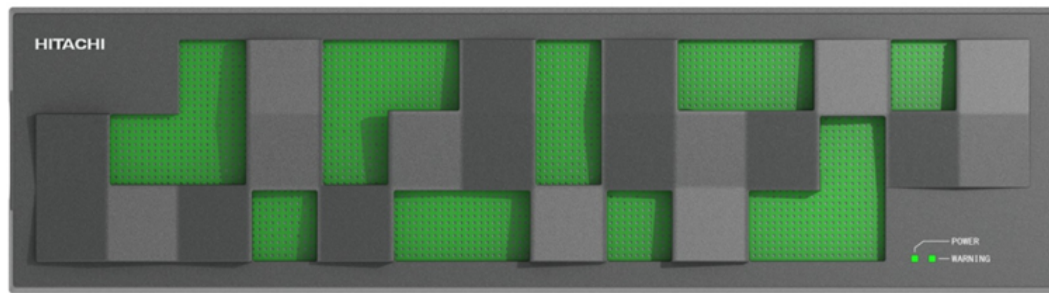


Figure 3 Server front panel plastic bezel

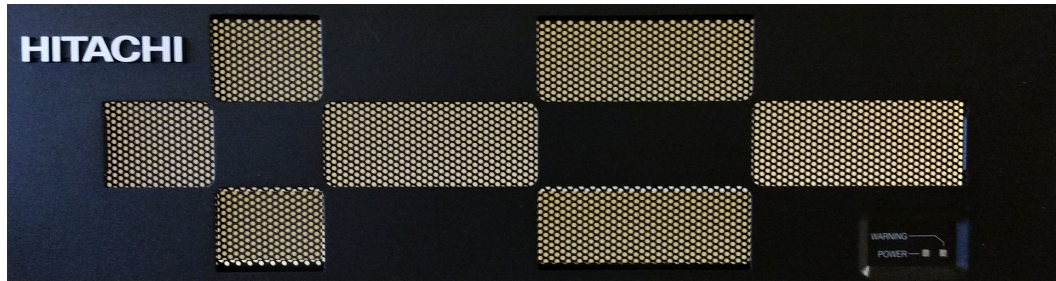


Figure 4 Server front panel metal bezel

Once the bezel is removed, the front-facing components on the server chassis are visible.

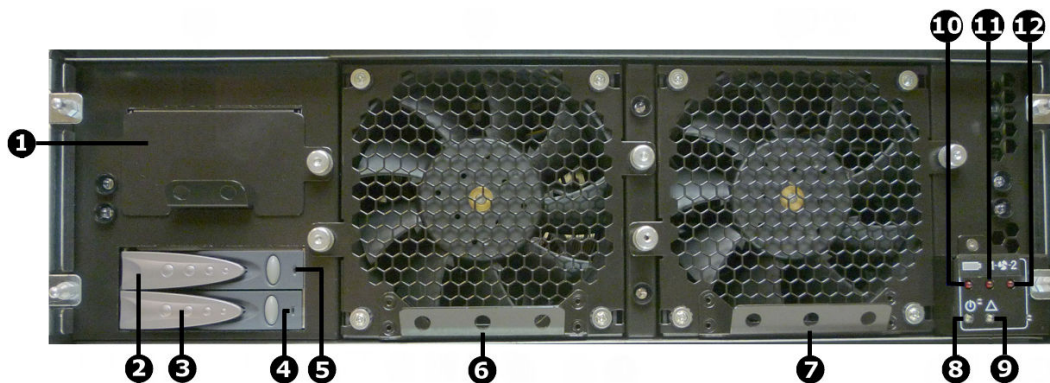


Figure 5 Server model 4040 front panel components (bezel removed)

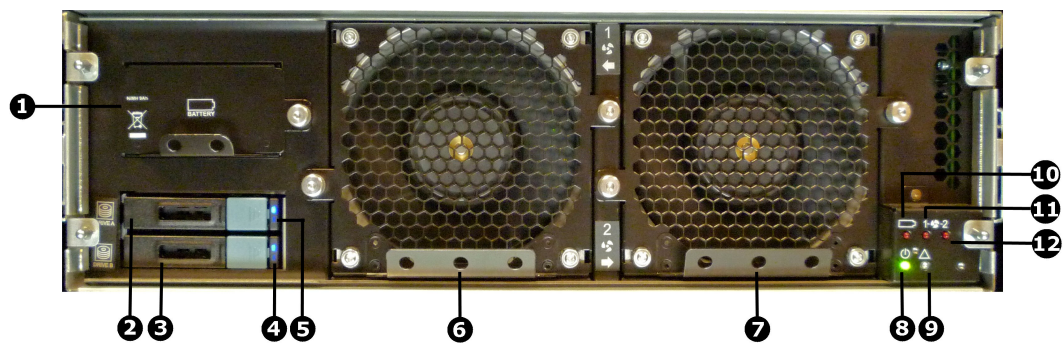


Figure 6 Server models 4060, 4080, 4100 front panel components (bezel removed)

Table 1 Server front panel component descriptions

Item	Description
1	NVRAM battery backup pack
2	Hard disk drive A (top)
3	Hard disk drive B (bottom)
4	Disk B status LED
5	Disk 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

LED status indicators

The LEDs (light emitting diodes) on the front of the chassis indicate the overall status of the server, as well as the status of some of the individual components. The NVRAM backup battery pack, each of the O/S disk drives, and each of the fan assemblies has a status LED.

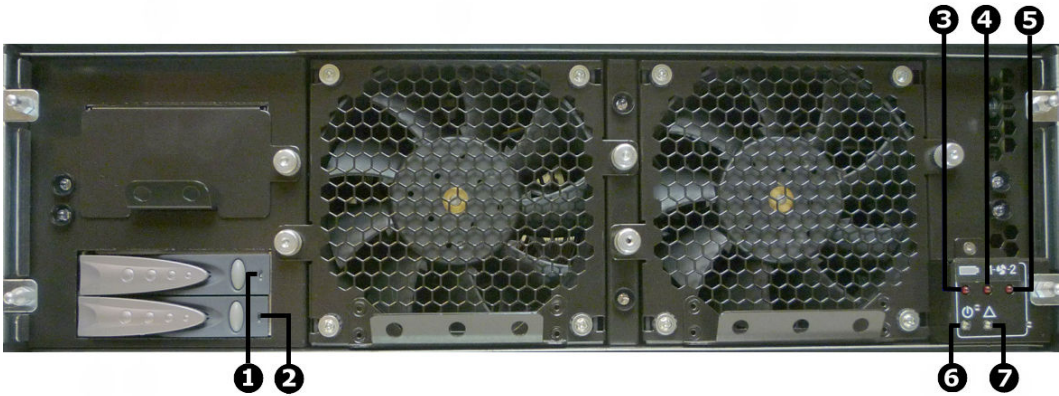


Figure 7 Model 4040 status LEDs

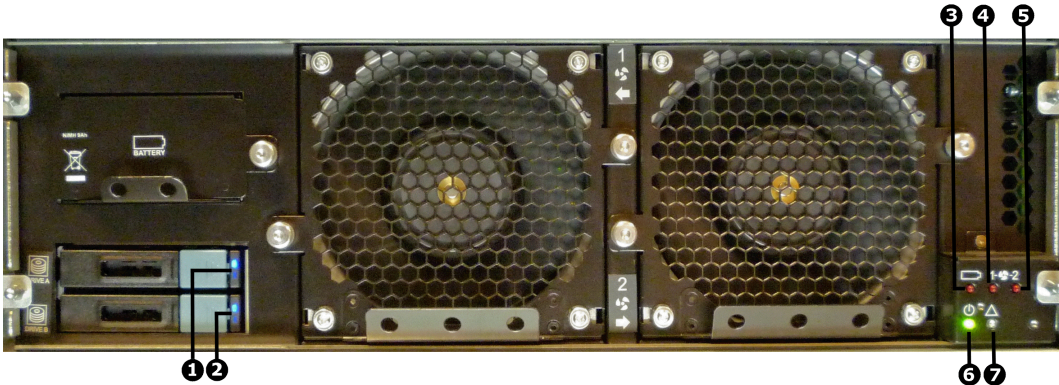


Figure 8 Models 4060, 4080, and 4100 status LEDs

Table 2 LED descriptions

LEDs	Meaning
1	O/S disk drive A status LED
2	O/S disk drive B status LED
3	NVRAM battery backup pack status LED
4	Fan 1 status LED
5	Fan 2 status LED
6	Power status LED
7	Server status LED

Table 3 Power status LED (green)

LEDs	Meaning
Green	Normal operation with a single server or an active cluster node in operation.
Slow flash (once every three seconds)	The system has been shut down.
Medium flash (once every .8 seconds)	The server is available to host file services but is not currently doing so. Also if no EVS is configured or all EVSs are running on the other node in a cluster.
Fast flash (five flashes per second)	The server is rebooting.
Off	The server is not powered up.

Table 4 Server status LED (amber)

LEDs	Meaning
Amber	Critical failure and the server is not operational.
Slow flash (once every three seconds)	System shutdown has failed. Flashes once every three seconds.
Medium flash (once every .8 seconds)	The server needs attention, and a non-critical failure has been detected, for example, a fan or power supply has failed. Flashes once every .8 seconds.
Off	Normal operation.

Table 5 Battery pack status LED

LEDs	Meaning
Red	If this LED is on immediately after installing a new battery pack, it indicates that an initial battery charging and conditioning cycle is in progress. The initial battery conditioning takes approximately 24 hours, and the LED will turn off after the cycle is complete. If this LED is on during normal operation (not after installing a new battery pack), either the battery has exceeded its two year life or a problem has been detected. Check the battery status before determining any service operation.

LEDs	Meaning
Off	Normal operation.

Table 6 Fan status LEDs

LEDs	Meaning
Red	Fan has failed, fan speed is out of acceptable range, or fan speed is not being reported. (This LED will be on if the corresponding fan has been removed.) Replace the fan as soon as possible.
Off	Normal operation.

Table 7 O/S disk activity and status LEDs

LEDs	Meaning
Blue	If this LED is on and blue, the disk is operating normally and no problems have been detected. If the LED is flashing blue, it indicates disk activity. If the LED is on, but not flashing, there is currently no disk activity.
Red	If this LED is on immediately after installing a new O/S disk, it indicates that the RAID configuration for the server is being rebuilt. The LED will turn off after the RAID configuration is restored. The amount of time it takes for the RAID configuration to be rebuilt after a new disk drive is installed depends on the amount of user and system configuration data stored. If this LED is on during the course of normal operation (not after installing a new O/S disk), either the disk has failed or the server's RAID configuration has been degraded.

NVRAM backup battery pack

Each server contains a battery pack. The battery pack maintains the NVRAM contents when the server is not receiving power (due to a power failure or a short-term shut down). The battery pack is located behind the front bezel cover of the server, on the left-hand side. The battery pack is hot-swappable and can only be accessed after the front bezel has been removed.



Figure 9 Model 4040 NVRAM backup battery pack (front view)



Figure 10 Model 4060, 4080, and 4100 NVRAM backup battery pack (front view)

Battery pack characteristics:

- Each server contains a single battery module. The module contains dual redundancy inside.
- The battery pack uses NiMH technology.
- A battery pack has a two year operational life. A timer starts when a server is booted for the first time, and the timer is manually restarted when a replacement batter pack is installed. After two years of operation, a log warning event is issued to warn the user that the battery pack should be replaced.
- The battery pack is periodically tested to ensure it is operational.
- A fully charged battery pack maintains the NVRAM contents for approximately 72 hours.
- When a new server is installed and powered on, the battery pack is not fully charged (it will not be at 100% capacity). After being powered on, the server performs tests and starts a conditioning cycle, which may take up to 24 hours to complete. During the conditioning cycle, the full NVRAM content backup protection time of 72 hours cannot be guaranteed.
- A replacement battery pack may not be fully charged (it may not be at 100% capacity) when it is installed. After a new battery pack is installed, the server performs tests and starts a conditioning cycle, which may take up to 24 hours. During the conditioning cycle, the full NVRAM content backup protection time of 72 hours cannot be guaranteed.

- If a server is left powered off, the battery will discharge slowly. This means that, when the server is powered up, the battery will take up to a certain number of hours to reach full capacity and the time depends upon whether a conditioning cycle is started. The scenarios are:
 - 24 hours if a conditioning cycle is started
 - 3 hours if a conditioning cycle is *not* started

During the time it takes for the battery pack to become fully charged, the full 72 hours of NVRAM content protection cannot be guaranteed. The actual amount of time that the NVRAM content is protected depends on the charge level of the battery pack.

- A battery pack may become fully discharged because of improper shutdown, a power outage that lasts longer than 72 hours, or if a server is left unpowered for a long period of time.

If the battery pack is fully discharged:

- The battery pack may permanently lose some long term capacity.
 - Assuming a battery conditioning cycle is not started, a fully discharged battery pack takes up to 3 hours before it is fully charged. If a battery conditioning cycle is started, a fully discharged battery pack takes up to 24 hours before it is fully charged.
 - A battery conditioning cycle is started if the server is powered down for longer than three months.
- A battery pack may be stored outside of the server for up to one year before it must be charged and/or conditioned. After one year without being charged and possibly conditioned, the battery capacity may be permanently reduced.

If you store battery packs for more than one year, contact your representative to find out about conditioning your battery packs.

- When preparing a server for shipment, if the NVRAM is still being backed up by battery (indicated by the flashing NVRAM LED), the battery can be manually isolated using the reset button. See [Reset button \(RST\) \(on page 56\)](#) for the location of the reset button.

When preparing a server for shipment or if it will be powered down for any length of time, it is important that the server has been shut down correctly before powering-off.

Otherwise, if the server is improperly shut down, the batteries supplying the NVRAM will become fully discharged. This also occurs if the system is powered down for too long without following the proper shutdown procedure.



Note: If the batteries become fully discharged, or the system is to be powered down for an extended period, see [Powering down the server \(on page 82\)](#). Contact customer support for information about recharging batteries.

To replace the NVRAM battery backup pack, see [Replacing the NVRAM backup battery pack \(on page 68\)](#).

Hard disk drives

The server contains two hard disks, which are configured as a Linux SW RAID 1 pair, and they store server or cluster-related data. These hard disks are not part of the customer-usable data storage that is available to the server.

Hard disks are located behind the bezel on the left side of the chassis.



Note: Failed hard disks are hot-swappable, so a failed hard disk can be replaced without shutting down the server. However, there are serious risks in trying to swap a drive that is not failed. It is strongly recommended to avoid performing disk replacement procedures during busy periods in order to minimise risk of any disruption being caused by the procedure.



Note: Do not attempt to replace or recover a hard disk without the assistance of Hitachi Vantara Customer Support.



Figure 11 Hard disk drives status and activity status LEDs - model 4040



Figure 12 Hard disk drives status and activity status LEDs - models 4060, 4080, and 4100

Item	Description
1	Disk A status and activity LEDs
2	Disk B status and activity LEDs

Table 8 O/S disk activity and status LEDs

LEDs	Meaning
Blue	If this LED is on and blue, the disk is operating normally and no problems have been detected. If the LED is flashing blue, it indicates disk activity. If the LED is on, but not flashing, there is currently no disk activity.
Red	If this LED is on immediately after installing a new O/S disk, it indicates that the RAID configuration for the server is being rebuilt. The LED will turn off after the RAID configuration is restored. The amount of time it takes for the RAID configuration to be rebuilt after a new disk drive is installed depends on the amount of user and system configuration data stored. If this LED is on during the course of normal operation (not after installing a new O/S disk), either the disk has failed or the server's RAID configuration has been degraded.

Fans

The server features dual hot-swappable fan assemblies. The fans provide for front-to-back airflow to be consistent with other storage system components.

The server's cooling airflow enables the system to operate in an ambient temperature range of 10°C to 35°C when mounted in a rack or cabinet with associated components required to make up a storage system. The storage system administrator is responsible for ensuring that the ambient temperature within the rack does not exceed the 35°C operating limit.

The server continues to operate following the failure of a single fan and during the temporary removal of a fan for replacement. Replace a failed fan as soon as possible.



Caution: If a fan has failed, replace the fan as soon as possible to reduce the amount of time the server is operating with reduced airflow.

The fans are contained within two assemblies, each containing a single variable-speed fan. Fan assemblies are located behind the front bezel. Each fan assembly is secured to the chassis with two thumbscrews and a blind-mate electrical connector; no tools are required to remove or install a fan assembly.

Two fan status LEDs provide fan status information. These LEDs are located behind the bezel on the right side of the chassis.

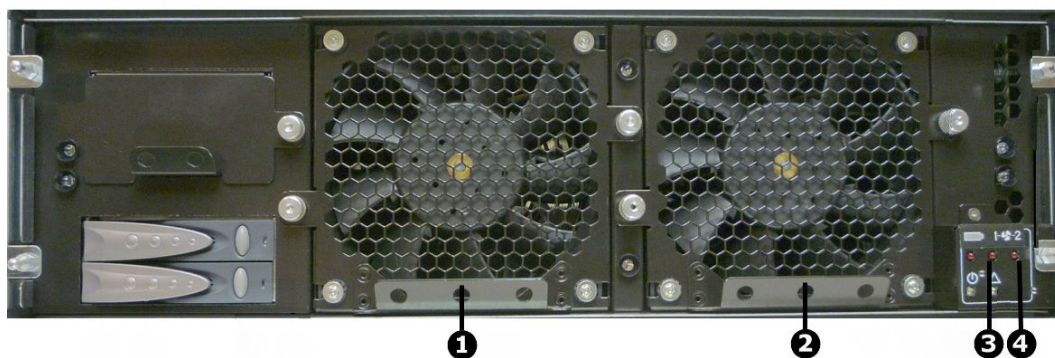


Figure 13 Fan and fan status LED locations - model 4040

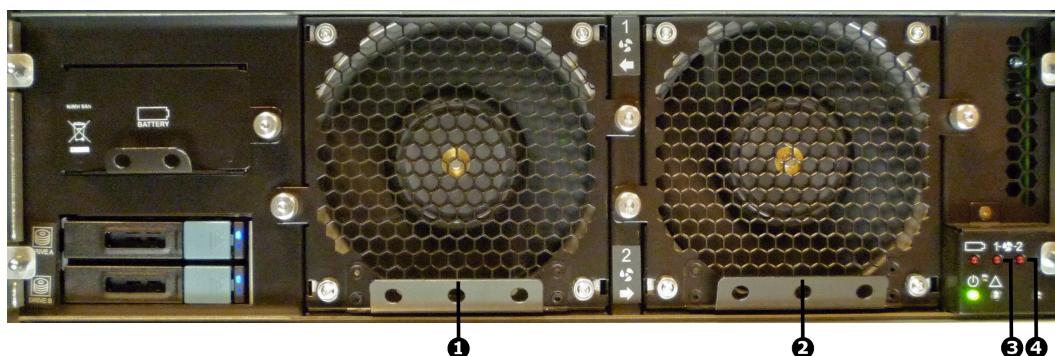


Figure 14 Fan and fan status LED locations - models 4060, 4080, and 4100

Item	Description
1	Fan 1 (left)
2	Fan 2 (right)
3	Fan 1 status LED
4	Fan 2 status LED

Table 9 Fan status LEDs

LEDs	Meaning
Red	Fan has failed, fan speed is out of acceptable range, or fan speed is not being reported. (This LED will be on if the corresponding fan has been removed.) Replace the fan as soon as possible.
Off	Normal operation.

Server rear panel - model 4040

The rear panel of the server features numerous ports, connectors, switches, and LEDs.

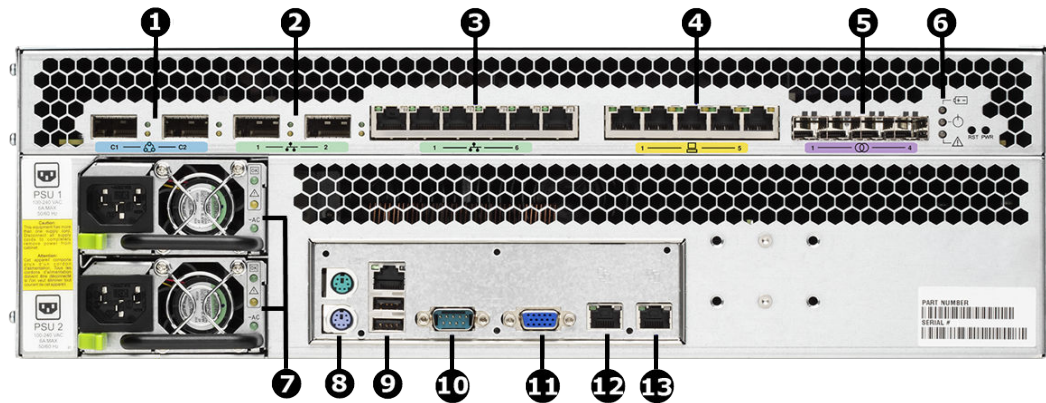


Figure 15 Server rear panel components for model HNAS 4040



Note: Except for the ports and connectors described in the following, none of the other ports or connectors should be used without guidance from technical support.

Item	Connectivity	Quantity	Description
1	Clustering ports 10 GbE	2	For cluster management and heartbeat, connect to: - Two way configuration: Connect to corresponding cluster server ports (left port to left port and right port to right port). - N-way configuration: Connect to 10 GbE switch.
2	10 GbE network ports	2	Connection to external 10 Gbps Ethernet data network.
3	Gigabit Ethernet network ports	6	Connection to external Ethernet data network.
4	10/100 Ethernet port	5	Connection to private management network.
5	Storage or FC switch	4	Connection to disk arrays or (where present) to the FC switches.
6	n/a	3	Status LEDs (NVRAM, power, and server), and Power and Reset buttons.

Item	Connectivity	Quantity	Description
7	Power supply units: PSU 1 PSU 2	2	Connect to the rack's Fault group: ▪ PSU 1 to Fault group A ▪ PSU 2 to Fault group B
8	I/O ports	2	Keyboard (purple) and mouse (green) ports. <i>(Reserved for Customer Service Engineer access only.)</i>
9	I/O ports	2	USB port. <i>(Reserved for Customer Service Engineer access only.)</i>
10	RS-232	1	Management interface. <i>(Reserved for Customer Service Engineer access only.)</i>
11	Video port	1	Video management interface port. <i>(Reserved for Customer Service Engineer access only.)</i>
12	ETH0 1000baseT Ethernet (gray logo)	1	External system management. Connect to the customer's management switch.
13	ETH1 1000baseT Ethernet (yellow logo)	1	Management port. Connect to the rack's internal Ethernet switch.

Rear panel server LED and button locations

The rear panel of the server contains three (3) status LEDs that indicate server status and two (buttons) that are used to power up and reset the server.

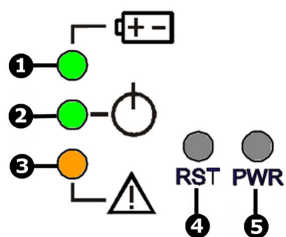


Figure 16 Rear panel server status LEDs and buttons

Table 10 Rear panel status LEDs and buttons

Item	Description
1	NVRAM battery backup status LED
2	Power status symbol and LED
3	Server status LED
4	Reset button
5	Power button

GE Ethernet network ports

The GE Ethernet Network ports are used to connect the server or cluster node to the customer's data network (also called the public network), and these ports may be aggregated into a single logical port (refer to the *Network Administration Guide* for more information on creating aggregations). GE ports operate at speeds of up to one (1) gigabit per second, and require the use of a standard RJ45 cable connector.

The GE Customer Ethernet Network ports are labeled as shown next:

**Figure 17 GE Customer Ethernet Network Ports Label**

Once connected, each GE port has two indicator LEDs; one green and one amber. These LEDs provide link status and network activity status information as follows:

Status/Activity (Per Port)		Meaning
Status	Green (On, not flashing)	1 Gbps link present
	Green Flashing	1 Gbps link standby in a redundant configuration
	Green Off	No link
Activity	Amber Flashing	Network activity
	Amber Off	No network activity

Rear panel LED state descriptions

The NVRAM, power, and server status LEDs indicate whether the server is powered, its operational state, and whether the NVRAM is currently being protected by the super capacitor's backup power. The way an LED flashes provides further information about what is currently occurring.

NVRAM Status LED (Green/Amber)

Table 11 NVRAM status LED (green/amber)

State	Meaning
Green (solid)	Normal operation
Amber (solid)	The NVDIMM or Supercapacitor backup energy source is faulty.
Off	Disabled or system powered down. The NVDIMM may contain data in internal flash memory that will be restored on boot.

The following table describes the various power status LEDs.

Table 12 Power status LED (green)

LEDs	Meaning
Green	Normal operational mode of an active cluster node.
Slow flash (once every three seconds)	The system has been shut down.
Medium flash (once every .8 seconds)	The server is available to host file services but is not currently doing so. This also occurs if no EVS is configured, or if all EVSs are running on the other node in a cluster.
Fast flash (five flashes per second)	The server is rebooting.
Off	The server is not powered up.

The following table describes the various server status LEDs:

Table 13 Server status LED (amber)

LEDs	Meaning
Amber	Critical failure and the server is not operational.

LEDs	Meaning
Slow flash (once every three seconds)	System shutdown has failed. Flashes once every three seconds.
Medium flash (once every .8 seconds)	The server needs attention, and a non-critical failure has been detected, for example, a fan or power supply has failed. Flashes once every .8 seconds.
Off	Normal operation.

10/100 private Ethernet ports

The 10/100 Private Ethernet Network ports function as an unmanaged switch for the private management network (refer to the *Network Administration Guide* for more information on the private management network). These ports are used by the server and other devices (such as an external SMU and other cluster nodes) to form the private management network. There are no internal connections to the server from these ports; instead, when joining a server to the private management network, you must connect from one of these ports to the management interface port on the server.

The 10/100 ports operate at speeds of up to 100 megabits per second, and require the use of a standard RJ45 cable connector.

The 10/100 Private Management Ethernet Network ports are labeled as shown next:



Figure 18 10/100 Private Management Network Ethernet Ports Label

Once connected, each 10/100 port has two indicator LEDs; one green and one amber. These LEDs provide link status and network activity status information as follows:

Status/Activity (Per Port)		Meaning
Status	Green (On, not flashing)	10 or 100 Mbps link present
	Green Off	No link
Activity	Amber Flashing	Network activity
	Amber Off	No network activity

Server rear panel - models 4060, 4080, and 4100

The rear panel of these server models features numerous ports, connectors, switches, and LEDs.



Note: Except for the ports and connectors described in the following figures, none of the other ports or connectors should be used without guidance from Hitachi Vantara Support Connect.

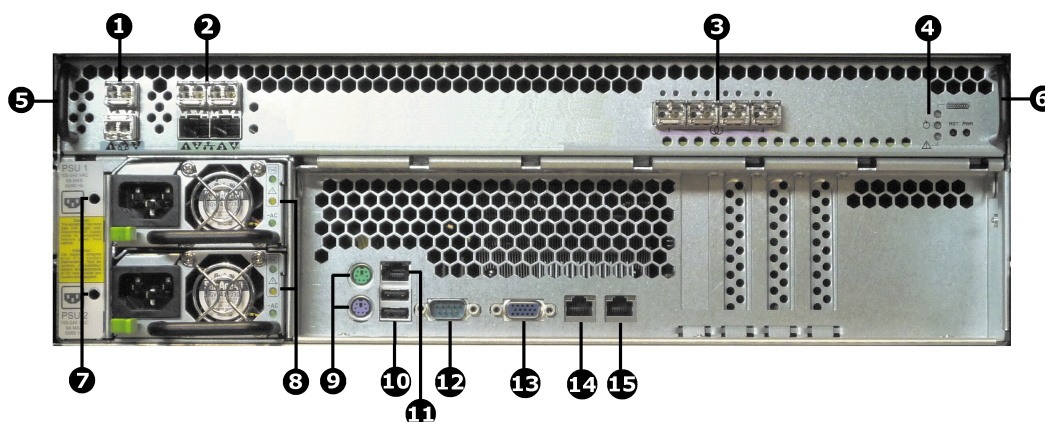


Figure 19 Server rear panel components for models HNAS 4060, HNAS 4080, and HNAS 4100

Item	Connectivity	Quantity	Description
1	Clustering ports 10 GbE (SFP+)	2	For cluster management and heartbeat, connect to: - Two way configuration: Connect to corresponding cluster server ports (top port to top port and bottom port to bottom port). - N-way configuration: Connect to 10 GbE switch.
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.  Caution: 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: - PSU 1 to Fault group A - PSU 2 to Fault group B
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.

Rear panel server LED and button locations

The rear panel of the server contains three (3) status LEDs that indicate server status and two (2) buttons that are used to power up and reset the server.

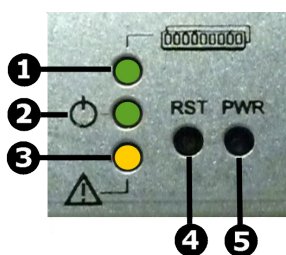


Figure 20 Rear panel server LEDs and buttons

Item	Meaning
1	NVRAM battery backup status LED
2	Power status symbol and LED
3	Server status LED
4	Reset button
5	Power button

Rear panel LED state descriptions

The NVRAM, power, and server status LEDs indicate whether the server is powered, its operational state, and whether the NVRAM is currently being protected by battery backup power. The way an LED flashes provides further information about what is currently occurring.

Table 14 NVRAM status LED (green/amber)

State	Meaning
Green (solid)	Normal operation

State	Meaning
Green (flashing)	NVRAM contents are protected by battery power
Amber (solid)	Battery pack is faulty or not fitted
Off	Disabled or NVRAM battery power exhausted

Table 15 Power status LED (green)

LEDs	Meaning
Green	Normal operation with a single server or an active cluster node in operation.
Slow flash (once every three seconds)	The system has been shut down.
Medium flash (once every .8 seconds)	The server is available to host file services but is not currently doing so. Also if no EVS is configured or all EVSs are running on the other node in a cluster.
Fast flash (five flashes per second)	The server is rebooting.
Off	The server is not powered up.

Table 16 Server status LED (amber)

LEDs	Meaning
Amber	Critical failure and the server is not operational.
Slow flash (once every three seconds)	System shutdown has failed. Flashes once every three seconds.
Medium flash (once every .8 seconds)	The server needs attention, and a non-critical failure has been detected, for example, a fan or power supply has failed. Flashes once every .8 seconds.
Off	Normal operation.

10 Gigabit Ethernet cluster interconnect ports

The 10 gigabit per second Ethernet (10 GbE) cluster ports allow you to connect cluster nodes together. The cluster ports are used only in a cluster configuration. The 10 GbE ports operate at speeds of ten (10) gigabits per second. The HNAS 4060, 4080, and 4100 models use an enhanced small form factor pluggable (SFP+) optical connector.

Do *not* use the 10 GbE cluster interconnect ports to connect to the customer data network (also known as the public data network).

For HNAS 4060, 4080, and 4100 models, the 10 GbE SFP+ transceiver modules are removable and interchangeable.



Note: When removed, the 10 GbE and 8 GB Fibre Channel (FC) SFP+ storage modules are indistinguishable from one another except for their part numbers. The part number is located on the side of the module housing and is only visible when the module is removed. Part number prefixes are different as follows:

- 10 GbE: FTLX<number>
- FC: FTLF<number>



Figure 21 10 GbE cluster interconnect ports label

Once connected, each 10 GbE port has two indicator LEDs; one green and one amber. These LEDs provide link status and network activity status information as follows:

Status/Activity (per port)		Meaning
Status	Green (on, not flashing)	10 Gbps link present
	Green flashing	10 Gbps link standby in a redundant configuration
	Green off	No link
Activity	Amber flashing	Network activity
	Amber off	No network activity

10 Gigabit Ethernet cluster interconnect ports

The 10 gigabit per second Ethernet (10 GbE) cluster ports allow you to connect cluster nodes together. The cluster ports are used only in a cluster configuration. The 10 GbE ports operate at speeds of ten (10) gigabits per second. The HNAS 4060, 4080, and 4100 models use an enhanced small form factor pluggable (SFP+) optical connector.

Do *not* use the 10 GbE cluster interconnect ports to connect to the customer data network (also known as the public data network).

For HNAS 4060, 4080, and 4100 models, the 10 GbE SFP+ transceiver modules are removable and interchangeable.



Note: When removed, the 10 GbE and 8 GB Fibre Channel (FC) SFP+ storage modules are indistinguishable from one another except for their part numbers. The part number is located on the side of the module housing and is only visible when the module is removed. Part number prefixes are different as follows:

- 10 GbE: FTLX<number>
- FC: FTLF<number>



Figure 22 10 GbE cluster interconnect ports label

Once connected, each 10 GbE port has two indicator LEDs; one green and one amber. These LEDs provide link status and network activity status information as follows:

Status/Activity (per port)		Meaning
Status	Green (on, not flashing)	10 Gbps link present
	Green flashing	10 Gbps link standby in a redundant configuration
	Green off	No link
Activity	Amber flashing	Network activity
	Amber off	No network activity

Server rear panel - all models

The rear panel of all server models features numerous ports, connectors, switches, and LEDs. The rear panel also offers access to the server's power supply units (PSUs).

Power button (PWR)

Under normal circumstances, the power button is rarely used. However, the power button can be used to restore power to the system when the server is in a standby power state.

When power cables are connected to the PSUs, the server normally powers up immediately. If, after 10 seconds, the LEDs on the power supplies are lit, but the Power Status LED is not lit, press the PWR button to restore power to the system. Open a case with Hitachi Vantara Support Connect to get the problem resolved.



Note: Do not use the power button during normal operation of the server. Pressing the power button immediately causes an improper shutdown of the system. The PSUs will continue to run.

Reset button (RST)

Pressing the reset button when the server is powered on causes a hard reset of the server.

This reset occurs after a 30-second delay, during which the server status LED flashes rapidly and the server attempts to shut down properly. Even with the delay, pressing the reset button does not guarantee a complete shutdown before rebooting. Only press the reset button when the server is powered on to recover a server which has become unresponsive. Pressing the reset button at this time may produce a dump automatically.



Caution: If the server is non-responsive, see [Restarting an unresponsive server \(on page 80\)](#). Do not pull the power cord. Pulling the power cord does not produce a dump.

Fibre channel storage ports

The Fibre Channel (FC) storage ports allow you to connect the server with other FC devices, such as storage subsystems.

FC ports operate at speeds of two to eight (8) gigabits per second. FC ports use an enhanced small form factor pluggable (SFP+) optical connector.

The SFP+ ports can be removed from the chassis.



Note: When removed, the 10 GbE and 8 GB Fibre Channel (FC) SFP+ storage ports are indistinguishable from one another except for their part numbers. The part number is located on the side of the port housing and is only visible when the port is removed. Part number prefixes are different as follows:

- 10 GbE: FTLX<number>
- FC: FTLF<number>



Figure 23 Fibre Channel storage ports label

Status/Activity (per port)		Meaning
Status	Green (on, not flashing)	FC link present

Status/Activity (per port)		Meaning
	Green off	No link
Activity	Amber flashing	Data activity
	Amber off	No data activity

10 Gigabit Ethernet customer data network ports

The 10 Gigabit Ethernet (GbE) customer data network ports are used to connect the server or cluster node to the customer's data network (also called the public data network). These ports may be aggregated into a 1, 2, 3, or 4 aggregated port.

See the *Network Administration Guide* for more information on creating aggregations.

The 10 GbE ports operate at speeds of ten (10) gigabits per second. The 10 GbE ports use enhanced small form factor pluggable (SFP+) optical connectors.



Note: The 10 GbE customer data network ports cannot be used to interconnect cluster nodes.

SFP+ optical transceiver module considerations. The SFP+ modules can be removed from the chassis. The 10 GbE SFP+ cluster interconnect modules are interchangeable with each other and with the 10 GbE SFP+ network modules.



Note: When removed, the 10 GbE and 8 GB Fibre Channel (FC) SFP+ storage modules are indistinguishable from one another except for their serial numbers. The serial number is located on the side of the module housing and is only visible when the module is removed. Serial numbers prefixes are different as follows:

- 10 GbE: FTLX<number>
- FC: FTLF<number>



Figure 24 10 GbE customer data network ports label

Once connected, each 10 GbE port has two indicator LEDs; one green and one amber. These LEDs provide link status and network activity status information as follows:

Status/Activity (per port)		Meaning
Status	Green (on, not flashing)	10 GbE network link present
	Green off	No link
Activity	Amber flashing	Network activity
	Amber off	No network activity

Power supply units

The server has dual, hot-swappable, load sharing, AC power supply units (PSUs). The PSUs are accessible from the rear of the server.

The server monitors the operational status of the power supply modules so that the management interfaces can indicate the physical location of the failed PSU. LED indicators provide PSU status information for the state of the PSU.

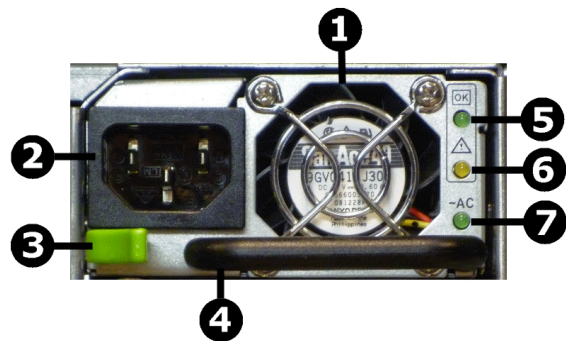


Figure 25 Power supply unit details

Item	Description
1	PSU fan exhaust
2	Power cord connector
3	PSU retention latch
4	PSU handle
5	DC power status LED
6	PSU status LED
7	AC power status LED



Note: There are no field-serviceable parts in the PSU. If a PSU unit fails for any reason, replace it. See [Replacing a power supply unit \(on page 76\)](#) for information about replacing a power supply.

Table 17 DC power status LED (green)

Status	Meaning
Green	DC output operating normally
Off	DC output not operating

If the DC Power status LED is off, unplug the power cable, wait 10 seconds, then reconnect the cable. If the DC Power Status LED remains off, the PSU has failed and must be replaced.

Table 18 PSU status LED (amber)

Status	Meaning
Off	PSU operating normally
Amber	PSU internal failure (over temperature, fan, or internal component)

If the PSU status LED is on, unplug the power cable, wait 10 minutes, then reconnect the cable. If the PSU Status LED remains off, the PSU has failed and must be replaced. See [Replacing a power supply unit \(on page 76\)](#) for more information on replacing a PSU.

Table 19 AC power status LED (green/amber)

Status	Meaning
Green	Receiving AC power and operating normally
Off	Not receiving AC power (check mains and power cable connections)

Mains power connections are an IEC inlet in each power supply. Each PSU is only powered from its mains inlet. Two power feeds are required for the system. PSU units do not have an on/off switch. To turn on power, simply connect the power cable. To turn off the unit, remove the power cable.

When both PSUs are installed, if only one PSU is connected and receiving adequate power, the fans on both PSUs will operate, but only the PSU receiving power will provide power to the server.

Each power supply auto-ranges over an input range of 100V to 240V AC, 50 Hz to 60 Hz.



Caution: If the server is non-responsive, see [Restarting an unresponsive server \(on page 80\)](#). Do not pull the power cord.

Ethernet management ports 0 and 1

Ethernet management ports 0 and 1 are standard 10/100/1000 Ethernet ports that are used to connect to the server for management purposes. Two LAN ports (eth0 and eth1) are located on the I/O back panel of the motherboard. Each Ethernet LAN port has two LEDs.

The green LED indicates activity, while the other link LED may be green, amber, or off to indicate the speed of the connection.

Refer to the following tables for more information.

Table 20 eth0/eth1 Activity LED (Right) LED State

LED Color	Status	Definition
Green	Flashing	Active

Table 21 eth0/eth1 Activity LED (Left) LED State

LED Color	Definition
Off	No connection/10 Mbps
Amber	1 Gbps
Green	100 Mbps

Serial port

A standard serial (RS-232) port, used to connect to the server for management purposes. See [RS-232 serial management port \(on page 62\)](#) for more information.

USB ports

Standard USB connectors. These ports are used to connect USB devices to the server during some operations.

Valid USB devices include:

- Flash drives
- External hard drives
- USB keyboards

Valid operations include:

- Management
- Install
- Upgrade
- Update
- Repair



Note: The USB ports should not be used without guidance from customer support.

In addition to eth0 and eth1, an IPMI LAN is also located on the I/O back panel. The amber LED on the right indicates activity, while the green LED on the left indicates the speed of the connection. Refer to the following table for more information.

IPMI port

In addition to eth0 and eth1, an IPMI LAN is also located on the I/O back panel. The amber LED on the right indicates activity, while the green LED on the left indicates the speed of the connection. Refer to the following table for more information.

Table 22 IPMI LAN LEDs

LED Color/State		Definition
Link (left)	▪ Green: Solid	▪ 100 Mbps
	▪ Amber: Solid	▪ 1 Gbps
Activity (right)	Amber: Blinking	Active

Management interfaces

The server panel features two types of physical management ports: RS-232 Serial (DB-9) and 10/100/1000 Ethernet (RJ45).

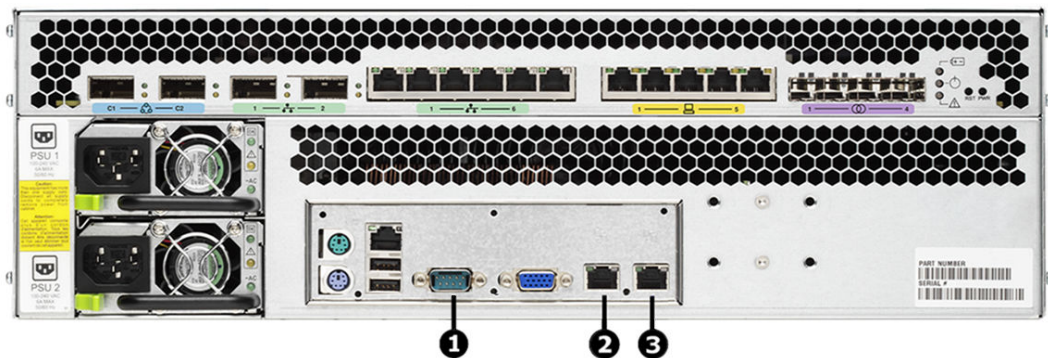


Figure 26 Management interface ports on rear panel - model 4040

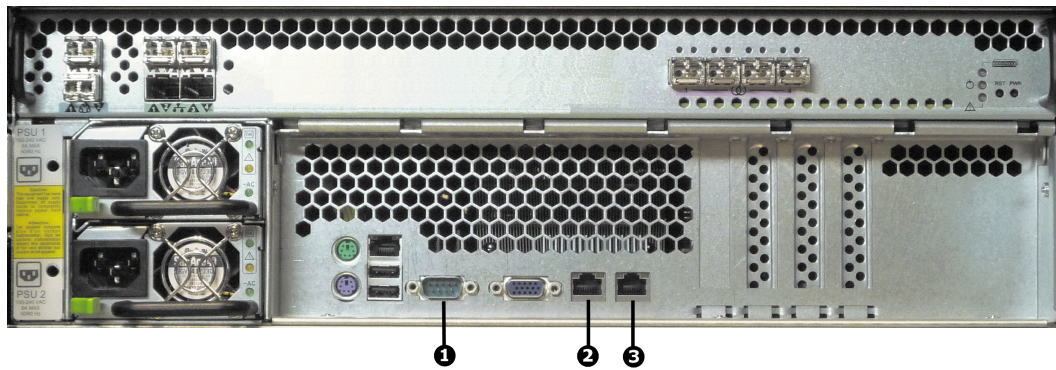


Figure 27 Management interface ports on rear panel - models 4060, 4080, and 4100

Item	Description
1	Serial management port (RS-232 DB-9 connector)
2	Ethernet management port 0 for customer facing management (RJ45 connector)
3	Ethernet management port 1 for private management (RJ45 connector)

RS-232 serial management port

The server has one RS-232 connection port, located on the rear panel of the server. This serial port is intended to be used during system setup. The serial port is not intended as a permanent management connection. This port should not be used as the primary management interface for the server. The primary management interface to the server is through the NAS Manager or through server's command line interface (CLI), which can be accessed through the network.

Any VT100 terminal emulation interface can be used to access to the CLI so that you can perform management or configuration functions. Connect the terminal to the serial port on the rear panel of the server, then set the host settings to the values shown in the following table to ensure proper communication between the terminal and the server.

Table 23 Host setting values

Terminal	Requirement
Connection	Crossover (null modem) cable
Emulation	VT100
Baud rate	115,200 Bps
Data bits	8
Stop bits	1

Terminal	Requirement
Parity	None
Flow control	None



Note: Once the initial setup has been completed, disconnect the serial cable. If you need to manage the server through a serial connection, connect to the serial port on the external SMU and use SSH to access the server's CLI. If your system does not include an external SMU, connect to the server's embedded SMU and use SSH to access the server's CLI.

10/100/1000 Ethernet management ports

The 10/100/1000 Ethernet management ports are used to connect the server or node to the customer facing management network and the private management network, or to connect directly to another device for management purposes.

The 10/100/1000 Ethernet ports operate at speeds of up to one (1) gigabit per second, and require the use of a standard RJ45 cable connector. Once connected, each GE port has two indicator LEDs; one on the top left and the second on the top right of the port.

These LEDs provide link status and network activity status information as described in the next table:

Left LED - Speed	Right LED - Link/Activity	Meaning
Off	Yellow (flashing)	10 Mbps link present
Green (not flashing)	Yellow (flashing)	100 Mbps link present
Orange (not flashing)	Yellow (flashing)	1 Gbps link present
Off	Off	No link

Ethernet cables

The HNAS 4040 model requires CAT6 cables that fully comply with the CAT6 SF/UTP standard for the 1000Base-T GE Ethernet network ports. Always use CAT6 cables that fully comply, such as those supplied by Harting.

See the following examples of Harting cables that comply with the standard:

Cable	Part number
CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 1 Meter	HARTING 09474747109
CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 2 Meter	HARTING 09474747111
CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 3 Meter	HARTING 09474747113
CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 5 Meter	HARTING 09474747115
CABLE ETHERNET PATCH LEAD CAT6 SF/UTP 10 Meter	HARTING 09474747121

Chapter 5: Replacing server components

This section describes which components are field replaceable units (FRUs) and how to replace them. This section also describes which components are hot-swappable.

Field-replaceable units

Some components are field-replaceable units (FRUs).



Important: The FRUs can only be replaced by certified engineers. These components are *not* customer replaceable units (CRUs).

FRUs include the following components:

- Hitachi NAS Platform or Hitachi Unified Storage File Module servers
- Bezels
- Hard disk drives (HDDs)
- Power supply unit (PSUs)
- NVRAM battery backup packs
- Fan assemblies
- SFP+ port adapters (HNAS 4060, 4080, and 4100)



Note: Main Motherboards (MMBs) and Main FPGA Boards (MFBs) are pre-installed boards that perform functions essential to the integrity of the server. If there is an issue with the MMB, or the MFB (typically), you must return the server for repair. MMBs are *not* FRUs, and, typically, MFBs are also *not* FRUs. However, an MFB may be replaced under certain specific circumstances. Contact Hitachi Vantara Support Connect to determine whether your MFB can be replaced as a FRU.

Some components are also hot-swappable. See [Hot-swappable components \(on page 65\)](#) for details.

Hot-swappable components

Some components are hot-swappable. Such components can be changed without shutting down the server.

Before replacing a component that is not hot-swappable, you must shut down and power off the server. See [Rebooting or shutting down a server \(on page 78\)](#) for details.

The HNAS 4040 model includes the following hot-swappable components:

- HDDs (see [Recovering or replacing a hard disk \(on page 75\)](#) for details)
- Power supply units (PSUs)
- NVRAM battery backup packs
- Fan assemblies

The HNAS 4060, 4080, and 4100 models include the following hot-swappable components:

- HDDs (see [Recovering or replacing a hard disk \(on page 75\)](#) for details)
- Power supply units (PSUs)
- NVRAM battery backup packs
- Fan assemblies
- SFP+ port adapters

Removing and replacing the front bezel

To access some server components or field replaceable units (FRUs), you must first remove the front bezel. Replace the bezel after the part replacement is complete.

Bezel removal

The server bezel is held onto the server chassis through a friction fit onto four retention posts, which are mounted to the chassis along the left and right edges of the chassis. There are no screws or other fasteners.

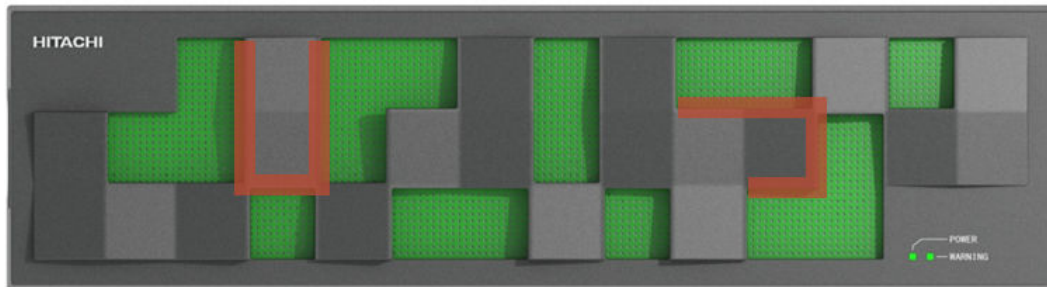


Figure 28 Server front plastic bezel with grasping areas

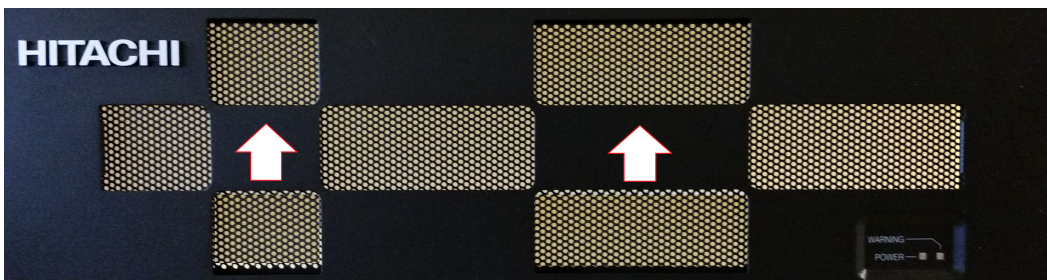


Figure 29 Server front metal bezel with grasping areas

Procedure

1. To remove the bezel, grasp the front of the bezel by the grasping areas.
2. Gently pull the bezel straight out away from the server.

Bezel replacement

Procedure

1. Place the bezel on the server, making sure that the bezel fits inside the outer edges of the chassis and that the retention posts and status LEDs are aligned.
2. Using the solid portions of bezel (near the edges), press the bezel straight into the server until it is firmly in place against the server chassis.

Replacing a fan

Replace a fan assembly, which is one of the server's hot-swappable components.

Procedure

1. Remove the front bezel. The fan assemblies will then be visible.
2. Identify the fan to be replaced.

Fans are labeled on the chassis, and are numbered 1 and 2, with fan 1 on the left and fan 2 on the right. Refer to the fan status LEDs on front panel of the server (behind the bezel) to see which fan has failed. In the following figure, number 1 indicates the status LED for fan 1 (the left-side fan), and number 2 indicates the status LED for fan 2 (the right-side fan).

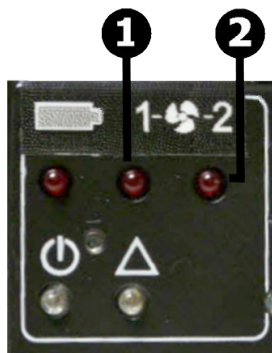


Figure 30 Fan status LEDs

Item	Description
1	Fan 1 status LED
2	Fan 2 status LED

3. Remove the faulty fan by loosening the thumbscrews (turning them counter-clockwise) until they are loose, then pulling the fan unit straight out of the chassis. (The fan lead connector disengages automatically as you remove the fan assembly.)



Figure 31 Fan assembly - model 4040



Figure 32 Fan assembly - models 4060, 4080, and 4100

4. Put the new fan assembly into place.
5. Gently press the fan assembly back into the chassis. The fan electrical connector will be aligned automatically when the fan is fully inserted into the chassis.
6. Secure the fan assembly in position by tightening the thumbscrews (turning them clockwise).
7. Replace the front bezel.

Replacing the NVRAM backup battery pack

To replace the NVRAM backup battery pack in a server, you remove the old battery and install the new replacement. Perform the battery pack replacement as quickly as possible, and only when the new pack is present.

The replacement NVRAM backup battery pack comes pre-assembled. Do *not* remove the batteries from the case.



Note: If possible, shut down the server before replacing the battery backup pack. Shutting down the server or migrating all of the EVSs to the other node is not required. However, during the replacement procedure, there will be a period of time when the NVRAM contents are not backed up by the battery pack. If a power failure occurs during this period, the NVRAM contents may be lost.

Checking battery pack status

The battery pack status LED indicates the status of the server's NVRAM battery pack.

Table 24 Battery pack status LED

LEDs	Meaning
Red	If this LED is on immediately after installing a new battery pack, it indicates that an initial battery charging and conditioning cycle is in progress. The initial battery conditioning takes approximately 24 hours, and the LED will turn off after the cycle is complete. If this LED is on during normal operation (not after installing a new battery pack), either the battery has exceeded its two year life or a problem has been detected. Check the battery status before determining any service operation.
Off	Normal operation.

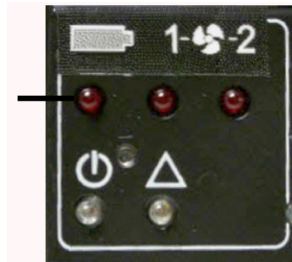


Figure 33 Battery pack status LED location

Battery-related events are recorded in the server's event log. Other battery-related information is also saved in a battery status log. These logs, along with the server's event log, are useful in monitoring the state of the battery.

Turning the battery status LED off can require one or more of the following steps. Try the steps in the following order:

Procedure

1. Perform a battery pack test cycle. To begin the test cycle, do the following:
 - a. Access the server CLI.
 - b. Issue the following Linux command: `touch /var/opt/chassis-monitor/.testbattery`
2. Remove and reinstall the battery pack.

3. If the battery is still having problems, replace the battery pack. (A new battery pack is required.)

Identifying a cluster node that requires battery replacement

If you have warnings or battery-related events in the Event Log of a cluster, you can identify the cluster node requiring battery replacement using the following procedure:

Procedure

1. Access the server Command Line Interface.
For information about how to access the server command line interface, refer to the *Hitachi NAS Platform System Access Guide*.
2. Log in to the server as manager.
These credentials provide access to the Bali console.
3. Enter the command `led-identify-node x`, where `x` is the node mentioned in the Event Log message.
Both the server status and fault LEDs on the node will flash, allowing you to identify the node. Refer to the *Hitachi NAS Platform Command Line Reference* for more information on the `led-identify-node` command.

Replacing the NVRAM battery module

You can easily replace the NVRAM battery pack in a server. The battery module is hot-swappable; however, if possible, shutdown the server before replacing the module.

Before you begin

Identify the server model before installing the battery.

The replacement battery module is pre-assembled. Do *not* remove the batteries from the case.



Important: During the replacement procedure, the NVRAM contents are not backed up by the battery pack. If a power failure occurs during this period, NVRAM contents may be lost. See the appropriate hardware reference or maintenance documentation for procedures to power down a server.

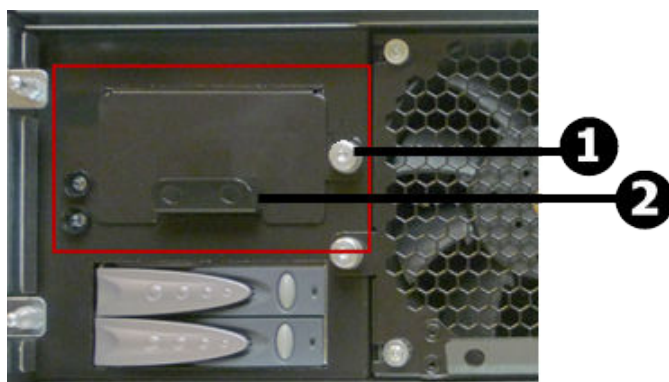


Figure 34 NVRAM battery module removal components - model 4040

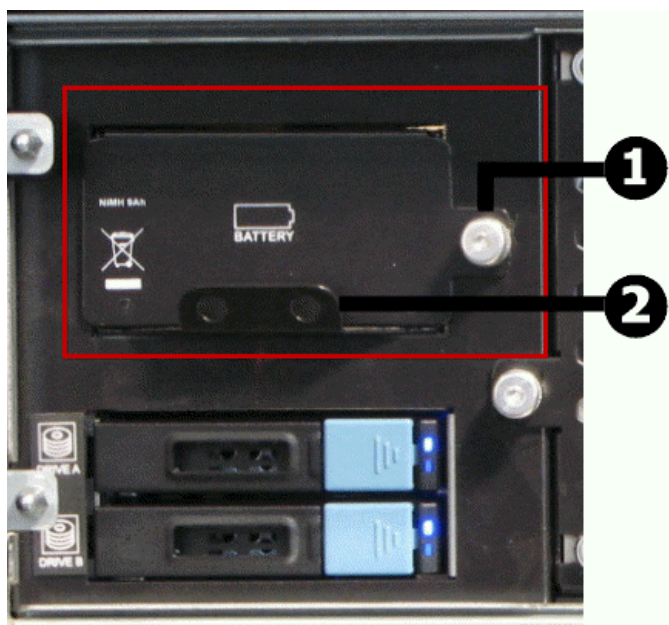


Figure 35 NVRAM battery module removal components - models 4060, 4080, and 4100

Item	Description
1	Thumbscrew that holds the battery pack in place
2	Handle for moving the battery pack forward and backward in the chassis

Procedure

1. Remove the bezel cover from the front of the server for access to the batteries.
2. Loosen the thumbscrew to the right of the battery pack module cover by turning it counter-clockwise.
3. Using the handle, pull the battery pack module straight out of the chassis.
The battery pack is automatically disconnected.

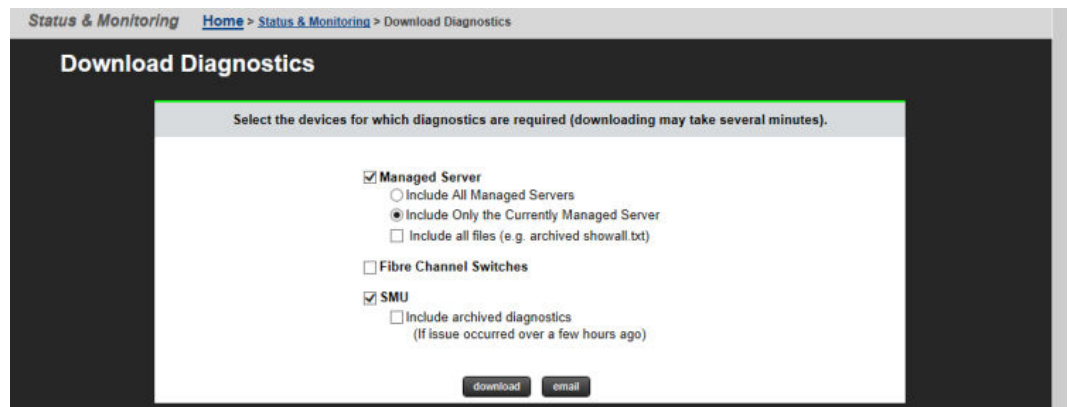
4. Insert the pre-assembled replacement module straight into the chassis, and gently but firmly push the pack into position.
The battery pack is automatically connected.
5. Tighten the thumbscrew by turning it clockwise.
6. Replace the server bezel.
7. Dispose of the old battery pack in accordance with environmental regulations or return to the supplier.

Collecting system backups and diagnostics

After replacing the battery, collect system backups and diagnostics.

Procedure

1. Connect to the back-end NAS Private Management Switch.
2. Open a browser session to the SMU. (External: 192.0.2.1; Embedded: 192.0.2.2).
3. Login as the admin user.
4. Back up the Server registry (Embedded SMU - this includes the SMU configuration).
 - a. Navigate to **Home > Server Settings > Configuration Backup and Restore**.
 - b. Click **Backup**.
 - c. Save the registry file to a location on your computer.
 - d. Verify that the archive file can be opened and the contents can be extracted.
5. Backup the SMU Configuration - External SMU ONLY.
 - a. In the GUI, navigate to **SMU Administration > SMU Backup and Restore**
 - b. Click **Backup SMU: Backup**.
 - c. Save the configuration file to a location on your computer.
 - d. Verify that the archive file can be opened and the contents can be extracted.
6. Collect Diagnostics from the cluster.
 - a. Navigate to **Home > Status and Monitoring > Download Diagnostics**
 - b. Check only the check boxes and radio button shown below .



- c. Click **download**.
- d. Save to a location on your computer.

- e. Verify that the archive file can be opened and the contents can be extracted.
- f. If the archive file contains the words "MISSING_FILES", repeat step 6. If this does not resolve the issue, then check that both nodes are fully operational and resolve any issues identified before repeating the procedure.

Resetting the battery age and restarting the chassis monitor

Reset the battery age and Restart the Chassis Monitor as necessary.

Procedure

1. Connect a serial cable to the serial port of the node with the new battery.
2. Open a putty application and set up a serial console session.
 - a. Select the **Serial Radio** button.
 - b. Enter the COM port that your serial dongle is using.
 - c. Enter 115200 in the **Speed** box.
 - d. Click **Serial** in the Category Tree on the left.
 - e. Make sure the Speed is 115200.
 - f. Set the Data bits to 8.
 - g. Set the Stop bits to 1.
 - h. Set the Parity to None.
 - i. Set the Flow Control to None.
 - j. Click **Session** in the Category Tree on the left.
 - k. Enter SMU serial (or similar) in the **Saved Sessions** box.
 - l. Click **Save**.
3. Turn on the putty session logging.
 - a. Click **Logging** from the Category Tree on the left.
 - b. Select **Printable output** in Session logging.
 - c. Set the location for the putty output file.
 - d. In the section **What to do if the log file already exists**, select **Ask the user every time**.
 - e. Click **Session** from the Category Tree on the left, which returns you to the Session window.
 - f. Click **Save**.
4. Click **Open** to open the session to the Node console.
 - a. Login as the manager user.
5. Type the command **ipaddr** and verify that you are connected to the correct node.
6. Perform ONLY ONE of the following procedures.
 - If the node firmware is **below** 11.1.3225.02, perform the following procedure:
 - a. Type the command: **new-battery-fitted --field --confirm**
 - b. Once the prompt returns, press: **<ctrl>+d** to exit to the Linux Layer.
 - c. Type **su** to change the login to root and enter the root password.

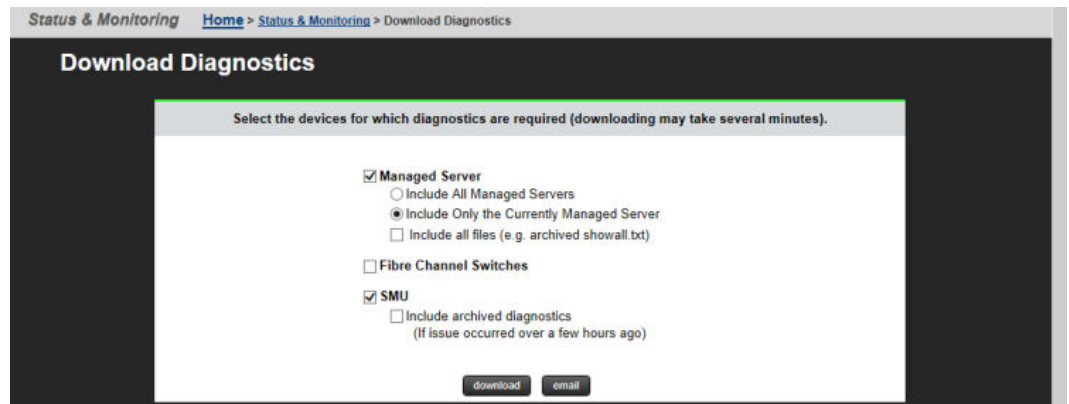
- d. Restart the chassis monitor by issuing the command: `/etc/init.d/chassis-monitor restart`
- e. Type `scc localhost` to return to the NAS prompt.
- If the node firmware is **at or later than** 11.1.3225.02 then perform the following procedure:
 - a. Type the command `new-battery-fitted --field --confirm`
- 7. Check the Battery Status.
 - a. Type the command `batt-log-show`; the output should show that the battery is fitted and initialization has started.
 - b. If the battery is not showing fitted or initialization does not start, call Customer Support for resolution.

Collecting a final diagnostic

Collect a final diagnostic as the last step in battery replacement.

Procedure

1. Open a browser session to the SMU. (External: 192.0.2.1; Internal: 192.0.2.2).
2. Login as the admin user.
3. Collect Diagnostics from the cluster.
 - a. Navigate to **Home > Status and Monitoring > Download Diagnostics**
 - b. Check only the checkboxes and radio button shown below.



- c. Click **download**.
- d. Save to a location on your computer.
- e. Verify that the archive file can be opened and the contents can be extracted.
- f. If the archive file contains the words "MISSING_FILES", repeat step 3. If this does not resolve the issue, then check that both nodes are fully operational and resolve any issues identified before repeating the procedure.
- g. Upload both the diagnostic taken in the beginning of the procedure and this diagnostic to TUF using the SR for the battery replacement.

Recovering or replacing a hard disk

Some hard disk drive failures require disk replacement, others only require performing a recovery process. Use the recovery process to help ensure that all partitions are recovered before proceeding with any further disk recovery or replacement procedures. Unless you are certain the hard disk has failed, perform a disk recovery.



Important: Do not attempt to replace or recover a hard disk without the assistance of Hitachi Vantara Customer Support. For the latest procedure, please refer to Support Connect article [How_to_Replace_a_Chassis_Hard_Disk_in_an_HNAS_Gateway_Node](#) (which is only visible to Service Partners and Employees).

Hard disks can fail for a number of reasons, including corrupt sectors or erroneous blocks of data. Typically, the RAID controller handles these types of errors and they do not cause the server to fail.

More serious errors may cause a disk failure, causing one or both hard disks to fall out of the RAID. Should one partition of a disk fail, attempt a disk recovery. If a partition fails repeatedly, replace the hard disk. If all the partitions fall out of RAID, replace the failed drive.



Caution: When removing a hard disk, take extreme care to only press one HDD lever. The push button latch mechanisms are close together and, if not careful, both latches can easily be depressed at one time. *This causes an immediate loss of access.*



Important: Before you consider replacing a hard disk drive, be sure you understand the following points:

- Failed hard disks are hot-swappable, so a failed hard disk can be replaced without shutting down the server. However, there are serious risks in trying to swap a drive that is *not* failed.
- Do *not* assume that because the red LED is illuminated that a drive is faulty. Under a RAID rebuild/recovery, the red LED would be illuminated. If the drive is failed and needs replacing, you can remove it from the server.
- Do *not* replace a drive that has not actually failed. If the disk shows signs of failure, shut down the server before replacing the drive and restarting the server.
- There should be no reason to pull out a hard drive while it is in a known good configuration, and doing so can potentially lead to data corruption.
- Unless you are certain the hard disk has failed, perform a disk recovery.
- Disk redundancy is unsupported while the disk is removed from the server.
- The new disk does not have to be the same capacity as the disk that is being replaced.



WARNING: It is strongly recommended to perform disk replacement procedures during a maintenance window in order to minimise risk of any disruption caused by the procedure and to allow for the movement of EVSs and other unexpected events that may occur.

Replacing a power supply unit

You can replace a power supply unit (PSU) as a hot-swappable server component. The server can operate on a single PSU if necessary, making it possible to replace a failed PSU without shutting down the server. If a PSU fails, it should be replaced as quickly as possible, because operating on a single PSU means that there is no redundancy in that area, increasing the risk of an interruption in service to clients.

LED indicators on each PSU indicate the PSU status.



Caution: You cannot use the power supply from an HNAS 4060, 4080, and 4100 server in an HNAS 4040. The HNAS 4040 server uses the same PSU as the HNAS 3080 and 3090 servers.



Note: Although the following figure shows the HNAS 4060, 4080, and 4100 rear panel, the PSU locations are the same on the HNAS 4040 model.

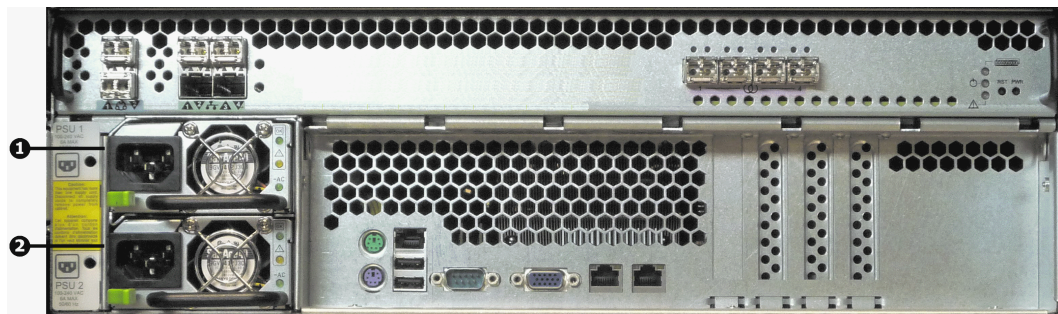


Figure 36 PSU locations on NAS Platform Series 4000 rear panel

Item	Description
1	PSU 1
2	PSU 2

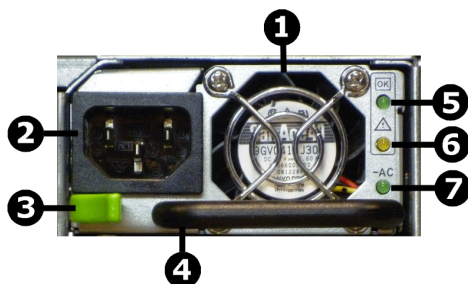


Figure 37 PSU components

Item	Description
1	PSU fan
2	Power plug
3	Retaining latch
4	Handle
5	DC power LED
6	Malfunction or failure LED
7	AC power LED

Procedure

1. Remove the power cord from the PSU.
2. Move the retaining latch to the right (you may hear a slight click if the PSU moves when the latch disengages).
3. Using the handle on the PSU, pull the PSU out from the back of the server until you can completely remove the PSU from the chassis.
4. Insert the replacement PSU. The retention latch should click into position all the way to the left when the PSU is fully inserted.
If the PSU that is not being replaced is receiving mains power when the replacement PSU is fitted, the fan on the replacement PSU becomes active.
5. Connect the power cord to the back of the PSU.
The PSU should start as soon as the power connection is made. If the PSU does not start immediately, make sure the mains power circuit is live and that the other end of the power cable is connected to a live outlet.

Chapter 6: Rebooting, shutting down, and powering off

This section provides instructions on how to reboot, shut down, and power off a server or cluster.

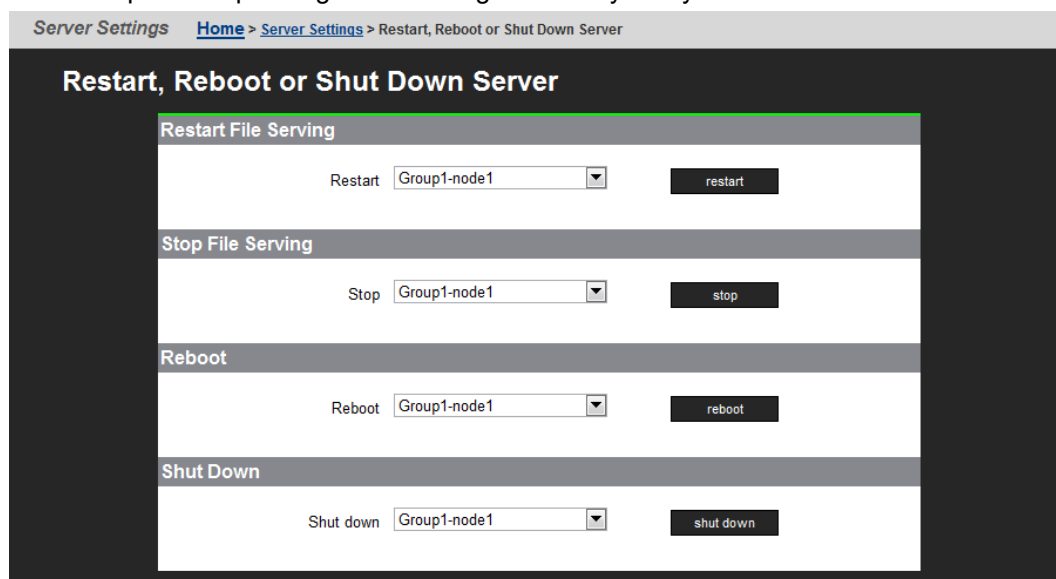
See the *System Installation Guide* for details about server software licenses.

Rebooting or shutting down a server

The server can be shutdown or reset if a manual reboot is necessary.

Procedure

1. Using NAS Manager, log in and select **Reboot/Shutdown** from the **Server Settings** page to display the Restart, Reboot and Shutdown page. Note that the page has different options depending on the configuration of your system.



Server Settings [Home](#) > [Server Settings](#) > Restart, Reboot or Shut Down Server

Restart, Reboot or Shut Down Server

Restart File Serving		
Restart	Group1-node1	restart
Stop File Serving		
Stop	Group1-node1	stop
Reboot		
Reboot	Group1-node1	reboot
Shut Down		
Shut down	Group1-node1	shut down

2. Click the button for the action you want to perform as described next:

- • Configuring cipher suites
- Configuring the SSL/TLS version
- Obtaining and importing a CA-signed certificate

Click **restart** to restart all file serving EVSs on the server.

- Click **stop** to stop file all serving EVSs on the server.
- Click **Reboot** to stop file serving EVSs on the server, and then reboot the entire server. Note that rebooting may take up to five minutes.
- Click **Shutdown** to stop file serving EVSs on the server, and then shut down and power off the server.

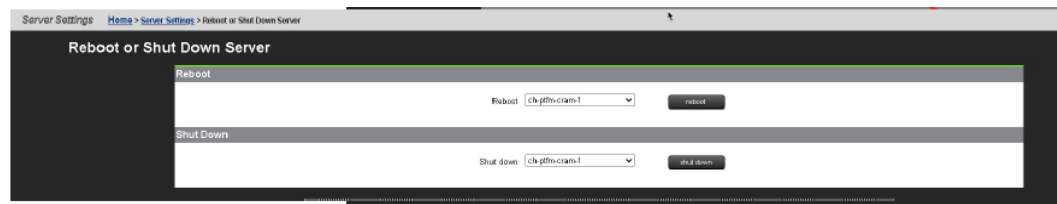
Rebooting or shutting down a server or cluster

Procedure

1. Using NAS Manager, log in and select **Reboot / Shut down** from the **Server Settings** page to display the Reboot or Shut Down Server page.



Note: The page has different options depending on the configuration of your system.



2. Click the button for the action you want to perform as described next:

Option	Action
Reboot	▪ To reboot a single node, use the drop-down list to select a node, and then click reboot. ▪ To reboot all cluster nodes simultaneously (sequentially), select the applicable drop-down option, then click reboot. Note: Clicking reboot stops all file serving EVSs on the selected node or all cluster nodes, then reboots the node/nodes. Rebooting may take up to five minutes.

Option	Action
Shutdown	- To shut down a single node, use the drop-down list to select a node, then click shut down. - To shut down all nodes at the same time, select all nodes simultaneously, and then click shut down.  Note: Clicking Shut down stops all file serving EVSs on the selected node or the cluster, then shuts down and powers off the selected node or all nodes in the cluster. The PSU is still powered on and the node is not ready for shipment.

Restarting an unresponsive server

Perform this process to restart an unresponsive server from the server operating system (OS) console. You generate a diagnostic log that can help you better understand the problems. You can gain access either by using SSH software to connect to the server's CLI or connecting to the server serial port.

Procedure

1. Connect to the SMU using the ssh software.
2. From the siconsole, select the server.
 - If the system fails to respond, go to step 3.
 - If the system takes you to the server OS console, issue the command: **bt active**, so you can view the display.
 - If you are still at the siconsole, select **q**, press **Return**, and then perform the following steps:
 - a. Connect directly to the MMB as manager using ssh.
 - b. If the connection succeeds, you are taken to the server OS console, where you issue the command: **bt active**
 - c. If the connection fails, continue to step 4.
3. Connect to the system with a serial null modem cable, and perform the following steps: See [Serial port \(on page 60\)](#) if you need details.
 - a. Login as manager or you will get the Linux prompt, not the server OS.
If you use root, use **ssc localhost**.
 - b. Issue the command: **bt active**
4. If you are still unable to get to the server OS, perform the following steps:
 - a. Check to make sure that the Bali CLI is booting successfully.
 - b. Log in through the serial cable connection.

- c. Tail `/var/opt/mercury-main/logs/dblog`
- d. Search the log for the entry `MFB.ini not found run nas-preconfig`.
 - If the entry is present, the system has been unconfigured by either running the `unconfig` script or removing the node from a cluster.
 - If the entry is not present, monitor the `dblog` during the boot cycle to see where it fails.



Warning: If the server is still unresponsive, do not pull the plug. Instead, see the next step. The reboot time varies from system to system. The reboot can take up to 20 minutes, because a dump is compiled during the reset process.

5. Check the green LED on the front panel of the server for the server status.

Table 25 Server status - model HNAS 4040

Server status LED	Meaning
Amber	Critical failure and server is not operational.
Slow green flash (every three seconds)	System has been shut down and you can remove the power.
Medium green flash (every .8 seconds)	Server needs attention, and a non-critical failure has been detected. For example, a fan or power supply has failed.
Off	Normal operation.

Table 26 Server status - models HNAS 4060, 4080, and 4100

Server status LED	Meaning
Solid green	System has rebooted and the server is online.
Slow green flash (every three seconds)	System has been shut down and you can remove the power.
Medium green flash (every 1.3 seconds, with the server online)	No enterprise virtual server (EVS) residing on the server.
Medium green flash (every .8 seconds)	Server is available.
Fast green flash (5 times per second)	Server is booting.

6. If the green LED is flashing 5 times per second, plug in the serial cable.
 - If the terminal screen is generating output, let the process complete.
 - If the terminal screen is blank, press the Reset button.



Note: Pulling the power cord from the server is *not* recommended. Do not pull the power cord unless it is absolutely necessary. First, complete the steps above.

Powering down the server

Follow this procedure whenever a server is about to be powered down for shipment or storage, and will be left off for more than a day. If the system is being restarted or power-cycled, this procedure is not required.

Contact your representative for special instructions if servers will be in storage for more than one year.

Procedure

1. From the NAS Platform operating system console, enter the command: `shutdown --powerdown`
2. Wait until the rear panel LEDs turn off.



Note: The PSUs continue to run and the PSU LEDs stay on.

3. Power down the server by removing the power cables from the PSU modules.

Powering on the server or cluster

To start/power on a server or cluster:

Procedure

1. Verify that all servers are switched off.
2. Start all storage systems, beginning with the expansion enclosures.

Wait until the disk LEDs on all of the expansion enclosures have stopped blinking (which indicates that they are spinning up) or two minutes, whichever comes first, then start the storage system RAID controller enclosures. Note that the disk drives in some storage enclosures do not spin up until commanded to do so by the RAID controller, so the LEDs may continue to blink until after the RAID controller enclosure has sent those commands and the drives have spun up.

3. For a cluster configuration, verify the virtual SMU has been installed and configured in the customer VMware or HyperV environment.
Wait one minute to allow the external SMU to start.
4. If you are starting a cluster, wait 5 - 10 seconds before powering on the next node in the cluster.

Recovering from power stand-by

When the server is in a power stand-by state, the power supplies are powered and the PSU LEDs are lit, but the Power Status LED on the rear panel is not.

The server enters a stand-by power state due to any the following conditions:

- The **shutdown --powerdown** command has been issued.
- The PWR button is pressed when the server is running.
- The server has shut down automatically due to an over-temperature condition.

You can restore the server to its normal power state by either of the following methods:

- Press the PWR button.
- Remove the power cables from both PSUs, wait for 10 seconds, then reconnect the cables to the PSUs.

Appendix A: Server replacement procedures

The replacement of the server as part of a field service process can take several forms depending on how the system was originally deployed. The typical field deployment scenarios documented for service replacement include:

- Two-node cluster using an external SMU for management-replacing only one node
- Two-node cluster using an external SMU for management-replacing both nodes



Important: This document does not treat migration scenarios between different configurations at the time of replacement.

Replacement procedure overview

This section provides information on the requirements and considerations for replacing nodes.

Server replacement requirements

Consider the following server replacement requirements:

- Much of the process required for a server replacement is the same as what is covered in installation and configuration training.
- Determine which replacement scenario is being encountered. The replacement process is different for each scenario.



Note: Replacement servers are shipped without an embedded system management unit (SMU), so you must install the SMU before you can connect to a stand-alone server.

You can use a keyboard, video, and mouse (KVM) device or a serial cable to connect to the serial port. Bring these with you just in case they are needed when the unit arrives. If you connect to the serial port, use the following SSH client settings:

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

Swapping components

The server can be replaced onsite, however, some components are not included in your replacement server. You must remove those components from the original server and use them in the replacement server. There are a minimum of three parts to be reused in the replacement server.

The components that can be swapped include:

- Power supplies
- Bezel
- Rack mounting guides
- SFP+ port adapters (HNAS 4060, 4080, and 4100)

Model selection

The Hitachi NAS Platform 4040 server has a unique chassis. The other three models of the Hitachi NAS Platform Series 4000 server share the same chassis: Hitachi NAS Platform 4060, Hitachi NAS Platform 4080, and Hitachi NAS Platform 4100. Models HNAS 4060 and HNAS 4080 are physically identical. From outside of the chassis, model HNAS 4100 is identical to the HNAS 4060 and HNAS 4080 models--it shares the same ports and connectivity. However, internally, the model HNAS 4100 uses a different MMB and MFB than the HNAS 4060 or the HNAS 4080.

The software for all server models is pre-loaded on the replacement server before it is shipped from either the factory or depot location.

If for any reason the model selection does not match that which is required for replacement, then an upgrade process may be required in the field.

To upgrade a model HNAS 4060 to a model HNAS 4080, you add a license. You cannot upgrade a model HNAS 4060 or model HNAS 4080 to a model HNAS 4100.

In a HNAS 4080 cluster configuration, when the node joins the cluster, the node software automatically upgrades from HNAS 4060 to HNAS 4080.

The upgrade process is outside the scope of this document and documented separately. Contact Hitachi Vantara Support Connect for upgrade information.

MAC ID and license keys

The replacement server has a new MAC ID, which means that you are required to have new license keys regardless of whether you are replacing a single node or a complete cluster.

As part of the field replacement process, Hitachi Vantara recommends that you obtain temporary keys to enable quick delivery and implementation. However, any temporary keys must eventually be replaced with a permanent key. This is required for all field scenarios, except when replacing a single node in a cluster.



Note: If the scenario is a single node or an all-cluster node replacement, use the `span-allow-access` command to attach the storage when the MAC ID changes.

Previous backups

A system backup preserves two critical components of information:

- SMU configuration
- Server configuration

The backup form for an embedded SMU is different than one from an external SMU. Depending on the replacement scenario severity, different limitations might exist for the system recovery.



Important: It is assumed that customers are frequently establishing backups somewhere safely off the platform for recovery purposes. If there is no backup, and the system to be replaced is nonfunctional, a manual recovery process is required to re-establish a functional system. The duration of this manual recovery is directly related to the complexity of the original configuration. All data and file systems are preserved independent of a backup.

Upgrades

Replacement servers can be down or above a revision, and not at the expected level of firmware required at the customer site. An upgrade is typically required during the replacement process, which is not covered in this document. It is assumed that all services personnel performing a replacement have already been trained, and know where to get this information within their respective organization.

Manually installing an embedded SMU (if necessary)

HNAS 3080/3090 spare or replacement units are shipped without the embedded SMU installed.

Before you begin

The SMU software will need to be manually installed in the following case:

- If the HNAS (all versions) is a spare/replacement and the field installer requires the embedded SMU to configure the replacement prior to adding to a cluster (or replacing a single node that has no external SMU). However, once added to the cluster, the embedded SMU should be uninstalled (`smu-uninstall` from the CLI of the newly added node). Note, when added to a cluster, the external SMU will disable the embedded SMU on the replacement node, but it is recommended to fully uninstall the embedded SMU.

Procedure

1. Obtain a copy of the *SMUsetup.iso* file and copy the file into /tmp
`scp /tmp/SMUsetup.iso`

2. As 'root' on the node:

```
cd /tmp
mount -o loop SMUsetup.iso /mnt/cdrom
/mnt/cdrom/autorun
```



Note: SMU iso images can be downloaded from Support Connect.

Replacing a single server with an embedded SMU

If a single server with an embedded SMU is non-functioning, and does not have a recent backup saved off platform, then a challenging and manual recovery process is necessary. If this circumstance is encountered, call the support organization for a copy of the system's latest diagnostics files. If available, these files can be used as a guide in reestablishing the system manually. The data and file systems will remain intact independent of the replacement and without a backup.



Note: Replacement servers are shipped without an embedded system management unit (SMU), so you must have a SMU installed before you can connect to a standalone server.



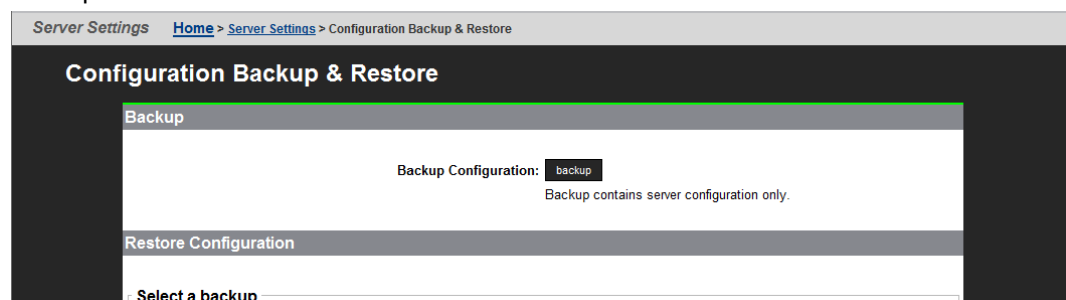
Important: Set expectations up front with the customer that this will delay time to recovery, and that some aspects of the systems configuration might never be recovered.

Obtaining backups, diagnostics, firmware levels, and license keys

On the old server:

Procedure

1. If the server is online, using NAS Manager, navigate to **Home > Server Settings > Configuration Backup & Restore**, click **backup**, and then select a location to save the backup file.



Ensure you save the backup file to a safe location off platform so that you can access it after the storage system is offline.

The backup process performed by the embedded SMU will automatically capture both the SMU and server configuration files in one complete set.

2. Navigate to **Home > Status & Monitoring > Diagnostics download** to download the diagnostic test results.

Status & Monitoring [Home](#) > [Status & Monitoring](#) > Download Diagnostics

Download Diagnostics

Select the devices for which diagnostics are required (downloading may take several minutes).

☒ **Managed Server**

- ☒ Include All Managed Servers
- ☐ Include Only the Currently Managed Server
- ☐ Include all files (e.g. archived showwall.txt)

☒ **Fibre Channel Switches**

☒ **SMU**

- ☒ Include archived diagnostics
(If issue occurred over a few hours ago)

[download](#) [email](#)

3. Navigate to **Home > SMU Administration > Upgrade SMU** to verify SMU type and firmware release level.
Both the server and SMU firmware versions must match those on the failed server; otherwise, the server cannot properly restore from the backup file. See the release notes and the *Hitachi NAS Platform and Hitachi Unified Storage File Module System Installation Guide* for release-specific requirements.
4. Navigate to **Home > Server Settings > Firmware Package Management** to verify the existing server (SU) firmware release level.

Server Settings [Home](#) > [Server Settings](#) > Firmware Package Management

Firmware Package Management

Filter

☐ Include System Patch Packages [filter](#)

Node View

Cluster Node	Status	Current Package	Default Package	Free Space	
ID (Name)					
1 (Group1-node1)	Online	12.1.3600.00	12.1.3600.00	293.77 GB (97 %)	details
2 (Group1-node2)	Online	12.1.3600.00	12.1.3600.00	297.36 GB (97 %)	details

Actions: [restart cluster file serving](#) [restart file serving on node](#) | [upload package](#)

Package View

Package	Present On Cluster Nodes	Install Status
☐ nas-11.3.3434.01.tar	1, 2	● OK
☐ nas-11.2.3319.06.tar	1, 2	● OK
☐ nas-11.2.3319.09.tar	1, 2	● OK
☐ nas-11.1.3225.00.tar	1, 2	● OK
☐ nas-12.1.3600.00.tar	1, 2	● OK
☐ nas-12.0.3525.00.tar	1, 2	● OK
☐ nas-12.0.3528.01.tar	1, 2	● OK

Actions: [delete](#) [set as default on all nodes](#)

5. Navigate to **Home > Server Settings > License Keys** to check the license keys to ensure you have the correct set of new license keys.

Shutting down the server you are replacing

On the server that you are replacing:

Procedure

1. From the server console, issue the command: **shutdown --ship --powerdown**

Wait until the console displays `Information: Server has shut down`, and the rear panel LEDs turn off. The PSU and server fans continue to run until you remove the power cables from the PSU module. See the appropriate system component section for more information.



Note: This specific **powerdown** command prepares the system for both shipping, and potential long-term, post-replacement storage.

2. Unplug the power cords from the power supplies.
3. Wait approximately 15 seconds, and then confirm the NVRAM status LED is off. If the LED is flashing or fixed, press and hold the **reset** button for five seconds until the LED starts flashing. The battery disables when you release the **reset** button.
4. Use the following rear panel figure and table to identify and label the cabling placement on the existing server.

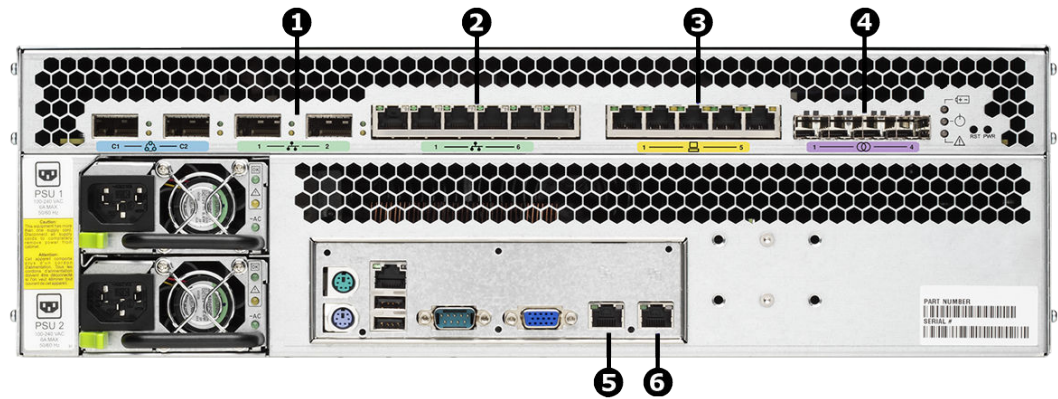


Figure 38 Rear view of server - model 4040

Item	Labels	Ports	Connections
1	1 — 2	1	Customer data network
		2	Customer data network
2	1 — 6	1	Gigabit Ethernet network port
		2	Gigabit Ethernet network port
		3	Gigabit Ethernet network port
		4	Gigabit Ethernet network port
		5	Gigabit Ethernet network port
		6	Gigabit Ethernet network port
3	1 — 5	1	10/100 Private management network Ethernet port
		2	10/100 Private management network Ethernet port
		3	10/100 Private management network Ethernet port
		4	10/100 Private management network Ethernet port
		5	10/100 Private management network Ethernet port
4	1 — 4	1	Storage or FC switch
		2	Storage or FC switch

Item	Labels	Ports	Connections
		3	Storage or FC switch
		4	Storage or FC switch
5		0	Customer facing management network
6		1	Private management network

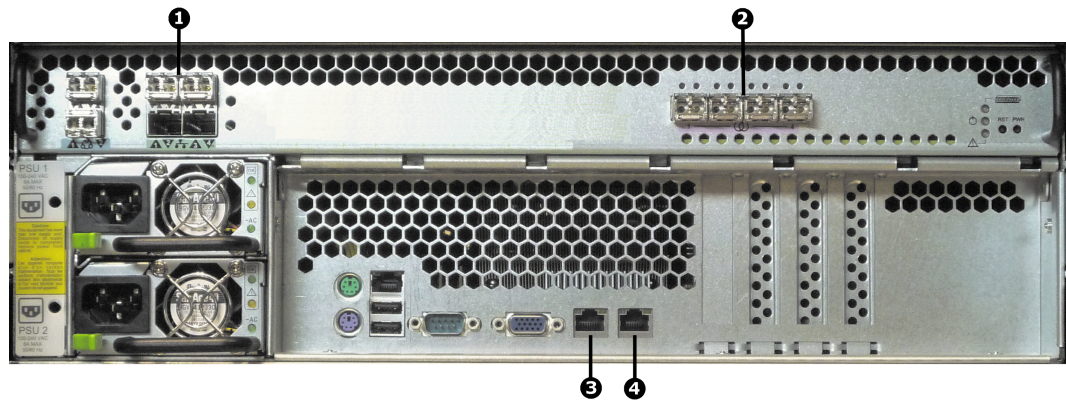


Figure 39 Rear view of server - models HNAS 4060, 4080, and 4100

Item	Labels	Ports	Connections
1		1	Customer data network
		2	Customer data network
		3	Customer data network
		4	Customer data network
2		1	Storage or FC switch
		2	Storage or FC switch
		3	Storage or FC switch
		4	Storage or FC switch
3		0	Customer facing management network
4		1	Private management network

5. If cables are not labeled, label them before removing them from the server.
6. Remove all cables from the server, and remove the server from the rack.
7. Remove the rail mounts from the old server, and install them on the new server.
8. Remove the battery from the old server, and install it in the new server.
9. Remove the bezel from the old server, and install it on the new server.
10. Insert the new server into the rack, and connect the power cords to the power supplies.



Note: Do not make any other cable connections at this time.

Configuring the replacement server

Before you begin

Obtain the necessary IP addresses to be used for the replacement server. Servers shipped from the factory have not yet had the `nas-preconfig` script run on them, so a replacement server will not have any IP addresses pre-configured for your use. You need IP addresses for the following:

- 192.0.2.200/24 eth1 (cluster IP)
- 192.0.2.2/24 eth1 (testhost private IP)
- 192.168.4.120/24 eth0 (testhost external IP, which might vary)

When you run the `nas-preconfig` script, it reconfigures the server to the previous settings. This step allows the SMU to recognize the server as the same and allows it to be managed. Reconfigured settings:

- IP addresses for Ethernet ports 0 and 1
- Gateway
- Domain name
- Host name

On the replacement server:

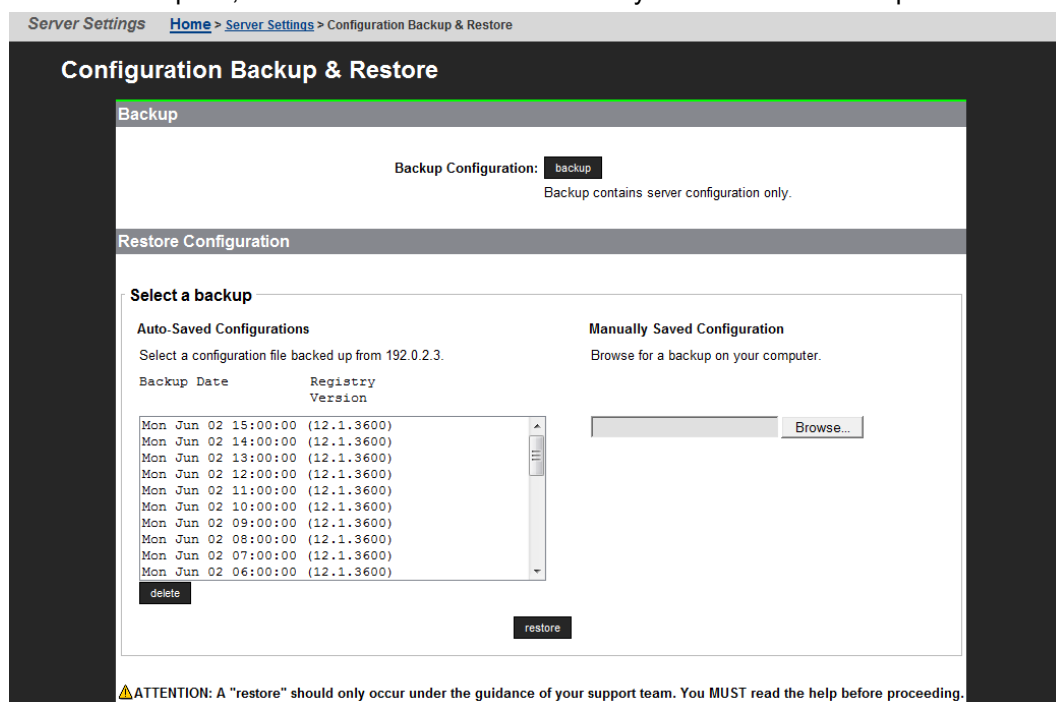
Procedure

1. Log in to the server.
2. Run the `nas-preconfig` script.
3. Reboot if you are instructed to by the script.
4. Log in to the SMU using one of the IP addresses you obtained.
5. Use a KVM (keyboard, video, and mouse) or a serial cable to connect to the serial port on the server.

Alternatively, you can connect by way of SSH using the following settings:

- 115,200 b/s
 - 8 data bits
 - 1 stop bit
 - No parity
 - No flow control
 - VT100 emulation
6. Log in as `root` and enter `ssc localhost` to access the BALI level command prompt.
 7. Enter `evs list` to obtain the IP configuration for the server.
 8. Using a supported browser, launch the NAS Manager using either of the IP addresses acquired from the EVS list output.
 9. Click **Yes**, and log in as `admin`.

10. Verify and, if necessary, convert the new server to the model profile required.
This step requires a separate process, training, and license keys. Contact Hitachi Vantara if the incorrect model arrives for replacement.
11. Navigate to **Home > SMU Administration > Upgrade SMU** to verify and, if necessary, upgrade the embedded SMU to the latest SMU release.
12. Navigate to **Home > Server Settings > Firmware Package Management** to verify and, if necessary, upgrade the new server to the latest SU release.
13. Navigate to **Home > Server Settings > Configuration Backup & Restore**, select the desired backup file, and click **restore** to restore the system from that backup file.



14. Reboot the server.
15. Reconnect the data cables to the server.

Finalizing and verifying the replacement server configuration

The Fibre Channel (FC) link speed varies according to the server model. Use the appropriate speed for your model.

Model	Fibre Channel link speed
HNAS 4040	4 Gbps
HNAS 4060, 4080, and 4100	8 Gbps

On the replacement server:



Note: The following steps show the FC link speed as 8 Gbps as an example.

Procedure

1. Navigate to **Home > Server Settings > License Keys** to load the license keys.
2. Remove the previous license keys in the backup file, and add the new keys.
3. Use **fc-link-speed** to verify and, if necessary, configure the FC port speed as required.; for example:



Note: The examples shows the link speed setting for models HNAS 4060, 4080, and 4100 .

- a. Enter **fc-link-speed** to display the current settings.

```
host:$ fc-link-speed
FC 1:      8 Gbps
FC 2:      8 Gbps
FC 3:      8 Gbps
FC 4:      8 Gbps
```

- b. Enter **fc-link-speed -i port_number -s speed** for each port.

```
host:$ fc-link-speed -i 1 -s 8
Set interface 1 link speed OK
FC 1:      8 Gbps
host:$ fc-link-speed -i 2 -s 8
Set interface 2 link speed OK
FC 2:      8 Gbps
host:$ fc-link-speed -i 3 -s 8
Set interface 3 link speed OK
FC 3:      8 Gbps
host:$ fc-link-speed -i 4 -s 8
Set interface 4 link speed OK
FC 4:      8 Gbps
```

- c. Enter **fc-link-speed** to verify the settings.

```
host:$ fc-link-speed
FC 1:      8 Gbps
FC 2:      8 Gbps
FC 3:      8 Gbps
FC 4:      8 Gbps
```

4. Use the **fc-link-type** command to configure the server in fabric (N) or loop (NL) mode.
5. Modify zoning and switches with the new WWPN, if you are using WWN-based zoning. If you are using port-based zoning, the no modifications are necessary for the switches configurations.
6. Open Storage Navigator and reconfigure LUN mapping and host group on the storage system that is dedicated to the server with the new WWPNs. Perform this step for every affected server port.

7. If the server does not recognize the system drives, enter **fc-link-reset** to reset the fiber paths.
8. Enter **sdpath** to display the path to the devices (system drives) and which hport and storage port are used.
9. Enter **sd-list** to verify the system drives statuses as OK and access is allowed.
10. Enter **span-list** to verify the storage pools (spans) are accessible.



Note: In this instance, *cluster* is synonymous with the standalone server.

11. Enter **span-list-cluster-uuids** *span_label* to display the cluster serial number (UUID) to which the storage pool belongs.
The UUID is written into the storage pool's configuration on disk (COD). The COD is a data structure stored in every SD, which provides information how the different SDs are combined into different stripesets and storage pools.
12. Enter **span-assign-to-cluster** *span_label* to assign all the spans to the new server.
13. Verify the IP routes, and enable all the EVSs for file services in case they are disabled.
14. Reconfigure any required tape backup application security.
15. Navigate to **Home > Status & Monitoring > Event Logs**, and click **Clear Event Logs**.
16. Navigate to **Home > Status & Monitoring > System Monitor** and verify the server status:
 - If the server is operating normally, and is not displaying any alarm conditions, run a backup to capture the revised configuration, and then download another diagnostic to support. Permanent license keys for the replacement server are normally provided within 7 days.
 - If the server is not operating normally for any reason, contact support for assistance.
17. Confirm all final settings, IP addresses, customer contact information, service restarts, client access, and that customer expectations are all in place. Features such as replication and data migration should all be confirmed as working, and all file systems and storage pools should be online.

Replacing a single server with an external SMU

Note that if it is a single server with an external SMU that is nonfunctioning, and does not have a recent backup saved off platform, then a challenging and manual recovery process is necessary. If this circumstance is encountered, call the support organization for a copy of the system's latest diagnostics files, if available, to be used as a guide in reestablishing the system manually. The data and file systems will remain intact independent of the replacement and without a backup.



Note: Replacement servers are shipped without an embedded system management unit (SMU), so you must have a SMU installed before you can connect to a standalone server.



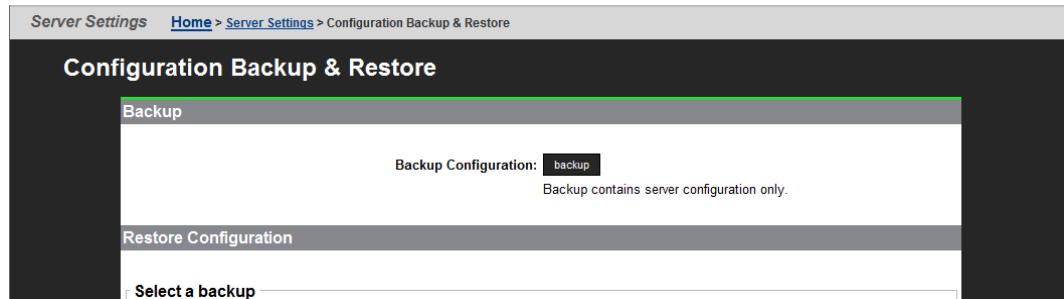
Important: Set expectations up front with the customer that this will delay time to recovery, and that some aspects of the systems configuration might never be recovered.

Obtaining backups, diagnostics, firmware levels, and license keys

On the old server:

Procedure

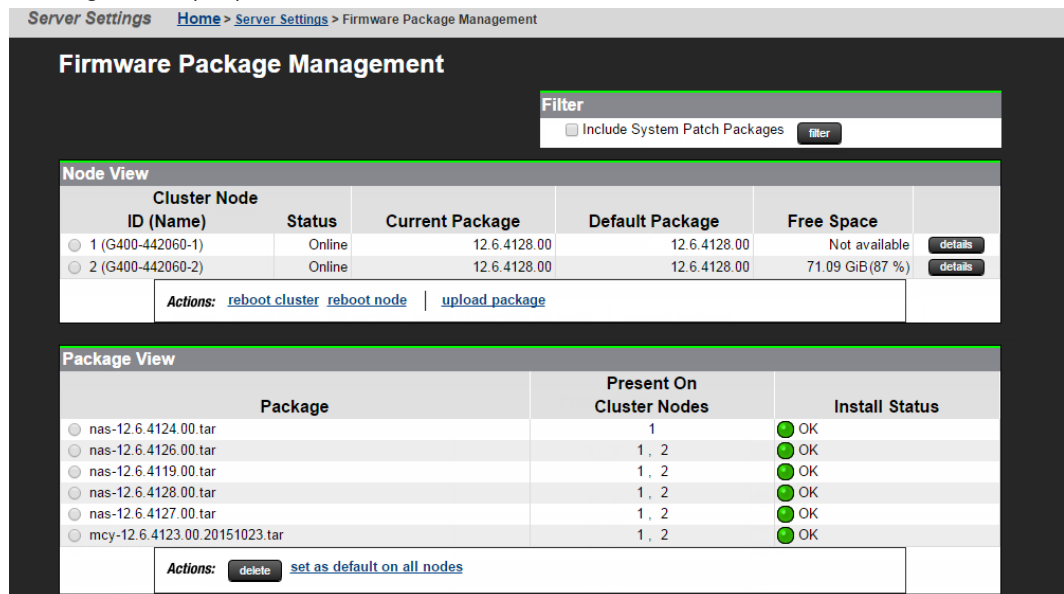
1. If the server is online, using NAS Manager, navigate to **Home > Server Settings > Configuration Backup & Restore**, click **backup**, and then select a location to save the backup file.



Ensure you save the backup file to a safe location off platform so that you can access it after the storage system is offline.

The backup process performed by the embedded SMU will automatically capture both the SMU and server configuration files in one complete set.

2. Navigate to **Home > Status & Monitoring > Diagnostics download** to download the diagnostic test results.
3. Navigate to **Home > Server Settings > Firmware Package Management** to verify the existing server (SU) firmware release level.



The server firmware version must match the failed server; otherwise, the server cannot properly restore from the backup file. See the release notes and system installation guide for release-specific requirements.

4. Navigate to **Home > Server Settings > License Keys** to check the license keys to ensure you have the correct set of new license keys.
5. Record the following information:
 - IP addresses for Ethernet ports 0 and 1
 - Gateway
 - Domain name
 - Host name

Shutting down the server you are replacing

On the server that you are replacing:

Procedure

1. From the server console, issue the command: **shutdown --ship --powerdown**

Wait until the console displays `Information: Server has shut down`, and the rear panel LEDs turn off. The PSU and server fans continue to run until you remove the power cables from the PSU module. See the appropriate system component section for more information.



Note: This specific **powerdown** command prepares the system for both shipping, and potential long-term, post-replacement storage.

2. Unplug the power cords from the power supplies.
3. Wait approximately 15 seconds, and then confirm the NVRAM status LED is off. If the LED is flashing or fixed, press and hold the **reset** button for five seconds until the LED starts flashing. The battery disables when you release the **reset** button.
4. Use the following rear panel figure and table to identify and label the cabling placement on the existing server.

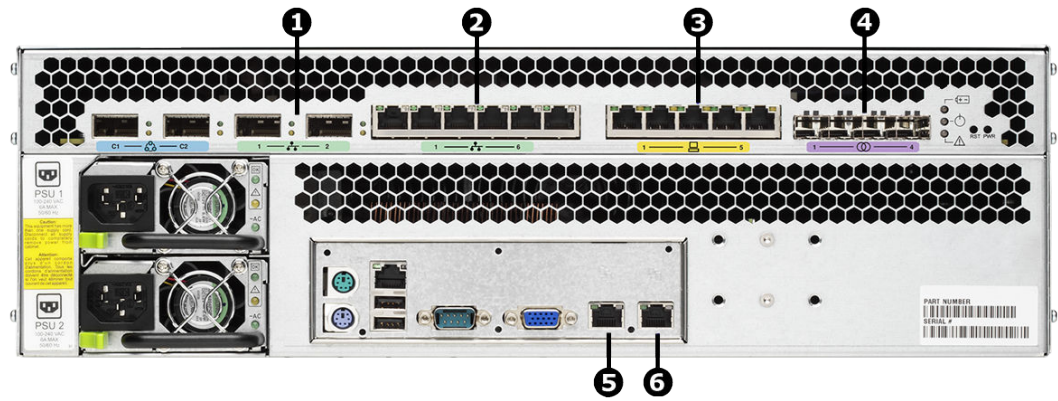


Figure 40 Rear view of server - model 4040

Item	Labels	Ports	Connections
1	1 — 2	1	Customer data network
		2	Customer data network
2	1 — 6	1	Gigabit Ethernet network port
		2	Gigabit Ethernet network port
		3	Gigabit Ethernet network port
		4	Gigabit Ethernet network port
		5	Gigabit Ethernet network port
		6	Gigabit Ethernet network port
3	1 — 5	1	10/100 Private management network Ethernet port
		2	10/100 Private management network Ethernet port
		3	10/100 Private management network Ethernet port
		4	10/100 Private management network Ethernet port
		5	10/100 Private management network Ethernet port
4	1 — 4	1	Storage or FC switch
		2	Storage or FC switch

Item	Labels	Ports	Connections
		3	Storage or FC switch
		4	Storage or FC switch
5		0	Customer facing management network
6		1	Private management network

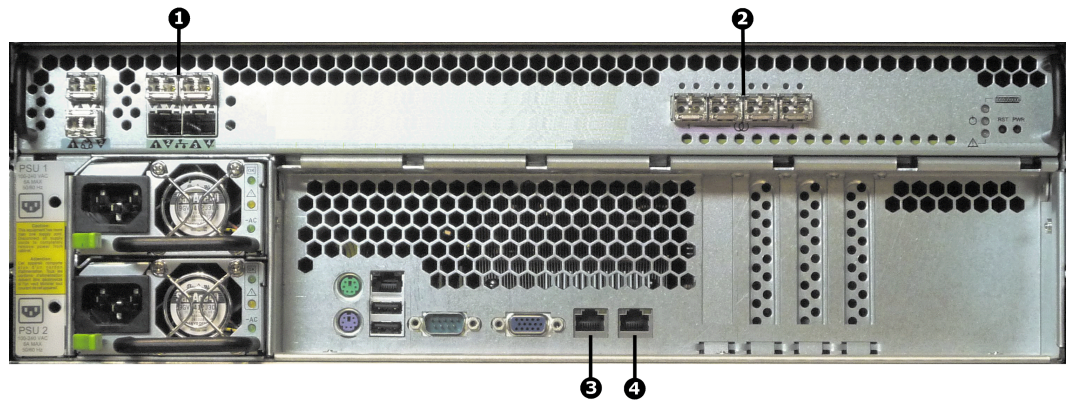


Figure 41 Rear view of server - models HNAS 4060, 4080, and 4100

Item	Labels	Ports	Connections
1		1	Customer data network
		2	Customer data network
		3	Customer data network
		4	Customer data network
2		1	Storage or FC switch
		2	Storage or FC switch
		3	Storage or FC switch
		4	Storage or FC switch
3		0	Customer facing management network
4		1	Private management network

5. If cables are not labeled, label them before removing them from the server.
6. Remove all cables from the server, and remove the server from the rack.
7. Remove the rail mounts from the old server, and install them on the new server.
8. Remove the battery from the old server, and install it in the new server.
9. Remove the bezel from the old server, and install it on the new server.
10. Insert the new server into the rack, and connect the power cords to the power supplies.



Note: Do not make any other cable connections at this time.

Configuring the replacement server

Before you begin

Obtain the necessary IP addresses to be used for the replacement server. Servers shipped from the factory have not yet had the `nas-preconfig` script run on them, so a replacement server will not have any IP addresses pre-configured for your use. You need IP addresses for the following:

- 192.0.2.200/24 eth1 (cluster IP)
- 192.0.2.2/24 eth1 (testhost private IP)
- 192.168.4.120/24 eth0 (testhost external IP, which might vary)

When you run the `nas-preconfig` script, it reconfigures the server to the previous settings. This step allows the SMU to recognize the server as the same and allows it to be managed. Reconfigured settings:

- IP addresses for Ethernet ports 0 and 1
- Gateway
- Domain name
- Host name

On the replacement server:

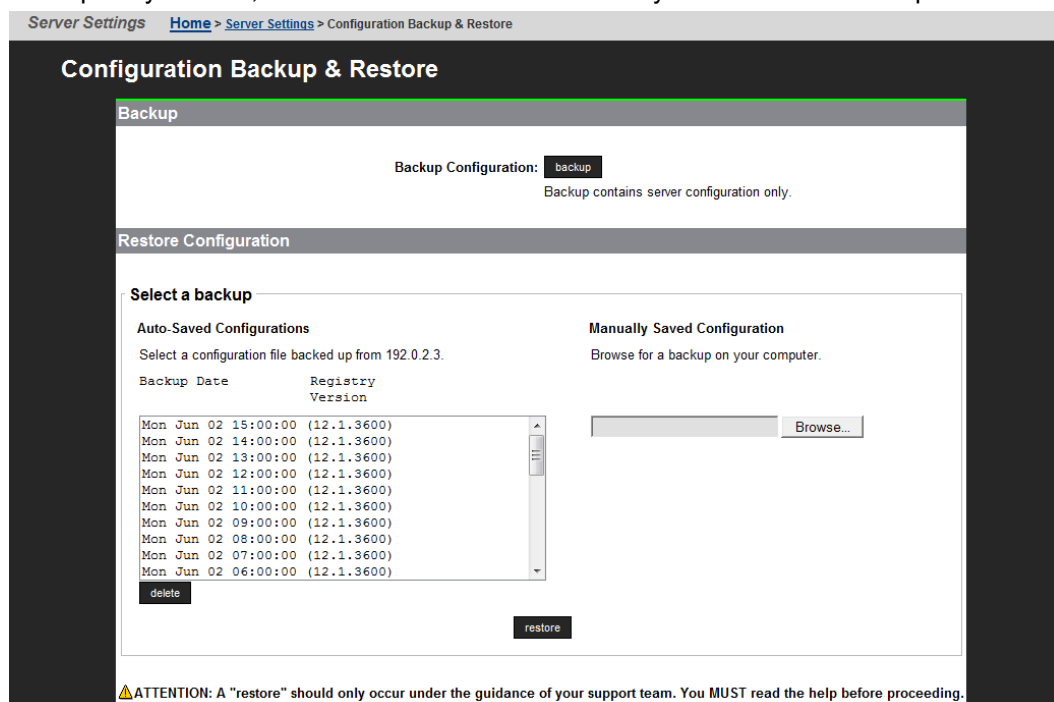
Procedure

1. Log in to the server.
2. Run the `nas-preconfig` script.
3. Reboot if you are instructed to by the script.
4. Log in to the SMU using one of the IP addresses you obtained once they can successfully connect using `ssc localhost`.
5. Use a KVM (keyboard, video, and mouse) or a serial cable to connect to the serial port on the server.

Alternatively, you can connect by way of SSH using the following settings:

- 115,200 b/s
 - 8 data bits
 - 1 stop bit
 - No parity
 - No flow control
 - VT100 emulation
6. Log in as `root`, and enter `ssc localhost` to access the BALI level command prompt.
 7. Enter `evs list` to obtain the IP configuration for the server.
 8. Using a supported browser, launch the NAS Manager using either of the IP addresses acquired from the EVS list output.
 9. Click **Yes** to proceed past the Security Alert, and log in as `admin`.

10. Verify and, if necessary, convert the new server to the model profile required.
This step requires a separate process, training, and license keys. Contact Hitachi Vantara Support Connect if the incorrect model arrives for replacement.
11. Navigate to **Home > Server Settings > Firmware Package Management** to verify and, if necessary, upgrade the new server to the latest SU release.
12. Navigate to **Home > Server Settings > Configuration Backup & Restore**, select the backup file you want, and click **restore** to restore the system from that backup file.



13. Reboot the server.
14. Reconnect the data cables to the server.
15. To uninstall the embedded SMU, log in as root and issue the command: `smu-uninstall`
16. Navigate to **Home > Server Settings > License Keys** to load the license keys.
17. Remove the previous license keys and add the new keys.

Finalizing and verifying the replacement server configuration

The Fibre Channel (FC) link speed varies according to the server model. Use the appropriate speed for your model.

Model	Fibre Channel link speed
HNAS 4040	4 Gbps
HNAS 4060, 4080, and 4100	8 Gbps

On the replacement server:



Note: The following steps show the FC link speed as 8 Gbps as an example.

Procedure

1. Navigate to **Home > Server Settings > License Keys** to load the license keys.
2. Remove the previous license keys in the backup file, and add the new keys.
3. Use **fc-link-speed** to verify and, if necessary, configure the FC port speed as required.; for example:



Note: The examples shows the link speed setting for models HNAS 4060, 4080, and 4100 .

- a. Enter **fc-link-speed** to display the current settings.

```
host:$ fc-link-speed
FC 1:      8 Gbps
FC 2:      8 Gbps
FC 3:      8 Gbps
FC 4:      8 Gbps
```

- b. Enter **fc-link-speed -i port_number -s speed** for each port.

```
host:$ fc-link-speed -i 1 -s 8
Set interface 1 link speed OK
FC 1:      8 Gbps
host:$ fc-link-speed -i 2 -s 8
Set interface 2 link speed OK
FC 2:      8 Gbps
host:$ fc-link-speed -i 3 -s 8
Set interface 3 link speed OK
FC 3:      8 Gbps
host:$ fc-link-speed -i 4 -s 8
Set interface 4 link speed OK
FC 4:      8 Gbps
```

- c. Enter **fc-link-speed** to verify the settings.

```
host:$ fc-link-speed
FC 1:      8 Gbps
FC 2:      8 Gbps
FC 3:      8 Gbps
FC 4:      8 Gbps
```

4. Use the **fc-link-type** command to configure the server in fabric (N) or loop (NL) mode.
5. Modify zoning and switches with the new WWPN, if you are using WWN-based zoning. If you are using port-based zoning, the no modifications are necessary for the switches configurations.

6. Open Storage Navigator and reconfigure LUN mapping and host group on the storage system that is dedicated to the server with the new WWPNs. Perform this step for every affected server port.
7. If the server does not recognize the system drives, enter `fc-link-reset` to reset the fiber paths.
8. Enter `sdpath` to display the path to the devices (system drives) and which hport and storage port are used.
9. Enter `sd-list` to verify the system drives statuses as OK and access is allowed.
10. Enter `span-list` to verify the storage pools (spans) are accessible.



Note: In this instance, *cluster* is synonymous with the standalone server.

11. Enter `span-list-cluster-uuids span_label` to display the cluster serial number (UUID) to which the storage pool belongs.
The UUID is written into the storage pool's configuration on disk (COD). The COD is a data structure stored in every SD, which provides information how the different SDs are combined into different stripesets and storage pools.
12. Enter `span-assign-to-cluster span_label` to assign all the spans to the new server.
13. Verify the IP routes, and enable all the EVSs for file services in case they are disabled.
14. Reconfigure any required tape backup application security.
15. Navigate to **Home > Status & Monitoring > Event Logs**, and click **Clear Event Logs**.
16. Navigate to **Home > Status & Monitoring > System Monitor** and verify the server status:
 - If the server is operating normally, and is not displaying any alarm conditions, run a backup to capture the revised configuration, and then download another diagnostic to support. Permanent license keys for the replacement server are normally provided within 7 days.
 - If the server is not operating normally for any reason, contact support for assistance.
17. Confirm all final settings, IP addresses, customer contact information, service restarts, client access, and that customer expectations are all in place. Features such as replication and data migration should all be confirmed as working, and all file systems and storage pools should be online.

Replacing a node within a cluster

Replacing a single node within a cluster assumes only two-node clusters and the presence of an external SMU, which acts as a quorum device. This helps to simplify the replacement process because a cluster preserves operational state of the entire system beyond any single node failure.

Because you are replacing an existing node from a cluster, you do not require any additional licenses, since the cluster will retain the licenses used from the existing node and the Cluster MAC-ID does not change, even if you are replacing node 1.

Capturing information from the existing node

To start, capture and record information from the existing node.

Procedure

1. Use the table below to record the information of the node to be replaced. This table will help you later during the node replacement process, by providing all the needed information.

Information of the node to be replaced	
Node Number	
Software Version	
ETH0 Node IP Address	
ETH0 Subnet Mask	
ETH1 IP Address (if applicable)	
WWN-Port 1	
WWN-Port 2	
WWN-Port 3	
WWN-Port 4	

2. How is the current node connected to the storage?

Direct Connected	SAN Connected
------------------	---------------

3. Is the storage using Host Group Security?

No	Yes
----	-----

Preparing the new node

Prepare the new node prior to installation.

Procedure

1. Obtain the HNAS Factory Reset code for the required level to be installed on the node.
2. Complete a factory reset of the new node per the documented procedure in order to install the node at the desired code level.

3. Run **nas-preconfig** on the node, entering the required information to allow BALI to start following a reboot of the new node.
For the Admin EVS, enter a valid IP address that is available for use temporarily. Once this node is joined to the cluster this address will be removed and the existing Admin IP address in the cluster will be used.
4. Ensure that the new node boots, and that you can connect to it via SSH and login to BALI.
5. Use the CLI **hport-wwn** command to get the WWN information for the new node.
Record the new WWN information for the new node.

WWN Information	
WWN-Port 1	
WWN-Port 2	
WWN-Port 3	
WWN-Port 4	

Preparing the old node for removal

Prepare the old node for removal before installing the new node.

Procedure

1. Backup the SMU.
2. Backup the Node Registry.
3. If the node that you are replacing is still running, login to the SMU GUI.
4. Migrate EVSs to an alternate node.
5. Shut down the node.
6. Once the node is shut down, go to **Home > Server Settings > Cluster Configuration** and delete the entry for the node that you are replacing.
7. Label the cables connected to each of the ports on the node, and disconnect the cables once they have been labelled. Ensure that you use dust covers where required.
8. Remove the old node from the rack.
9. Place the old node into the packaging that the new node was shipped in and mark it as a bad part.

Installing the new node

You are now ready to install the new node.

Procedure

1. Physically rack the new node into the place of the old node.
2. Connect the cables to the new node, according your labelling.

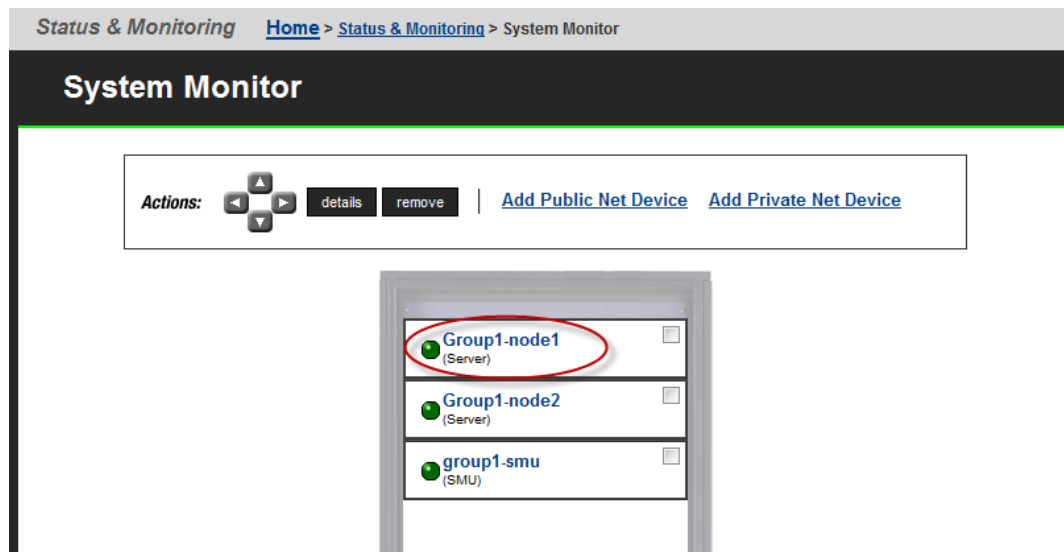
3. Power up the new node and ensure that BALI loads again.
4. If the customer is using SAN attached, and/or host group security, update this to reflect the changes that are being made to the WWN, as you documented previously in Preparing the node, step 5.
5. Add the new node as a managed server on the SMU.
6. From the drop down in the SMU, select the existing Cluster.
7. Go into **Home > Server Settings > Cluster Configuration** and click on **AddCluster node**.
8. Complete the **add cluster node wizard**, selecting the new node which will appear in the selection box, and enter the supervisor password where prompted (the default is supervisor). Upon completion of the wizard, the new node will reboot and join the cluster.

Finalizing and verifying the server configuration

On the new server:

Procedure

1. Navigate to **Home > Status & Monitoring > System Monitor** to verify the server status:



- If the server is operating normally, and is not displaying any alarm conditions, run a backup to capture the revised configuration, and then download another diagnostic to support. Permanent license keys for the new server will be provided within 15 days.
 - If the server is not operating normally for any reason, contact support for assistance.
2. Navigate to **Home > Server Settings > Cluster Configuration** to verify the cluster configuration status. Ensure that the cluster is shown as Online and Robust and has the correct number of nodes.

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

Cluster Configuration

Cluster Nodes					EVS	
Name	IP Address	Status	Model	Health		
Group1-node1	192.0.2.200	Online	3090-G2	OK	Group1-admin , g1-evs3 , g1-evs1 , LNAS , g1-evs2 , EVS1	details
Group1-node2	192.0.2.201	Online	3090-G2	OK	donotdelete	details

Cluster Information

Cluster Name: [rename](#)

Status: Online

Health: Robust

Cluster UUID: a6e6ddf0-9627-11cb-9000-d428dd993ca4

MAC: d4-28-dd-99-3c-a4

Quorum Device

Name: GROUP1-SMU

IP Address: 192.0.2.1

Status: Configured

[add](#) [remove](#)

Actions: [Add Cluster Node](#)

Shortcuts: [Quorum Services v2](#) [EVS Management](#) [EVS Migration](#)

- Use CLI to verify that the new node has access to the System Drives. Use `sd-list` from the node that you have just replaced.
For example: `pn x sd-list` where x is the node number in the cluster.

```
FSS-HNAS-1:$ sd-list
```

Device	Status	Alw	GiByte	Mirror	In span	Span Cap
0	OK	Yes	1607	Pri	FSS_Pool_1	3214
1	OK	Yes	1607	Pri	FSS_Pool_1	3214
4	OK	Yes	390	Pri	FSS_AMS200	1560
5	OK	Yes	390	Pri	FSS_AMS200	1560
6	OK	Yes	390	Pri	FSS_AMS200	1560
7	OK	Yes	390	Pri	FSS_AMS200	1560

- If EVS mapping or balancing is required, select the EVS to migrate, assign it to the preferred node, and then click **migrate**.

Server Settings [Home](#) > [Server Settings](#) > EVS Migration

EVS Migration

EVS Mappings

Node	Current EVS Mapping	Preferred EVS Mapping
Group1-node1	g1-evs3 , g1-evs1 , LNAS , g1-evs2 , EVS1	g1-evs3 , LNAS , g1-evs2 , EVS1
Group1-node2	donotdelete	donotdelete , g1-evs1

[Save current](#) as preferred | [Migrate all](#) to preferred

An **orange** EVS indicates the EVS is **not on its preferred** cluster node.

A **grey** EVS indicates the EVS does **not have a preferred** cluster node.

A **black** EVS indicates the EVS is **on its preferred** cluster node.

EVS Migrations

☐ Migrate EVS Group1-admin to cluster node Group1-node2

☐ Migrate all EVSes from cluster node Group1-node1 to cluster node Group1-node2

Migrating the EVS will disrupt file system services to any existing clients.

migrate

- To set the preferred node for any remaining EVSs, navigate to **Home > Server Settings > EVS Management > EVS Details**.

g1-cluster - 192.0.2.3 Help About Sign Out

Server Settings [Home](#) > [Server Settings](#) > [EVS Management](#) > EVS Details

EVS Details EVS1

Name: EVS1 **rename**

EVS ID: 6

Status: Online

Type: File Services

Enabled: Yes

Preferred Cluster Node: Group1-node1 **apply**

EVS Security: Global **change...** (Disable EVS to alter EVS security)

Default File System Security Mode: [Mixed \(Windows and Unix\)](#)

File Systems

[FS11](#)

IP Addresses

Port	IP Address
ag1	172.31.60.47/24
ag1	face::17/64

- Select the node from the Preferred Cluster Node list, and then click **apply**.
- Navigate to **Home > Status & Monitoring > Event Logs**, and then click **Clear Event Logs**.

8. Confirm all final settings, IP addresses, customer contact information, service restarts, client access, and that customer expectations are all in place. Features such as replication and data migration should all be confirmed as working, and all file systems and storage pools should be online.

Replacing all servers within a cluster

If both servers with an external SMU that are nonfunctioning, and does not have a recent backup saved off platform, then a challenging and manual recovery process is necessary. If this circumstance is encountered, call the support organization for a copy of the system's latest diagnostics files, if available, to be used as a guide in reestablishing the system manually. The data and file systems will remain intact independent of the replacement and without a backup.



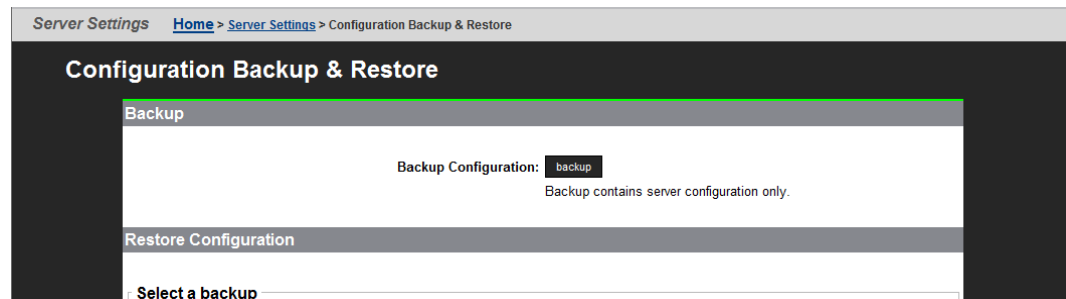
Important: Set expectations up front with the customer that this will delay time to recovery, and that some aspects of the systems configuration might never be recovered.

Obtaining backups, diagnostics, firmware levels, and license keys

On the old server:

Procedure

1. If the server is online, using NAS Manager, navigate to **Home > Server Settings > Configuration Backup & Restore**, click **backup**, and then select a location to save the backup file.



Ensure you save the backup file to a safe location off platform so that you can access it after the storage system is offline.

The backup process performed by the embedded SMU will automatically capture both the SMU and server configuration files in one complete set.

2. Navigate to **Home > Status & Monitoring > Diagnostics download** to download the diagnostic test results.

Status & Monitoring [Home](#) > [Status & Monitoring](#) > Download Diagnostics

Download Diagnostics

Select the devices for which diagnostics are required (downloading may take several minutes).

☒ **Managed Server**

- ☒ Include All Managed Servers
- ☐ Include Only the Currently Managed Server
- ☐ Include all files (e.g. archived showwall.txt)

☒ **Fibre Channel Switches**

☒ **SMU**

- ☒ Include archived diagnostics (if issue occurred over a few hours ago)

[download](#) [email](#)

Select the devices for which diagnostics are required by checking the appropriate boxes. Then click **download**.

3. Navigate to **Home > Server Settings > Firmware Package Management** to verify the existing server (SU) firmware release level.

Server Settings [Home](#) > [Server Settings](#) > Firmware Package Management

Firmware Package Management

Filter ☐ Include System Patch Packages [filter](#)

Node View

Cluster Node ID (Name)	Status	Current Package	Default Package	Free Space	
1 (Group1-node1)	Online	12.1.3600.00	12.1.3600.00	293.77 GB (97 %)	details
2 (Group1-node2)	Online	12.1.3600.00	12.1.3600.00	297.36 GB (97 %)	details

Actions: [restart cluster file serving](#) [restart file serving on node](#) | [upload package](#)

Package View

Package	Present On Cluster Nodes	Install Status
☐ nas-11.3.3434.01.tar	1, 2	OK
☐ nas-11.2.3319.06.tar	1, 2	OK
☐ nas-11.2.3319.09.tar	1, 2	OK
☐ nas-11.1.3225.00.tar	1, 2	OK
☐ nas-12.1.3600.00.tar	1, 2	OK
☐ nas-12.0.3525.00.tar	1, 2	OK
☐ nas-12.0.3528.01.tar	1, 2	OK

Actions: [delete](#) [set as default on all nodes](#)

The new server firmware version must match the failed server; otherwise, the server cannot properly restore from the backup file. See the release notes and the *System Installation Guide* for release-specific requirements.

4. Navigate to **Home > Server Settings > IP Addresses** to obtain:

- Admin IP address and name
- Cluster node IP address

The `evs list` command also displays these IP addresses.

Shutting down the servers you are replacing

On the servers that you are replacing:

Procedure

- 1. From the server console, issue the command: `cn node shutdown --ship --powerdown`

(where *node* represents the targeted node)

Wait until the console displays `Information: Server has shut down`, and the rear panel LEDs turn off. The PSU and server fans continue to run until you remove the power cables from the PSU module. See the appropriate system component section for more information.

 **Note:** This specific `powerdown` command prepares the system for both shipping, and potential long-term, post-replacement storage.

- 2. Unplug the power cords from the power supplies.
- 3. Wait approximately 15 seconds, and then confirm the NVRAM status LED is off. If the LED is flashing or fixed, press and hold the **reset** button for five seconds or until the LED starts flashing. The battery disables when you release the **reset** button.
- 4. Use the following rear panel figure and table to identify and label the cabling placement on the existing server.

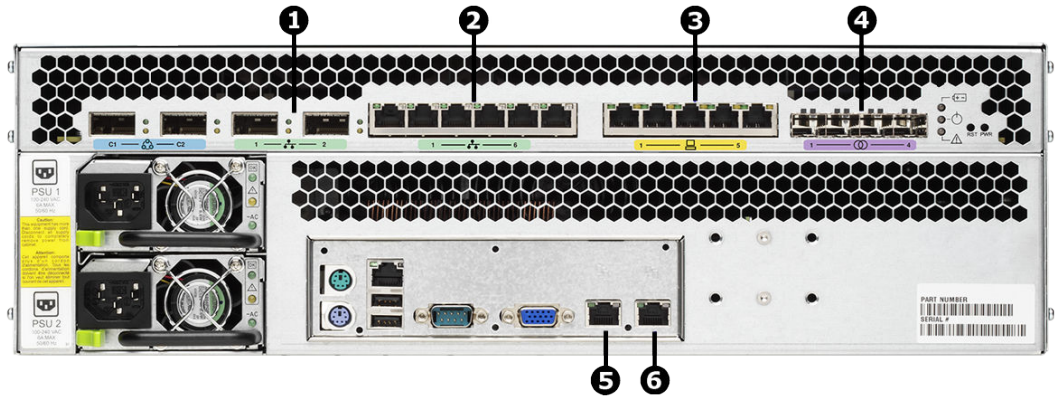


Figure 42 Rear view of server - HNAS 4040 model

Item	Labels	Ports	Connections
1		1	10 GbE data network
		2	10 GbE data network
2		1	Gigabit Ethernet network port
		2	Gigabit Ethernet network port
		3	Gigabit Ethernet network port

Item	Labels	Ports	Connections
		4	Gigabit Ethernet network port
		5	Gigabit Ethernet network port
		6	Gigabit Ethernet network port
3		1	10/100 Private management network Ethernet port
		2	10/100 Private management network Ethernet port
		3	10/100 Private management network Ethernet port
		4	10/100 Private management network Ethernet port
		5	10/100 Private management network Ethernet port
4		1	Storage or FC switch
		2	Storage or FC switch
		3	Storage or FC switch
		4	Storage or FC switch
5		0	Customer facing management network
6		1	Private management network

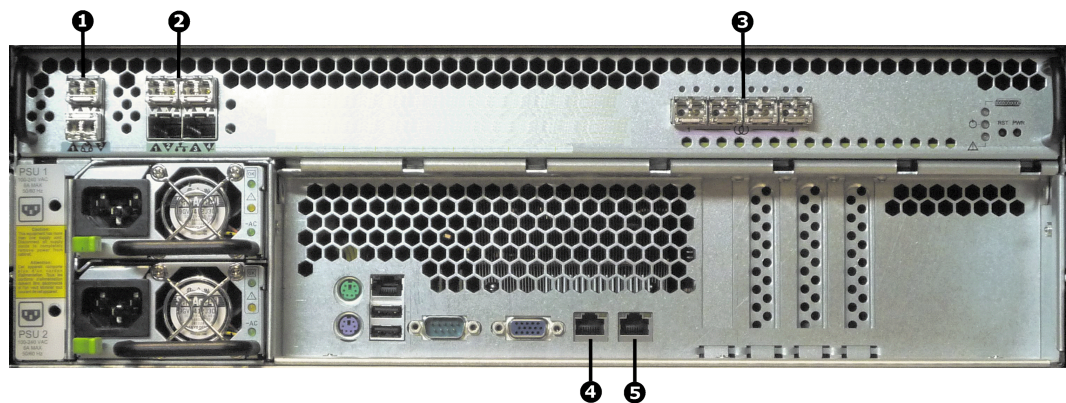


Figure 43 Rear view of server - HNAS 4060, 4080, and 4100 models

Item	Labels	Ports	Connections
1		1	Cluster interconnect for additional servers
		2	Cluster interconnect for additional servers
2		1	Customer data network
		2	Customer data network
		3	Customer data network
		4	Customer data network
3		1	Storage or FC switches
		2	Storage or FC switches
		3	Storage or FC switches
		4	Storage or FC switches
4		0	Customer facing management network
5		1	Private management Ethernet network

5. If cables are not labeled, label them before removing them from the server.
6. Remove all cables from the server, and remove the server from the rack.
7. Remove the rail mounts from the old server, and install them on the new server.
8. Remove the battery from the old server, and install it in the new server.
9. Remove the bezel from the old server, and install it on the new server.
10. Insert the new server into the rack, and connect the power cords to the power supplies.



Note: Do not make any other cable connections at this time.

Configuring the replacement servers

Before you begin

Obtain the necessary IP addresses to be used for the replacement server. Servers shipped from the factory have not yet had the `nas-preconfig` script run on them, so a replacement server will not have any IP addresses pre-configured for your use. You need IP addresses for the following:

- Eth1 (cluster IP)
- Eth1 (testhost private IP)
- Eth0 (testhost external IP)
- 192.0.2.200/24 eth1 (cluster IP)
- 192.0.2.2/24 eth1 (testhost private IP)
- 192.168.4.120/24 eth0 (testhost external IP, which might vary)

On a replacement server:

Procedure

1. Log in to the server.
2. Run the `nas-preconfig` script.
The IP addresses are assigned at this step.
3. Reboot if you are instructed to by the script.
4. Log in to the SMU using one of the IP addresses you obtained once they can successfully connect using `ssc localhost`.
5. Use a KVM (keyboard, video, and mouse) or a serial cable to connect to the serial port on the server.
Alternatively, you can connect by way of SSH using the following settings:
 - 115,200 b/s
 - 8 data bits
 - 1 stop bit
 - No parity
 - No flow control
 - VT100 emulation
6. Log in as `root`, and enter `ssc localhost` to access the BALI level command prompt.
7. Enter `evs list` to see the IP configuration for the server.
8. Using a supported browser, launch the NAS Manager using either one of the IP addresses acquired from the EVS list output.
9. Click **Yes** to proceed past Security Alert, and log in as `admin`.
10. Verify and, if necessary, convert the new server to the model profile required.
This step requires a separate process, training, and license keys. Contact Hitachi Vantara if the incorrect model arrives for replacement.

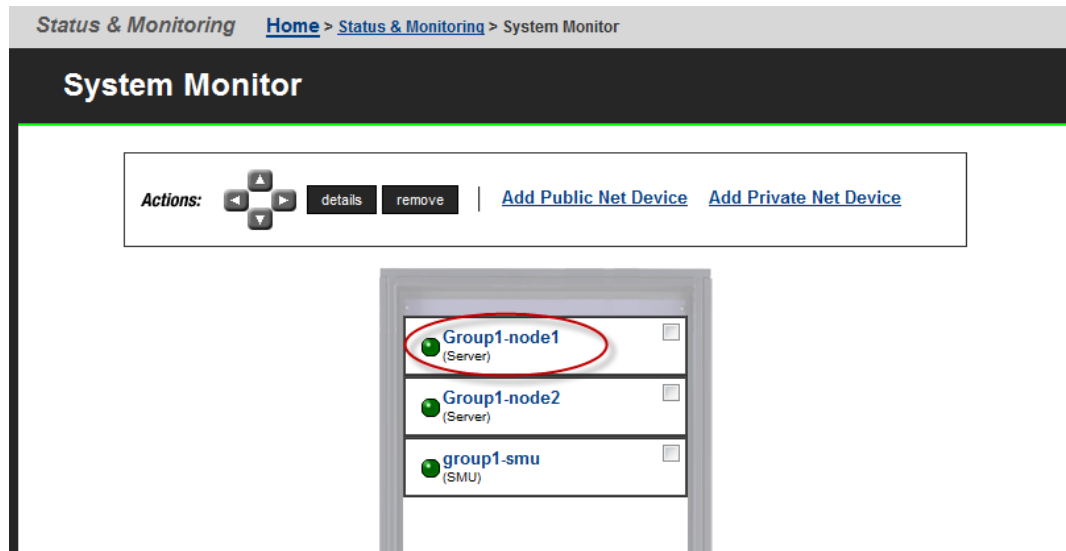
11. Navigate to **Home > Server Settings > Firmware Package Management** to verify and, if necessary, upgrade the new server to the latest SU release.
12. Navigate to **Home > Server Settings > Cluster Wizard**, and promote the node to the cluster.
13. Enter the cluster name, cluster node IP address, subnet, and select a quorum device. Note that the node reboots several times during this process.
14. When prompted, add the second node to the cluster.
15. Enter the physical node IP address, log in as `supervisor`, and click **finish**. Wait for the system to reboot.
16. Enter `smu-uninstall` to uninstall the embedded SMU.
17. Navigate to **Home > Server Settings > Configuration Backup & Restore**, locate the desired backup file, and then click **restore**.
18. Reconfigure the server to the previous settings:
 - IP addresses for Ethernet ports 0 and 1
 - Gateway
 - Domain name
 - Host nameThe SMU should recognize the node as the same and allow it to be managed.
19. Navigate to **Home > Server Settings > License Keys** to load the license keys.
20. Repeat steps for any other replacement servers to be configured.

Finalizing and verifying the system configuration

On the new server:

Procedure

1. Navigate to **Home > Status & Monitoring > System Monitor** to verify the server status:



- If the server is operating normally, and is not displaying any alarm conditions, run a backup to capture the revised configuration, and then download another diagnostic to support. Permanent license keys for the new server will be provided within 15 days.
 - If the server is not operating normally for any reason, contact support for assistance.
2. Navigate to **Home > Status & Monitoring > Event Logs**, and then click **Clear Event Logs**.
 3. Confirm all final settings, IP addresses, customer contact information, service restarts, client access, and that customer expectations are all in place. Features such as replication and data migration should all be confirmed as working, and all file systems and storage pools should be online.

Appendix B: Accessing the server CLI

Performing certain tasks require that you access the server through the command line interface (CLI). Refer to the *System Access Guide* for more information.

Accessing the command line interface

Performing some tasks require you to access the server through the command line interface (CLI). Use one of the following methods to access the CLI: serial (console) port and KVM, or SSH connection.

Using the serial (console) port

The SMU ships without a preconfigured network setup. To perform the initial setup, access the SMU through a direct serial connection or KVM. After its network configuration has been completed, access the SMU's CLI directly through SSH or through a Java-enabled SSH session running under NAS Manager.

To connect using a serial console:

Procedure

1. Attach an RS232 null-modem cable (DB-9 female to DB-9 female) to the serial port on the SMU back panel. Attach the other end of the serial cable to a terminal (for instance, a laptop).
2. Start a console session using your terminal emulation with the following settings:
 - 115,200 b/s
 - 8 data bits
 - 1 stop bit
 - No parity
 - VT100 emulation
 - No flow control

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

3. Log in as the user `manager`. When prompted, enter the password for the user `manager`.
4. After connecting, launch the storage server CLI or select the SMU shell. From the SMU command line, access the server CLI using a method in the displayed menu, or enter `q` to access the SMU shell.

Using an SSH connection

The SMU can be accessed using any SSH client. Note that the client should be configured to support the UTF-8 (Unicode) character encoding.

Appendix C: Parts list for Series 4000 servers

Parts for model 4040 servers

Part number	Description	Notes
SX325097	MK1 Battery Module ea	
SX325099	Hard Disk ea (500GB)	
SX325116	Fan Tray	
SX325130	PSU Module - 450W	
SX325143	Server	Does not include PSUs, battery, bezel, or rail kit

Parts for model 4060 and 4080 servers

Part number	Description	Notes
SX325097	MK1 Battery Module ea	
SX325116	Fan Tray	
SX325125	Hard Disk (250GB)	
SX325136	PSU Module (High Efficiency)	
SX325140	Server	Does not include PSUs, battery, bezel, or rail kit

Parts for model 4100 servers

Part number	Description	Notes
SX325097	MK1 Battery Module (each)	
SX325116	Fan Tray	
SX325125	Hard Disk (250GB)	

Part number	Description	Notes
SX325136	PSU Module (High Efficiency)	
SX325141	Server	Does not include PSUs, battery, bezel, or rail kit

Switch parts

Part number	Description	Notes
SX220421	HP ProCurve 1800-24G (Managed 24 port Ethernet 10/100/1000BASE-T)	
SX220480	HP ProCurve 1810-24G (Managed 24 port Ethernet 10/100/1000 BASE-T)	
224-5880	Dell PowerConnect 2824 Switch (24 Ports, GigE)	Can use part number 222-2257
XBR-VDX6730-16-R	Brocade VDX 6730 10GbE Switch, 16 Ports SFP+, AC, Port Side Exhaust AF	
XBR-250WPSAC-R	Brocade VDX 6730 250W AC PS/fan, Port Side Exhaust	
XBR-VDX6730-16-F	Brocade VDX 6730 10GbE Switch, 16 Ports SFP+, AC, Non Port Side Exhaust AF	
XBR-250WPSAC-F	Brocade VDX 6730 250W AC PS/fan, Non Port Side Exhaust	
XBR-VDX6730-40-R	Brocade VDX 6730 10GbE Switch, 40 Ports SFP+, AC, Port Side Exhaust AF	

Part number	Description	Notes
XBR-500WPSAC-R	Brocade VDX 6730 500W AC PS, Port Side Exhaust	
XBR-FAN-80-R	Brocade VDX 6730 80MM Fan assy, Port Side Exhaust	
XBR-VDX6730-40-F	Brocade VDX 6730 10GbE Switch, 40 Ports SFP+, AC, Non Port Side Exhaust AF	
XBR-500WPSAC-F	Brocade VDX 6730 500W AC PS, Non Port Side Exhaust	
XBR-FAN-80-F	Brocade VDX 6730 80MM Fan assy, Non Port Side Exhaust	
SFP-H10GB-CU1M	Copper cable - SFP+ 10GE passive twinax, Cluster & 10GbE, 1 meter	
SFP-H10GB-CU3M	Copper cable - SFP+ 10GE passive twinax, Cluster & 10GbE, 3 meters	
SFP-H10GB-CU5M	Copper cable - SFP+ 10GE passive twinax, Cluster & 10GbE, 5 meters	

Optics used with model 4040 servers

Part number	Description	Notes
FTLF8524P2BNV	SFP - multi-mode Fiber - 4 Gbps	Equivalent part number SX350010
FTLX8511D3	XFP - 10G 850NM 1-ea for cluster only	Part number SX350011

Part number	Description	Notes
FTLX1412D3BCL (SX350020-02)	Multi-source XFP 10Gbps; single mode 1310nm; LC 3.3v	Substitute - FTLX1411D3
FTLX1411D3	XFP - 10G LWL 10km Finisar 1-Pk	Can use FTLX1412D3BCL

Optics used with model 4060/4080/4100 servers

Part number	Description	Notes
FTLX8571D3BCV	SFP+ 10GE 300 meters 850 nm. multimode 3.3v	
FTLF8528P3BNV	SFP+ 8G FC short reach multimode 850 nm 3.3v	
FTLX1471D3BCV	SFP+ 10GE 10Km 1310 nm. single mode	
FTLX8574D3BCL	SFP+ 10GE 400 meters 850 nm. multimode 3.3v	

Copper cables used with model 4060/4080/4100 servers

Part number	Description	Notes
SFP-H10GB-CU1M	SFP+ 10GE passive twinax, Cluster & 10GbE, 1 meter	
SFP-H10GB-CU3M	SFP+ 10GE passive twinax, Cluster & 10GbE, 3 meters	
SFP-H10GB-CU5M	SFP+ 10GE passive twinax, Cluster & 10GbE, 5 meters	

Hitachi Vantara



Corporate Headquarters

2535 Augustine Drive

Santa Clara, CA 95054 USA

HitachiVantara.com | community.HitachiVantara.com

Contact Information

USA: 1-800-446-0744

Global: 1-858-547-4526

HitachiVantara.com/contact