



## **Hitachi NAS Platform**

# **3080 and 3090 G1 Hardware Reference**

**Release 13.0**

© 2011, 2016 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 (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 at [https://support.hds.com/en\\_us/contact-us.html](https://support.hds.com/en_us/contact-us.html).

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

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

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and
2. Verifying that 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 is a registered trademark of Hitachi, Ltd., in the United States and other countries.

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

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

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



# Contents

<b>Preface .....</b>	<b>7</b>
Related Documentation.....	7
Accessing product documentation.....	10
Getting help.....	10
Comments.....	10
 <b>1 About this manual.....</b>	 <b>13</b>
Audience.....	14
Conventions.....	14
 <b>2 Safety information.....</b>	 <b>19</b>
Electrostatic discharge precautions.....	20
Safety and handling precautions.....	20
Electrical precautions.....	21
Data protection precautions.....	21
 <b>3 Mandatory regulations.....</b>	 <b>23</b>
International standards.....	24
Federal Communications Commission (FCC).....	24
European Union (EU) Statement.....	25
Canadian Department of Communication Compliance Statement.....	25
Avis de conformité aux normes du ministère des Communications du Canada.....	26
Radio Protection for Germany.....	26
Food and Drug Administration (FDA).....	26
Chinese RoHS Compliance Statement.....	26
 <b>4 System overview.....</b>	 <b>29</b>
System components.....	30
Server specifications.....	31
Attaching a rack stabilizer plate.....	32

<b>5 Hitachi NAS Platform server components.....</b>	<b>33</b>
Introducing the Hitachi NAS Platform.....	34
Ventilation.....	34
Front view of server.....	34
NVRAM backup battery pack.....	36
Server rear panel.....	37
Rear panel server LED and button locations.....	39
Rear panel LED state descriptions.....	39
Power button (PWR).....	40
Reset button (RST).....	41
10 GbE Ports.....	41
10 Gigabit Ethernet cluster interconnect ports.....	41
10 Gigabit Ethernet customer data network ports.....	42
GE Ethernet network ports .....	43
10/100 private Ethernet ports.....	43
Fibre channel storage ports.....	44
Serial port .....	45
Power supply units .....	45
10/100/1000 Ethernet management ports.....	47
USB ports.....	47
Management interfaces.....	48
RS-232 serial management port .....	48
<b>6 Replacing server components.....</b>	<b>49</b>
Removing and replacing the front bezel.....	50
Bezel removal.....	50
Replacing a fan.....	50
Replacing the NVRAM backup battery pack.....	52
Removing the battery pack from the caddy.....	52
Removing the battery pack: type 1 chassis .....	54
Inserting the new battery pack: type 1 chassis .....	55
Removing the battery pack: type 2 chassis .....	57
Inserting the new battery pack: type 2 chassis.....	60
Collecting system backups and diagnostics.....	62
Resetting the battery age and restarting the chassis monitor .....	63
Collecting a final diagnostic .....	64
Replacing a hard disk.....	65
Replacing a power supply unit.....	67
<b>7 Rebooting, shutting down, and powering off.....</b>	<b>69</b>
Rebooting or shutting down a server.....	70
Rebooting or shutting down a cluster.....	71
Restarting an unresponsive server.....	72
Powering down the server for maintenance.....	73
Powering down the server for shipment or storage.....	74
Recovering from power standby.....	75
<b>8 Hard disk replacement.....</b>	<b>77</b>
Intended Audience.....	79

Downtime considerations for hard disk replacement.....	79
Requirements for hard disk replacement.....	80
Overview of the Procedure.....	80
Accessing Linux on the server and node.....	81
Using the Serial (Console) Port.....	81
Using SSH for an Internal SMU.....	82
Using SSH for an External SMU.....	82
Step1: Performing an Internal Drive Health Check.....	83
Step 2: Gathering information about the server or node.....	88
Step 3: Backing up the server configuration.....	90
Step 4: Locating the server.....	90
Step 5: Save the preferred mapping and migrate EVSs (cluster node only).....	91
Step 6: Replacing a Server's Internal Hard Disk.....	93
Step 7: Synchronizing server's new disk.....	100
Step 8: Replacing the server's second disk.....	101
Step 9: Synchronizing the second new disk.....	101
Step 10: Restore EVSs (cluster node only).....	101
<b>A Server replacement procedures.....</b>	<b>105</b>
Replacement procedure overview.....	106
Requirements.....	106
Swapping components.....	106
Model selection.....	107
MAC ID and license keys.....	107
Previous backups.....	107
Upgrades.....	108
Manually installing an internal SMU (if necessary) .....	108
Replacing a single server with an embedded SMU.....	108
Obtaining backups, diagnostics, firmware levels, and license keys.....	109
Shutting down the server you are replacing.....	111
Configuring the replacement server.....	111
Finalizing and verifying the replacement server configuration.....	113
Replacing a single server with an external SMU.....	115
Obtaining backups, diagnostics, firmware levels, and license keys.....	115
Shutting down the server you are replacing.....	116
Configuring the replacement server.....	117
Finalizing and verifying the replacement server configuration.....	119
Replacing a node within a cluster.....	121
Capturing information from the existing node.....	121
Preparing the new node.....	122
Preparing the old node for removal.....	122
Installing the new node.....	123
Finalizing and verifying the server configuration.....	123
Replacing all servers within a cluster.....	126
Obtaining backups, diagnostics, firmware levels, and license keys.....	127
Shutting down the servers you are replacing.....	128
Configuring the replacement servers.....	129
Finalizing and verifying the system configuration.....	131
<b>B Parts list for 3080/3090 G1 servers.....</b>	<b>133</b>



# 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: 3080 and 3090.

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 and 3090*

### 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 firmware, 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 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 USP-V/VSP Best Practice Guide for HNAS Solutions* (MK-92HNAS025)—The practices outlined in this document describe how to configure the system to achieve the best results.



- *Hitachi Unified Storage VM Best Practices Guide for HNAS Solutions* (MK-92HNAS026) —The system is capable of heavily driving a storage array and disks. The practices outlined in this document describe how to configure the system to achieve the best results
- *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.
- *Brocade VDX 6730 Switch Configuration for use in an HNAS Cluster Configuration Guide* (MK-92HNAS046)—This document describes how to configure a Brocade VDX 6730 switch for use as an ISL (inter-switch link) or an ICC (inter-cluster communication) switch.
- *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 12.1 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 v 12.1 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.
- *Brocade VDX 6740 Switch Configuration for use in an HNAS Cluster Configuration Guide* (MK-92HNAS066)—This document describes how to configure a Brocade VDX 6740 switch 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 Virtual SMU Administration Guide* (MK-92HNAS074)—This guide provides information about how to install and configure a virtual System Management Unit (SMU).
- *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 Hitachi Data Systems Support Connect: <https://knowledge.hds.com/Documents>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

## Getting help

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

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

## Comments

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

**Thank you!**



## 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: 3080 and 3090.

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

- ☐ [Audience](#)
- ☐ [Conventions](#)

## Audience



This guide is written for owners and field service personnel who may have to repair the system hardware. It is written with the assumption that the reader has a good working knowledge of computer systems and the replacement of computer parts.



## Conventions

The following conventions are used throughout this document:

Convention	Meaning
<b>Command</b>	This fixed-space font denotes literal items such as commands, files, routines, path names, signals, messages, and programming language structures.
<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 messages are used throughout this manual. It is recommended that these icons and messages are read and clearly understood before proceeding:

	A tip contains supplementary information that is useful in completing a task.
	A note contains information that helps to install or operate the system effectively.

	A caution indicates the possibility of damage to data or equipment. Do not proceed beyond a caution message until the requirements are fully understood.
	A warning contains instructions that you must follow to avoid personal 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 kuvatun 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.



## Safety information

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

- ☐ [Electrostatic discharge precautions](#)
- ☐ [Safety and handling precautions](#)
- ☐ [Electrical precautions](#)
- ☐ [Data protection precautions](#)

## Electrostatic discharge precautions

To ensure proper handling of system components and to prevent hardware faults caused by electrostatic discharge, follow all 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 of the safety precautions and instructions.



**Caution:** Observe safe lifting practices. Each server or each storage array can weigh 57 lb. (26 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.
- 

To help prevent serious injuries, load the components in the storage cabinet in the prescribed order:

1. If present, install the rack stabilizer plate to the front of the system cabinet.
2. Load the Fibre Channel (FC) switches in the storage cabinet at the positions recommended in the *System Installation Guide*. The positions can be adjusted according to a specific storage cabinet configuration.
3. Load and position the server(s) directly above the FC switches, if used in your configuration.
4. The System Management Unit (SMU), if used in your configuration, should be placed directly below the FC switches.
5. The first storage enclosure should be positioned at the bottom of the storage cabinet. Additional enclosures are then placed above existing enclosures, going towards the top of the system cabinet.
6. Once the bottom half of the storage cabinet has been filled, the top half of the storage cabinet can be filled. Begin by placing a storage component directly above the server and then fill upwards.

## Electrical precautions

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

- Provide a suitable power source with electrical overload protection to meet the power requirements of the entire system (the server/cluster, and all storage subsystems and switches). The power requirements per cord are - North America: 2 phase, 208Vac, 24A max; 1 phase 110Vac, 16A max. Europe: 230Vac, 16A max.
- Provide a power cord that is 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, please contact your local sales 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 needs to be moved or if it is damaged.



**Note:** For additional data protection, Hitachi recommends that you use an external UPS to power the server. Also, each of the redundant power supplies in the server and in the storage subsystems should be operated from a different mains power circuit in order to provide a degree of protection from mains power supply failures. In the event that one circuit fails, the other continues to power the server and the storage subsystem.

---

## 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. 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. Contact the Hitachi Data Systems Support Center for technical details about replacement parts.
- Maintain backup routines. Do not abandon backup routines. No system is completely foolproof.

## 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](#)
- ☐ [Federal Communications Commission \(FCC\)](#)
- ☐ [European Union \(EU\) Statement](#)
- ☐ [Canadian Department of Communication Compliance Statement](#)
- ☐ [Radio Protection for Germany](#)
- ☐ [Food and Drug Administration \(FDA\)](#)
- ☐ [Chinese RoHS Compliance Statement](#)

## 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 RoHS2 and WEEE
- China: CCC
- Russia: GOST-R
- Taiwan: BSMI
- Argentina: IRAM
- Australia & New Zealand: C-Tick
- Mexico: NOM and CONUEE
- South Africa: SABS (safety) and EMC (self-certification by CoC)

## 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
- 2002/95/EC Restriction in the use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) - This product is 6/6 (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
电池包 Battery Pack	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.



## System overview


This chapter describes the components in the Hitachi NAS Platform server system for the following models:

- Hitachi NAS Platform, Model 3080
- Hitachi NAS Platform, Model 3090

- ☐ [System components](#)
- ☐ [Server specifications](#)
- ☐ [Attaching a rack stabilizer plate](#)

## 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	<p>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 Data Systems supports two switches for redundancy.</p> <p>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> .</p> <hr/> <p> <b>Note:</b> For additional data protection, it is recommended to use an external UPS to power the server. Also, each of the redundant power supplies in the server and in the storage subsystems should be operated from a different mains power circuit in order to provide a degree of protection from mains power supply failures. In the event that one circuit fails, the other will continue to power the server and the storage subsystem.</p> <hr/>
System management unit (SMU)	<p>A standalone server can operate without an external SMU, but all of the cluster configurations require an external SMU.</p> <p>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.</p> <p>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.</p>
Storage subsystems	<p>A Hitachi NAS Platform or 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.</p>
Fibre Channel (FC) switches	<p>The server supports FC switches that connect multiple servers and storage subsystems. Some configurations require FC switches, but they are optional in other configurations.</p> <p>An external FC Switch is required when connecting more than two storage subsystems to a standalone server or a cluster. An external FC Switch is optional when connecting less than three storage subsystems to a stand alone server or a cluster.</p> <p>Contact customer support for information about which FC switches are supported.</p>

Component	Description
External Fast Ethernet (10/100) or Gigabit Ethernet (GigE) switches	<p>A standalone server can operate without an external Ethernet switch, provided that it uses an embedded SMU and there are less than three RAID subsystems attached.</p> <p>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.</p> <p>All cluster configurations require an external Ethernet switch.</p>
10 Gigabit Ethernet (10 GbE) switches	<p>Used in cluster configurations only.</p> <p>A server connects to a 10 GbE switch for connection with the public data network (customer data network).</p> <p>A 10 GbE switch is required for internal cluster communications for clusters of three or more nodes.</p> <p>Contact Hitachi Data Systems Support Center 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.</p> <p>Hitachi Data Systems 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.</p>

## 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.)
- 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.

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)

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

## Attaching a rack stabilizer plate

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

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



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

---

### Procedure

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



## 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 Data Systems 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 (Mercury Motherboard)
- MFB (Mercury FPGA Board)
- Two hot-swappable fan assemblies
- Dual power supplies
- NVRAM backup battery pack
- Dual 2.5 inch disk drives

☐ [Introducing the Hitachi NAS Platform](#)

☐ [Ventilation](#)

☐ [Front view of server](#)

☐ [NVRAM backup battery pack](#)

☐ [Server rear panel](#)

## Introducing the Hitachi NAS Platform

This section introduces you to the Hitachi NAS Platform or the system and server.

A Hitachi NAS Platform chassis is 3U (5.25 inches) high, 480 millimeters (19 inches) wide, rack mountable, and a maximum of 686 millimeters (27 inches) deep, excluding the fascia. The Hitachi NAS Platform chassis consists of:

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

The pre-installed boards perform functions essential to the integrity of the server. If there is an issue with a board, return the server for repair (boards are not field replaceable). Field replaceable units (FRUs) include power supplies, an NVRAM backup battery pack, fan assemblies, and disk drives. For more information, see [Replacing server components on page 49](#).

## 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.

---

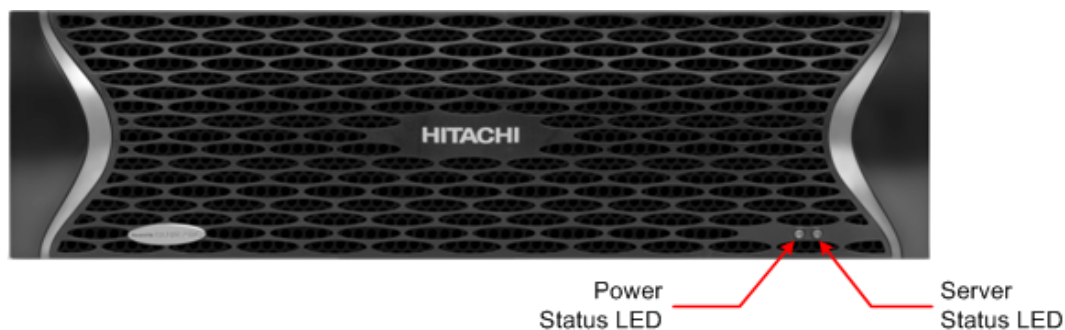


**Caution:** Do not place the server in a built-in installation unless proper ventilation is provided.

Do not operate the server in a cabinet whose internal ambient temperature exceeds 35° C (95° F).

---

## Front view of server



On the front panel there are two LED indicators (Power and Status), which indicate the system status as follows:

**Table 1 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 2 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.

## 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.

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 battery 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 41](#) 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.



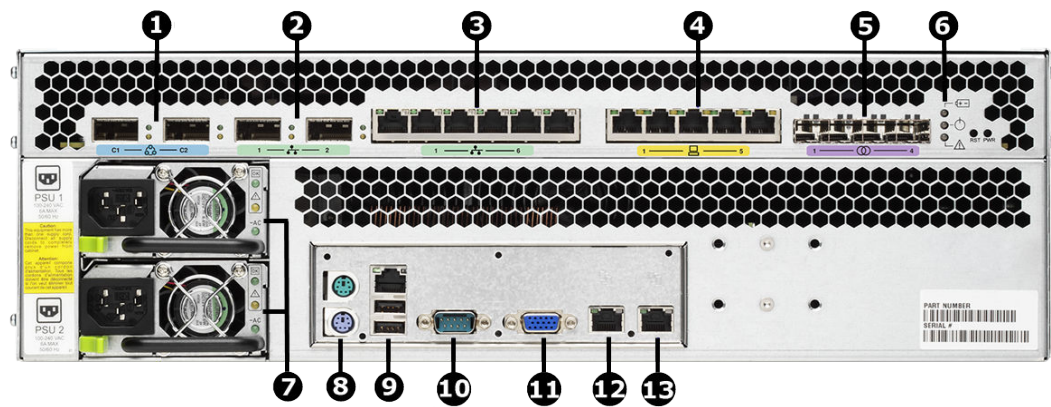
**Note:** If the batteries become fully discharged, or the system is to be powered down for an extended period, see [Powering down the server for shipment or storage on page 74](#). Contact customer support for information about recharging batteries.

---

To replace the NVRAM battery backup pack, see [Replacing the NVRAM backup battery pack on page 52](#).

## Server rear panel

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



**Figure 1 Server rear panel components**

**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.

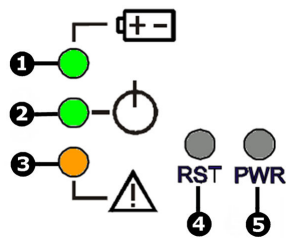
**Table 3 Server rear panel components descriptions**

Item	Connectivity	Quantity	Description
1	Clustering ports 10 GbE	2	For cluster management and heartbeat, connect to: <ul style="list-style-type: none"> <li>Two way configuration: Connect to corresponding cluster server ports (left port to left port and right port to right port).</li> <li>N-way configuration: Connect to 10 GbE switch.</li> </ul>
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.
7	Power supply units: PSU 1 PSU 2	2	Connect to the rack's Fault group: <ul style="list-style-type: none"> <li>PSU 1 to Fault group A</li> <li>PSU 2 to Fault group B</li> </ul>
8	I/O ports	2	Keyboard (purple) and mouse (green) ports. <i>(Reserved for Customer Service Engineer access only.)</i>

Item	Connectivity	Quantity	Description
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 2 Rear panel server status LEDs and buttons**

**Table 4 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

## 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 5 NVRAM status LED (green/amber)**

State	Meaning
Green (solid)	Normal operation
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 6 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 7 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.

## 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 the Hitachi Data Systems Support Center 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)

The reset button has several functions.

- 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.

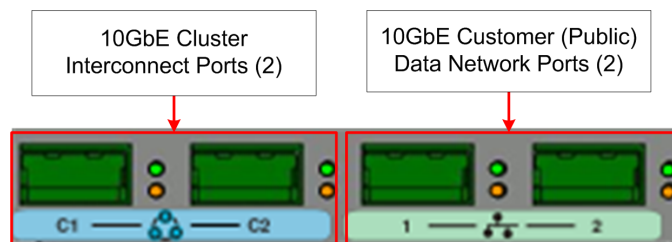
- Pressing the reset button for more than five seconds when the server is not powered up disables the NVRAM battery pack (which may be necessary prior to shipping if an incomplete shutdown occurred.) See [Powering down the server for shipment or storage on page 74](#) for more information.



**Caution:** If the server is non-responsive, see [Restarting an unresponsive server on page 72](#). Do not pull the power cord. Pulling the power cord does not produce a dump.

---

## 10 GbE Ports



**Figure 3 NAS Platform 10 GbE Ports**

### 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.

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



**Figure 4 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
<b>Status</b>	Green (on, not flashing)	10 Gbps link present
	Green flashing	10 Gbps link standby in a redundant configuration
	Green off	No link
<b>Activity</b>	Amber flashing	Network activity
	Amber off	No network 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.



**Figure 5 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

## 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 6 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

## 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 7 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
<b>Status</b>	Green (On, not flashing)	10 or 100 Mbps link present
	Green Off	No link
<b>Activity</b>	Amber Flashing	Network activity
	Amber Off	No network activity

## 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 8 Fibre Channel storage ports label**

Status/Activity (per port)		Meaning
<b>Status</b>	Green (on, not flashing)	FC link present
	Green off	No link
<b>Activity</b>	Amber flashing	Data activity
	Amber off	No data activity

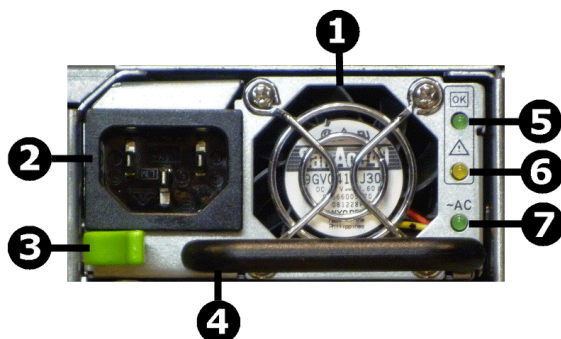
## Serial port

A standard serial (RS-232) port, used to connect to the server for management purposes. See [RS-232 serial management port on page 48](#) for more information.

## 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 9 Power supply unit details**

Item	Description
1	PSU fan exhaust
2	Power cord connector

Item	Description
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 67](#) for information about replacing a power supply.

**Table 8 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 9 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 on, the PSU has failed and must be replaced. See [Replacing a power supply unit on page 67](#) for more information on replacing a PSU.

**Table 10 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 72](#). Do not pull the power cord.

---

#### Related tasks

- [Replacing a power supply unit](#) on page 67

## 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.

## USB ports

Standard USB 2.0 (Universal Serial Bus 2.0) 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.

---

## Management interfaces

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

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 Web Manager GUI 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 11 Host setting values**

Terminal	Requirement
Connection	Crossover (null modem) cable
Emulation	VT100
Baud rate	115,200 Bps
Data bits	8
Stop bits	1
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 internal SMU and use SSH to access the server's CLI.



## Replacing server components

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

- ☐ [Removing and replacing the front bezel](#)
- ☐ [Bezel removal](#)
- ☐ [Replacing a fan](#)
- ☐ [Replacing the NVRAM backup battery pack](#)
- ☐ [Replacing a hard disk](#)
- ☐ [Replacing a power supply unit](#)

## 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 10 Server front 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.

### Replacing a fan

Fans provide for front-to-back airflow to be consistent with other storage system components. The server continues to operate following the failure of a single fan and during the temporary removal of a fan for replacement. A failed fan must be replaced as soon as possible.

The fans are contained within three assemblies, which are located behind the front fascia and are removable from the front of the server. All servers have three fans (one fan per assembly).

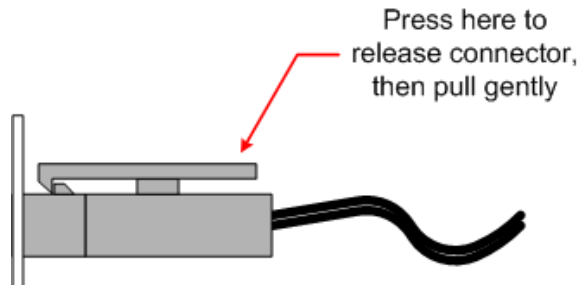
The server's cooling airflow enables the system to operate in an ambient temperature range of 10°C to 35°C when mounted in a storage cabinet with associated components required to make up a storage system. The storage system administrator is responsible for ensuring that the ambient temperature within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



**Caution:** If a fan has failed, replace the fan as soon as possible to avoid over-heating and damaging the server.

### Procedure

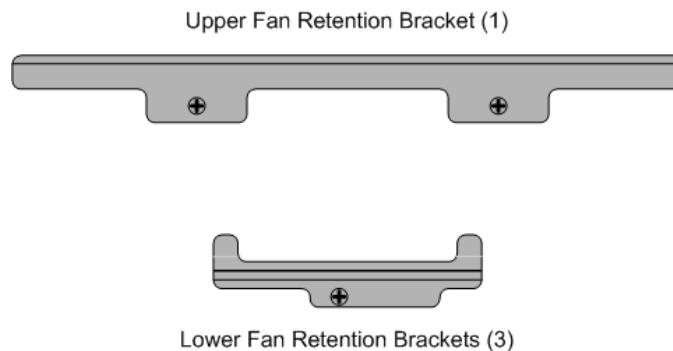
1. Remove the front fascia (and the fan guard plate), see [Bezel removal on page 50](#) for more information. The fan assemblies will then be visible.
2. Identify the fan to be replaced. Fans are labeled on the chassis, and are numbered 1 to 3, with fan 1 on the left and fan 3 on the right.
3. Disconnect the fan lead from its connector by pressing down on the small retaining clip, as shown next.



**Figure 11 Disconnecting the Fan Lead Connector**

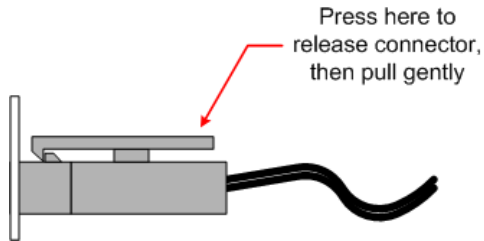
4. Remove the upper fan retention bracket and place it in a safe location. Note that the upper fan retention bracket helps to hold all three fan assemblies in position.

**Figure 12 Fan Retention Brackets**



5. For each fan assembly you are replacing, remove the lower fan retention bracket and place it in a safe location.
6. Remove the faulty fan assembly, and put the new fan assembly into place. Make sure to:
  - Fit the new fan assembly in the same orientation as the old fan assembly (the arrow indicating the direction of airflow must point into the server).
  - Align the fan lead and its protective sleeve in the space allotted for it on the bottom right side of the fan assembly mounting area.
  - Fit the fan assembly between the left and right mounting guides.

- Gently press the fan assembly back into the chassis



**Figure 13 Fan Connector and Protective Sleeve**

7. Secure the fan assembly in position by first replacing the lower retention bracket, then replacing the upper retention bracket.
8. Connect the fan lead into its connector.
9. Replace the front fascia.

## 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.



**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. The server uses one of two types of chassis:

- Type 1: Without a battery retention bracket.
- Type 2: With a battery retention bracket.

This section explains how to change the battery pack in both types of chassis.



**Note:** Replacement battery pack wires may be unwrapped, or they may be wrapped. Wire routing is identical for both, but additional care is required when the wires are not wrapped to ensure that they are correctly placed and that they do not get pinched between parts.

## Removing the battery pack from the caddy

Prepare the new battery. Separate the battery pack from the caddy (module case).

### Procedure

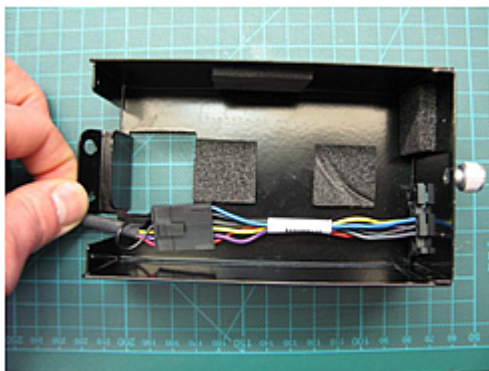
1. Loosen thumbscrew on the rear of the caddy (the side with the electrical connector).



2. Separate the caddy from the rest of the battery pack by sliding the metal cover away from the thumbscrew and lift it off the module.



3. Remove the battery pack from the caddy.
4. Disconnect the battery from the caddy by pressing down on the retention clip that holds the connector together and then separating the connector. The metal portion of the module can be returned to the supplier or be discarded.



## Removing the battery pack: type 1 chassis

Remove the NVRAM battery backup pack (type 1, no bracket).

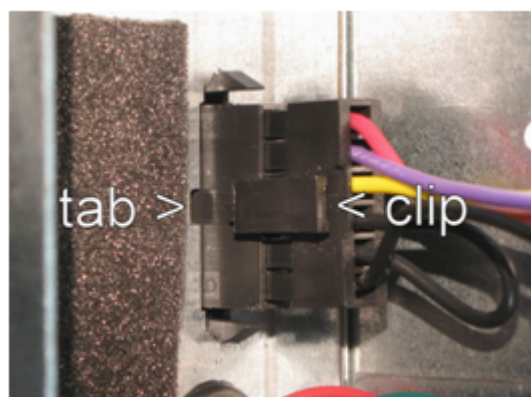


### Procedure

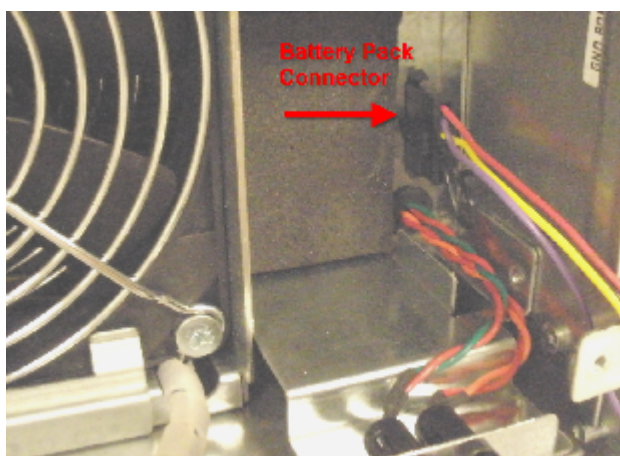
1. Make sure you have the new battery pack present.
2. Remove the fascia (see [Bezel removal on page 50](#) for more information).
3. Gently slide the old battery pack out of the server.



4. Disconnect the battery:
  - a. Carefully push in on the retention clip.
  - b. Carefully pull the connector away from the socket.



**Note:** Disconnect the battery pack by grasping the battery pack connector; do not pull on the wires.



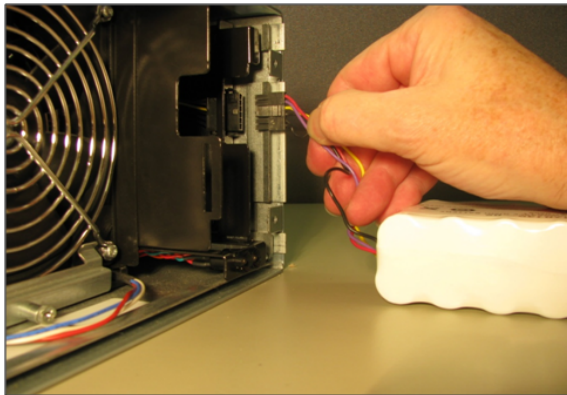
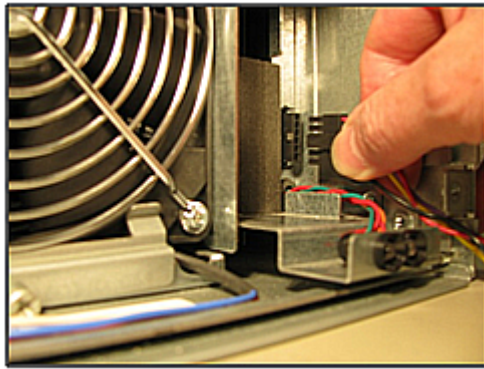
5. Properly dispose of the old battery pack in compliance with local environmental regulations, or return it to the battery pack supplier.

## Inserting the new battery pack: type 1 chassis

### Procedure

1. Plug the connector in **before** inserting the new battery pack. The connector plug must be positioned so that the retention clip is on the **left** side before pushing it in as shown.





2. To plug in the battery connector:



**Caution:** Do not force the connector into the socket. Forcing the connector into the socket when the retention tab is on the wrong side of the receptacle can cause permanent damage to the server.

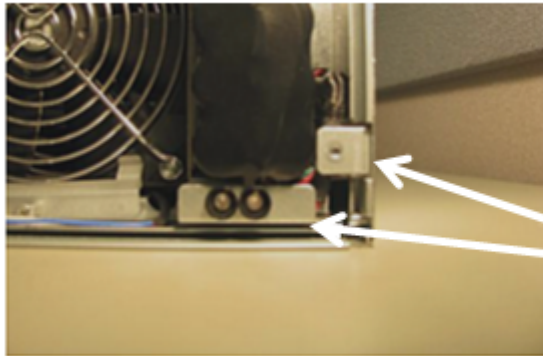
- a. Position the battery connector so that the retention clip is on the left side.
  - b. Make sure that the retention clip is aligned with the tab on the chassis receptacle.
  - c. Insert the battery connector into the chassis receptacle and push until the retention clip locks onto the retention tab.  
Do not force the plug in. When correctly aligned, it will slide in easily.
3. Carefully insert the battery pack. Ensure that the print is facing left and the cable is on the bottom.





**Note:** The new cable is wrapped in a braided sheath and may be thicker than the wires on the previous battery pack. Due to the thicker cable, you must carefully work the new battery pack into the server.

4. Carefully work with the battery connector cable so that it is along the right side of the battery compartment. It must be fully **behind** the fascia mounting tab and the LED mounting tab.

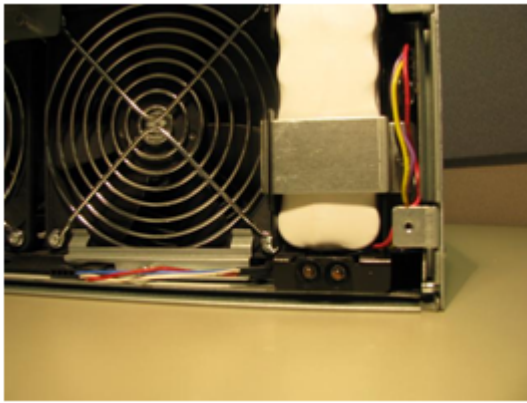


Braided cable placed behind the mounting tab and the LED tab.

5. Check the battery connector to make sure the battery is plugged in correctly.
6. Go to [Collecting system backups and diagnostics on page 62](#).

## Removing the battery pack: type 2 chassis

Remove the NVRAM battery backup pack (type 2, bracket).



### Procedure

1. Prepare the new battery. See [Removing the battery pack from the caddy on page 52](#).
2. Remove the fascia.
3. Disconnect the battery connector, located on the right side of the battery compartment.





**Note:** Disconnect the battery pack by grasping the battery pack connector; do not pull on the wires.

---

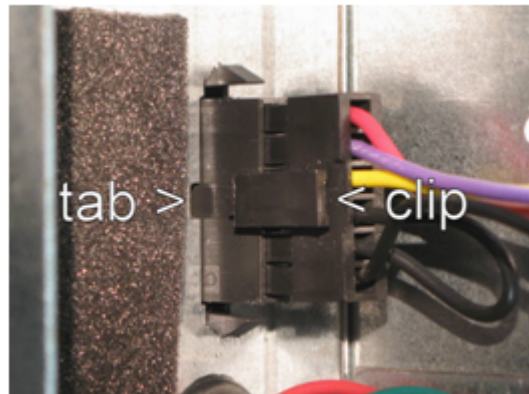
4. Remove the battery retention bracket.



5. Gently remove the old battery pack from the compartment.



6. Disconnect the battery:
  - a. Carefully press down on the retention clip.
  - b. Pull the connector away from the socket.



7. Properly dispose of the old battery pack in compliance with local environmental regulations, or return it to the battery pack supplier.

## Inserting the new battery pack: type 2 chassis

### Procedure

1. Insert the battery pack with the connector cable on the bottom and the printing on the left side.

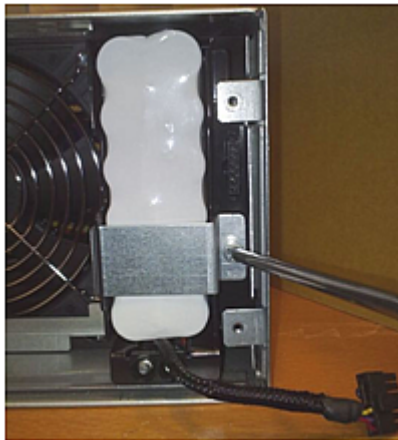


**Note:** Do not connect the battery connector yet.

2. Fit the left-side of the battery retention bracket into the slot.



3. Fasten the battery retention bracket into place.



4. Before proceeding to the next step, make sure that the clip is on the left.



5. To connect the battery:
  - a. Position the battery connector so that the retention clip is on the left side.

- b. Make sure the retention clip is aligned with the tab on the chassis receptacle.
- c. Insert the battery connector into the chassis receptacle and push until the retention clip locks onto the retention tab.

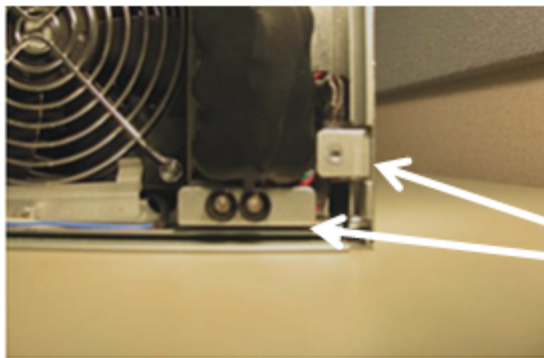


**Warning:** Do not force the connector into the receptacle.

Forcing the connector into the receptacle when the retention clip is on the wrong side of the receptacle can cause permanent damage to the server.

---

6. Carefully work with the battery connector so that it is along the right side of the battery compartment. It must be fully **behind** the fascia mounting tab and the LED mounting tab.



Braided cable placed behind the mounting tab and the LED tab.

7. Check the battery connector to make sure the battery is plugged in correctly.
8. Install the fascia or bezel (the server cover).
9. Go to [Collecting system backups and diagnostics on page 62](#).

## Collecting system backups and diagnostics

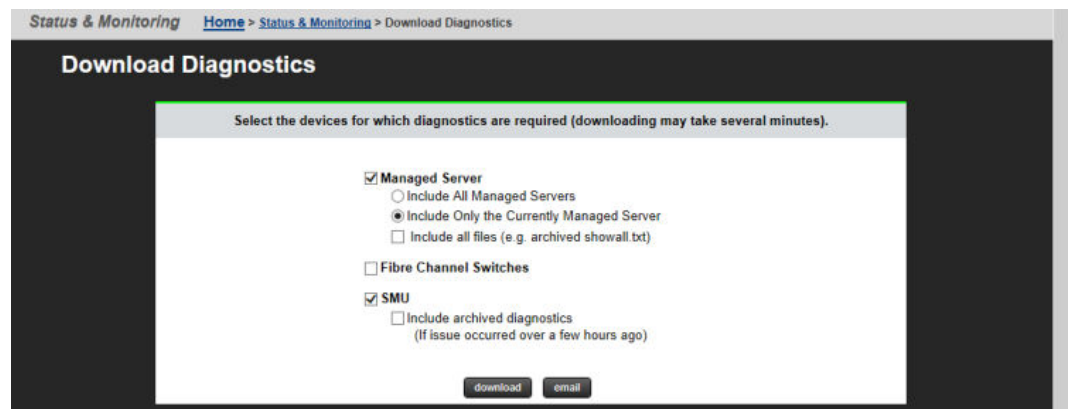
After replacing the battery, collect system backups and diagnostics.

### Procedure

1. Connect to the back-end HNAS Private Management Switch.
2. Open a browser session to the SMU. (External: 192.0.2.1; Internal: 192.0.2.2).
3. Login as Username: `admin` Password: `nasadmin`
4. Back up the Server registry (Internal SMU - this will include 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 Username: `manager` Password: `nasadmin`
  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 out of BALI into the Linux Layer.
      - c. Type `su` to change the login to root.
      - d. Password: `nasadmin`.
      - e. Restart the chassis monitor by issuing the command: `/etc/init.d/chassis-monitor restart`
      - f. Type `scc localhost` to return to the Bali 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 the GCC to open a SR for resolution.

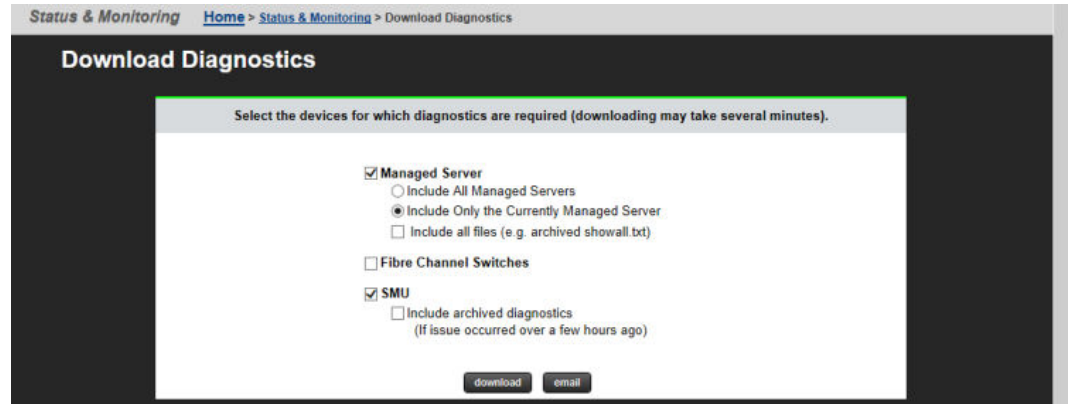
## Collecting a final diagnostic

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 Username: `admin` Password: `nasadmin`
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.

## Replacing a hard disk

If necessary, either of the hard disks in the server can be replaced. Do not attempt to replace a hard disk unless instructed to do so by customer support. Hard disk replacement is not a hot-swap operation; replacing a hard disk requires that the server be shut down and that the power cables are disconnected from the PSUs.

Hard disk replacement requires that you remove fan assemblies, and remove and replace the hard disks through the fan mounting area.

## Procedure

1. Make sure you have the new hard disk(s) present.
2. Shut down the server (see [Rebooting or shutting down a cluster on page 71](#) for more information).

3. Remove the power cables from the PSUs.  
The hard disk(s) can now be replaced.
4. Remove the left and center fan assemblies (fan 1 and fan 2). See [Replacing a fan on page 50](#) for this procedure.
5. Identify the hard disk to replace.  
Note that there are two (2) hard disks in the server. Hard disk A is on the left (behind fan assembly number 1) and hard disk B is on the right (behind fan assembly number 2). Labels on the chassis identify the disk drives.



6. Disconnect the power and SATA cables from the hard disk being replaced. (Do not remove the SATA cable from the motherboard.)



7. Remove the hard disk to be replaced.  
Each hard disk is in a carrier (bracket) held to the bottom of the chassis by a thumbscrew on the right side and a tab that fits into a slot on the chassis floor on the left side.
  - a. Remove the thumbscrew on the right side of the hard disk carrier.
  - b. Gently lift the right side of the hard disk about 1/8 inch (1/4 centimeter) and slide the disk carrier to the right.
  - c. Once the disk carrier is completely disengaged from the chassis, remove it from the server.
8. Install the replacement hard disk:



**Note:** The replacement hard disk should be mounted in the **lower** position of the carrier. If the hard disk is not mounted in a carrier, you can mount the replacement hard disk in the old carrier. If the hard disk is mounted in the upper position, it should be moved to the lower position in the carrier. In either of the cases described above, you must remove and reuse the four (4) TORX10 mounting screws that hold the hard disk in the carrier before mounting/remounting the hard disk.

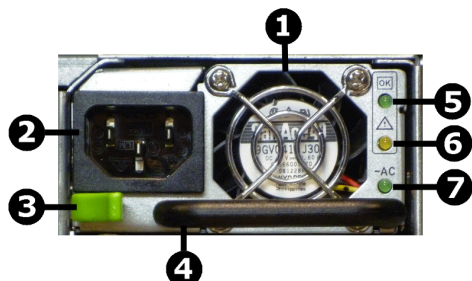
- a. Insert the tabs on the left side of the disk carrier into the slots on the floor of the server chassis.
- b. Move the carrier to the left until the tabs are fully engaged and the thumbscrew is aligned. (Note that the right side of the carrier must be elevated slightly to clear part of the chassis.)
- c. Tighten the thumbscrew to secure the drive carrier. Do not overtighten the thumbscrew.
- d. Connect the power and SATA cables to the replacement hard disk.
- 9.** Replace the fan assemblies (see [Replacing a fan on page 50](#) for this procedure).
- 10.** Replace the fascia.
- 11.** Reconnect the power cables to the PSUs.
- 12.** Start the server.
- 13.** Log in to the server as the root user.
  - a. Use SSH to connect to the server using the manager account. By default, the password for the manager account is nasadmin, but this password may have been changed.
  - b. To gain access as root, press `Ctrl-D` to exit the console, then enter `su -`. When you are prompted for the root password, enter it for the root user account. By default, the password for the root account is nasadmin, but this password may have been changed.
- 14.** Run the script `/opt/raid-monitor/bin/recover-replaced-drive.sh`, which will partition the disk appropriately, update the server's internal RAID configuration, and initiate rebuilding the RAID pair. Rebuilding the RAID pair ensures all data is accurate across both hard disks. After the script has finished, no further interaction is required. The RAID system rebuilds the disk as a background operation, and events are logged as the RAID partitions rebuild and become fully fault tolerant. The status indicator will turn to indicate normal operation (solid or flashing blue) once the RAID configuration has been repaired.
- 15.** Log out.
- 16.** Properly dispose of the old hard disk; do not attempt to re-install or re-use it.

## 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.

Item	Description
1	PSU 1
2	PSU 2



**Figure 14 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.

## 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](#)
- ☐ [Rebooting or shutting down a cluster](#)
- ☐ [Restarting an unresponsive server](#)
- ☐ [Powering down the server for maintenance](#)
- ☐ [Powering down the server for shipment or storage](#)
- ☐ [Recovering from power standby](#)

# Rebooting or shutting down a server

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

## Procedure

1. Using Web 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

**Stop File Serving**  
Stop

**Reboot**  
Reboot

**Shut Down**  
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

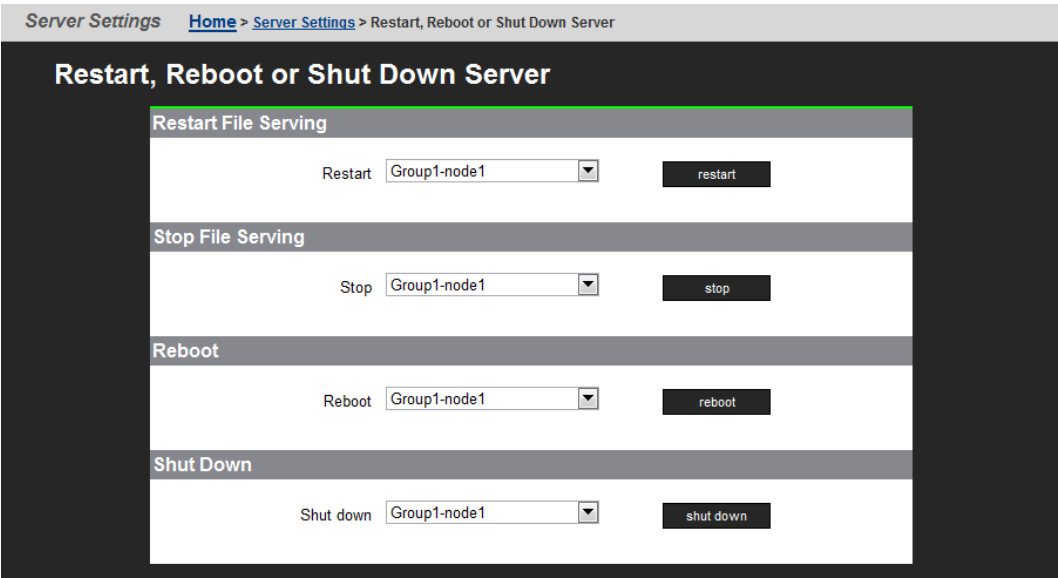
Click **restart** to restart all file serving EVSs on the server.

- 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 cluster


## Procedure

1. Using Web 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.



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

Option	Action
Restarting File Serving	<ul style="list-style-type: none"><li>• To restart all file serving EVSs on a single node, select the <b>Restart on node</b> option, use the drop-down list to select a node, and then click <b>restart</b>.</li><li>• To restart all file serving EVSs on all cluster nodes, select the <b>Restart on all nodes</b> option and then click <b>restart</b>.</li></ul>
Stop File Serving	<ul style="list-style-type: none"><li>• To stop all file serving EVSs on a single node, select the <b>Stop file serving on node</b> option, use the drop-down list to select a node and then click <b>stop</b>.</li><li>• To stop all file serving EVSs on all cluster nodes, select the <b>Stop file serving on all nodes</b> option and then click <b>stop</b>.</li></ul>
Reboot	<ul style="list-style-type: none"><li>• To reboot a single node, select the <b>Reboot node</b> option, use the drop-down list to select a node, and then click <b>reboot</b></li><li>• To reboot all cluster nodes, select the <b>Reboot all nodes</b> option and then click <b>reboot</b>.</li></ul> <div> <b>Note:</b> 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.</div>

Option	Action
Shutdown	<ul style="list-style-type: none"> <li>To shut down a single node, select the <b>Shutdown node</b> option, use the drop-down list to select a node, and then click <b>shutdown</b></li> <li>To shut down all cluster nodes, select the <b>Shutdown all nodes</b> option, and then click <b>shutdown</b>.</li> </ul> <hr/> <div>  <b>Note:</b> Clicking <b>Shutdown</b> 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. </div> <hr/>

## 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:
    1. Connect directly to the MMB as manager using ssh.
    2. If the connection succeeds, you are taken to the server OS console, where you issue the command: **bt active**
    3. 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 45](#) if you need details.

  1. Login as manager or you will get the Linux prompt, not the server OS.  
If you use root, use **ssc localhost**.
  2. Issue the command: **bt active**
4. If you are still unable to get to the server OS, perform the following steps:
  1. Check to make sure that the Bali CLI is booting successfully.
  2. Log in through the serial cable connection.



3. Tail `/var/opt/mercury-main/logs/dblog`
4. 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.
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 for maintenance

This procedure should be followed whenever a server is to be powered down and will be left off for less than a day. If, however, the system is being rebooted, this procedure is not necessary.

### Procedure

1. Shut down the server(s) as described in [Rebooting or shutting down a server on page 70](#).
2. If your system is configured with an external System Management Unit (SMU), depress the red button located on the right of the unit to turn it off (an internal SMU is turned off when the server shuts down).
3. Power off the storage subsystems, beginning with the enclosures that house the RAID controllers.
4. Power off the expansion enclosures for the storage subsystems.

## Powering down the server for shipment or storage

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

When the system is properly shut down, depending on the battery charge level, the battery may last up to one year without being charged or conditioned . See [NVRAM backup battery pack on page 36](#) for details.

Contact your representative for special instructions if servers or NVRAM battery backup packs will be in storage for more than one year. Special provisions are required for field or factory recharging and retesting of NVRAM battery backup packs.

### Procedure

1. From the NAS operating system (Bali) console, issue the command:  
`shutdown --ship --powerdown`
2. Wait until the console displays the message **Information: Server has shut down** and 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.
4. Wait 10-15 seconds, then check that the NVRAM Status LED on the rear panel of the server is off.
  - If the NVRAM status LED is off, the battery backup pack no longer powers the NVRAM, so that the battery does not drain.



**Note:** Use this state for server storage or shipment.

---

- If the NVRAM status LED is on (either on steady or flashing), press and hold the reset button for five seconds until the NVRAM Status LED begins to flash rapidly. Release the reset button to disable the battery. The NVRAM Status LED goes out.



**Note:** The NVRAM contents are lost. The battery is re-enabled when power is restored to the server.

---

## Recovering from power standby

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

The server will enter a standby power state due to any the following:

- The `shutdown --ship --powerdown` command has been issued.
- The PWR button was 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:

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



# Hard disk replacement

This section provides instructions and information about replacing the hard disks in the following servers:

- Hitachi NAS Platform, Model 3090
- Hitachi NAS Platform, Model 3080



**Note:** In the remainder of this document, all server models are referred to as a "NAS server."

- ☐ [Intended Audience](#)
- ☐ [Downtime considerations for hard disk replacement](#)
- ☐ [Requirements for hard disk replacement](#)
- ☐ [Overview of the Procedure](#)
- ☐ [Accessing Linux on the server and node](#)
- ☐ [Step1: Performing an Internal Drive Health Check](#)
- ☐ [Step 2: Gathering information about the server or node](#)
- ☐ [Step 3: Backing up the server configuration](#)
- ☐ [Step 4: Locating the server](#)
- ☐ [Step 5: Save the preferred mapping and migrate EVSs \(cluster node only\)](#)
- ☐ [Step 6: Replacing a Server's Internal Hard Disk](#)
- ☐ [Step 7: Synchronizing server's new disk](#)

- ☐ [Step 8: Replacing the server's second disk](#)
- ☐ [Step 9: Synchronizing the second new disk](#)
- ☐ [Step 10: Restore EVSs \(cluster node only\)](#)

## Intended Audience

These instructions are intended for Hitachi field personnel, and appropriately trained authorized third-party service providers. To perform this procedure, you must be able to:

- Use a terminal emulator to access the HNAS server CLI and Bali console.
- Log in to Web Manager (the HNAS server GUI).
- Migrate EVSs.
- Physically remove and replace fan assemblies and hard disks.



**Note:** You may also be required to upgrade the firmware. See [Requirements for hard disk replacement on page 80](#) for information about the minimum required firmware version.

---

## Downtime considerations for hard disk replacement

Downtime is required because hard disk replacement is not a hot-swap operation. Replacing a hard disk requires that you shut down the server, disconnect the power cables from the Power Supply Units (PSUs), physically replace server parts, and start the process of rebuilding the server's internal RAID subsystem.

- Standalone server

The complete disk replacement process requires approximately 2.5 hours, and the server will be offline during this time. You could restore services in approximately 1.5 hours by restoring services before the second disk of the server's RAID subsystem has completed synchronizing.



**Caution: Early service restoration is not recommended.** If the second disk of the internal RAID subsystem has not completed synchronizing, and there is a disk failure, you may lose data. Do not restore services before the RAID subsystem has been completely rebuilt unless the customer understands, and agrees to, the risks involved in an early restoration of services.

---

- Cluster node

The complete disk replacement process requires approximately 2.5 hours for each node, and the node will be offline during this time. You can, however, replace a node's internal hard disks with minimal service interruption for the customer by migrating file serving EVSs between nodes. Migrating EVSs allows the cluster to continue to serve data in a degraded state. Using EVS migration, each EVS will be migrated twice, once away from the node, and then to return the EVS to the node after hard disk replacement.

## Requirements for hard disk replacement

Before replacing the hard disks, ensure that you have:

- Completed a disk health check. This health check should be performed at least one week in advance of the planned disk replacement. See [Step1: Performing an Internal Drive Health Check on page 83](#) for more information.
- The following tools and equipment:
  - #2 Phillips screwdriver.
  - A laptop that can be used to connect to the server's serial port. This laptop must have an SSH (Secure Shell) client or terminal emulator installed. The SSH client or terminal emulator must support the UTF-8 (Unicode) character encoding. See [Accessing Linux on the server and node on page 81](#) for more information.
  - A null modem cable.
  - An Ethernet cable.
  - Replacement hard disks.
  - Minimum firmware revision of 7.0.2050.17E2:  
If the system firmware version is older than 7.0.2050.17E2, update it to the latest mandatory or recommended firmware level before beginning the hard disk replacement procedure. Refer to the *Server and Cluster Administration Guide* for more information on upgrading firmware.
- The password for the "manager," "supervisor," and "root" user accounts on the server with the hard disks to be replaced.
- A maintenance period as described in [Downtime considerations for hard disk replacement on page 79](#).
- Access to the Linux operating system of the server/node. See [Accessing Linux on the server and node on page 81](#) for more information.

## Overview of the Procedure

This section provides a high-level overview of the hard disk replacement process. See the sections referenced in each step for detailed instructions.



**Note:** Approximately one week before starting this disk replacement, perform the disk health check. See "Step 1: Performing an Internal Drive Health Check" on page 55 for more information. The hard disk replacement process is as follows:

### Procedure

1. Perform a health check: See [Step1: Performing an Internal Drive Health Check on page 83](#) for more information.



2. Gather and record IP address and disk status information about the server: See [Step 2: Gathering information about the server or node on page 88](#).
3. Back up the server's configuration: See [Step 3: Backing up the server configuration on page 90](#).
4. Physically locate the server: See [Step 4: Locating the server on page 90](#).
5. For cluster nodes, save the preferred mapping, and migrate EVSs to a different node in the cluster: See [Step 5: Save the preferred mapping and migrate EVSs \(cluster node only\) on page 91](#).
6. Physically replace the first disk: See [Step 6: Replacing a Server's Internal Hard Disk on page 93](#).
7. Synchronize the first new disk and the existing disk: See [Step 7: Synchronizing server's new disk on page 100](#).
8. Physically replace the server's second hard disk: See [Step 8: Replacing the server's second disk on page 101](#).
9. Synchronize the second new disk and the first new disk: See [Step 9: Synchronizing the second new disk on page 101](#).
10. For cluster nodes, restore migrated EVSs to their preferred node: See [Step 10: Restore EVSs \(cluster node only\) on page 101](#).

When performing parts of the disk replacement process, you must access the Linux operating system and/or the Bali console of the NAS server/node. Instructions on how to access these components are provided in [Accessing Linux on the server and node on page 81](#)

## Accessing Linux on the server and node

To run some of the commands, you must access the Linux layer of the NAS server or node using one of two methods:

- The serial (console) port, located on the rear panel of the server. See [Using the Serial \(Console\) Port on page 81](#) for more information.
- SSH connection. See [Using SSH for an Internal SMU on page 82](#) or [Using SSH for an External SMU on page 82](#),

### Using the Serial (Console) Port

Use the terminal emulator and null modem cable to access the NAS server's Linux operating system.

#### Procedure

1. Configure the terminal emulator as follows:
  - Speed: 115200
  - Data bits: 8 bits
  - Parity: None
  - Stop bits: 1

- Flow control: No flow control



**Note:** To increase readability of text when connected, set your terminal emulator to display 132 columns.

---

2. Log in as '**root**.'
3. Connect to localhost using the SSC (server control) utility to run the Bali commands by entering the command:  
`ssc localhost`

## Using SSH for an Internal SMU

These instructions apply if you have an internal SMU. If you have an external SMU, see [Using SSH for an External SMU on page 82](#).

### Procedure

1. Use SSH to log in to the internal SMU as '**manager**.' Enter the following command:  
`ssh manager@[IP Address]`  
where *[IP Address]* is the IP address of the NAS server administrative service EVS.
2. Enter the password for the '**manager**' user account.  
By default, the password for the manager account is "nasadmin", but this password might have been changed.  
This logs you into the Bali console.
3. Access the Linux prompt by exiting the Bali console. Enter the following command:  
`exit`  
or press the Ctrl+D keys.
4. Log in as the '**root**' user. Enter the following command:  
`su -; [password]`  
where *[password]* is the password for the root user account.

## Using SSH for an External SMU

These instructions apply if you have an external SMU. If you have an internal SMU, see [Using SSH for an Internal SMU on page 82](#).

### Procedure

1. SSH into the external SMU as manager. Enter the following command:  
`ssh manager@[IP Address]`  
where *[IP Address]* is the IP address of the NAS server/node.

This logs you into the siconsole.

2. Select the system (the server or the cluster node) that has the hard disks to be replaced.

This logs you into the Bali console.

3. Synchronous Disaster Recovery Cluster the cluster node IP addresses. Enter the following command:

```
ipaddr
```

4. Record the cluster IP addresses.

5. Access the Linux prompt by exiting the Bali console. Enter the following command:

```
exit
```

or press the Ctrl+D keys.

This logs you into the siconsole.

6. Quit to the SMU's Linux prompt. Enter the following command:

```
q
```

7. Access cluster IP address using SSH and logging in as the 'supervisor' user. Enter the following command:

```
ssh supervisor@[Cluster_IP_Address]
```

where [Cluster\_IP\_Address] is the IP address of the NAS server/node.

8. Enter the password for the 'supervisor' user. By default, the password for the 'supervisor' user account is the "supervisor," but this may have been changed.

9. Log in as the 'root' user. Enter the following command:

```
su -; [password]
```

where [password] is the password for the root user account.

You are now at the Linux prompt.

## Step1: Performing an Internal Drive Health Check

The health check evaluates both internal disks to determine if there are any pending disk failures. Perform the health check twice:

- Approximately one week before hard disk replacement to allow time to resolve any errors before running the disk replacement procedure.
- When you start the hard disk replacement procedure to make sure the disks are ready for the replacement.

The health check includes retrieving and evaluating the disk's SMART (Self-Monitoring, Analysis, and Reporting Technology) information and reviewing the server's internal RAID subsystem status.

If you find errors on either of the two disks, note the disk and make sure that the disk with the errors is the first one to be replaced. If both disks have errors, contact technical support and escalate the errors based on the health check output.

To run the health check:

## Procedure

1. Log in to each node/server using the SSH process, which is described in [Accessing Linux on the server and node on page 81](#).
2. Verify the mapping of physical disks to SCSI devices.  
To display the mapping between the physical drive and the dev/sdX name, there are symlinks displayed by the output from the `ls -l /dev/disk/by-path` command.

In the example below, the portion of the output that displays the mapping between the SATA port and the SCSI device number is underlined. This example shows the standard post boot situation, where SATA port 0 (Physical Drive A) is `/dev/sda` and port 2 (Physical Drive B) is `/dev/sdb`.

```
mercury100:~$ ls -l /dev/disk/by-path
total 0
lrwxrwxrwx 1 root root 9 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-0:0:0:0 -> ../../sda
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-0:0:0:0-part1 -> ../../sda1
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-0:0:0:0-part2 -> ../../sda2
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-0:0:0:0-part3 -> ../../sda3
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-0:0:0:0-part5 -> ../../sda5
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-0:0:0:0-part6 -> ../../sda6
lrwxrwxrwx 1 root root 9 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-2:0:0:0 -> ../../sdb
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-2:0:0:0-part1 -> ../../sdb1
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-2:0:0:0-part2 -> ../../sdb2
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-2:0:0:0-part3 -> ../../sdb3
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-2:0:0:0-part5 -> ../../sdb5
lrwxrwxrwx 1 root root 10 2011-06-27 12:17 pci-0000:00:1f.2-
scsi-2:0:0:0-part6 -> ../../sdb6
mercury100:~$
```

3. Retrieve the SMART data for each of the internal disks by entering the following commands:
  - For disk A: `smartctl -a /dev/sda`
  - For disk B: `smartctl -a /dev/sdb`
4. Review the Information section of the retrieved data to verify that the SMART support is available and enabled on both disks.

In the sample output from the `smartctl` command below, the portion of the information that indicates SMART support is underlined:

```
=== START OF INFORMATION SECTION ===
Device Model:          ST9250610NS
Serial Number:         9XE00JL3
```

```

Firmware Version: SN01
User Capacity:    250,059,350,016 bytes
Device is:        Not in smartctl database [for details use:
-P showall]
ATA Version is:   8
ATA Standard is:  ATA-8-ACS revision 4
Local Time is:    Thu Mar  3 12:48:44 2011 PST
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

```

**5. Scroll past the Read SMART Data section, which looks similar to the following example.**

```

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

General SMART Values:
Offline data collection status:  (0x82) Offline data
collection activity
                                was completed
without error.
                                Auto Offline Data
Collection: Enabled.
Self-test execution status:      (   0) The previous self-
test routine completed
                                without error or no
self-test has been run.
Total time to complete Offline
data collection:                 ( 634) seconds.
Offline data collection
capabilities:                     (0x7b) SMART execute
Offline immediate.
                                Auto Offline data
collection on/off
                                support.
                                Suspend Offline
collection upon new
                                command.
                                Offline surface scan
supported.
                                Self-test supported.
                                Conveyance Self-test
supported.
                                Selective Self-test
supported.
SMART capabilities:              (0x0003) Saves SMART data
before entering
                                power-saving mode.
                                Supports SMART auto
save timer.
Error logging capability:        (0x01) Error logging
supported.
                                General Purpose
Logging supported.
Short self-test routine
recommended polling time:        (   1) minutes.
Extended self-test routine
recommended polling time:        (  49) minutes.
Conveyance self-test routine

```

recommended polling time: ( 2) minutes.  
 SCT capabilities: (0x10bd) SCT Status supported.  
 SCT Feature Control  
 supported.  
 SCT Data Table  
 supported.

6. Review the SMART Attributes Data section of the retrieved data to verify that there are no "Current\_Pending\_Sector" or "Offline\_Uncorrectable" events on either drive.

In the sample output from the smartctl command below, the portion of the information that indicates "Current\_Pending\_Sector" or "Offline\_Uncorrectable" events is underlined:

```
SMART Attributes Data Structure revision number: 10
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH
TYPE      UPDATED    WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000f   080    064    044    Pre-
fail Always - 102792136
  3 Spin_Up_Time            0x0003   096    096    000    Pre-
fail Always - 0
  4 Start_Stop_Count        0x0032   100    100    020
Old_age Always - 13
  5 Reallocated_Sector_Ct   0x0033   100    100    036    Pre-
fail Always - 0
  7 Seek_Error_Rate         0x000f   065    060    030    Pre-
fail Always - 3326385
  9 Power_On_Hours          0x0032   100    100    000
Old_age Always - 156
 10 Spin_Retry_Count        0x0013   100    100    097    Pre-
fail Always - 0
 12 Power_Cycle_Count       0x0032   100    100    020
Old_age Always - 13
184 Unknown_Attribute       0x0032   100    100    099
Old_age Always - 0
187 Reported_Uncorrect      0x0032   100    100    000
Old_age Always - 0
188 Unknown_Attribute       0x0032   100    100    000
Old_age Always - 0
189 High_Fly_Writes        0x003a   100    100    000
Old_age Always - 0
190 Airflow_Temperature_Cel 0x0022   074    048    045
Old_age Always - 26 (Lifetime Min/Max 25/27)
191 G-Sense_Error_Rate      0x0032   100    100    000
Old_age Always - 0
192 Power-Off_Retract_Count 0x0032   100    100    000
Old_age Always - 12
193 Load_Cycle_Count        0x0032   100    100    000
Old_age Always - 13
194 Temperature_Celsius     0x0022   026    052    000
Old_age Always - 26 (0 20 0 0)
195 Hardware_ECC_Recovered  0x001a   116    100    000
Old_age Always - 102792136
197 Current_Pending_Sector 0x0012   100    100    000
Old_age Always - 0
198 Offline_Uncorrectable 0x0010   100    100    000
Old_age Offline - 0
```

```
199 UDMA_CRC_Error_Count      0x003e    200    200    000
Old_age      Always          -           0
```

If the RAW\_VALUE for "Current\_Pending\_Sector" or "Offline\_Uncorrectable" events are more than zero, this indicates that those events have been detected, and that the drive may be failing.

**7. Check the SMART Error log for any events.**

In the sample output from the `smartctl` command below, the portion of the information that indicates SMART Error Log events is underlined:

```
SMART Error Log Version: 1
No Errors Logged
```

**8. Validate all self test short and extended tests have passed.**

In the sample output from the `smartctl` command, the portion of the information that indicates SMART Self-test log events is underlined:

```
SMART Self-test log structure revision number 1
Num  Test_Description      Status                    Remaining
LifeTime(hours)  LBA_of_first_error
# 1  Short offline          Completed without error
00%                143                -
# 2  Short offline          Completed without error
00%                119                -
# 3  Short offline          Completed without error
00%                94                 -
# 4  Short offline          Completed without error
00%                70                 -
# 5  Extended offline       Completed without error
00%                46                 -
# 6  Short offline          Completed without error
00%                21
```

If you find that one disk has no errors, but the other disk does have errors, replace the disk **with** errors first. If you find errors on both disks, contact technical support and provide them with the `smartctl` output.

**9. Perform the RAID subsystem health check to review the current status of the RAID subsystem synchronization. Enter the following command:**

```
cat /proc/mdstat outout

Group5-node1:~# cat /proc/mdstat
Personalities : [raid1]
md1 : active raid1 sda6[0] sdb6[1] <-- Shows disk and
partition (volume) status
      55841792 blocks [2/2] [UU] <-- [UU] = Up/Up and [U_] =
Up/Down
      bitmap: 1/1 pages [4KB], 65536KB chunk

md0 : active raid1 sda5[0] sdb5[1]
      7823552 blocks [2/2] [UU]
      bitmap: 1/1 pages [4KB], 65536KB chunk

md2 : active raid1 sda3[0] sdb3[1]
      7823552 blocks [2/2] [UU]
      bitmap: 0/1 pages [0KB], 65536KB chunk

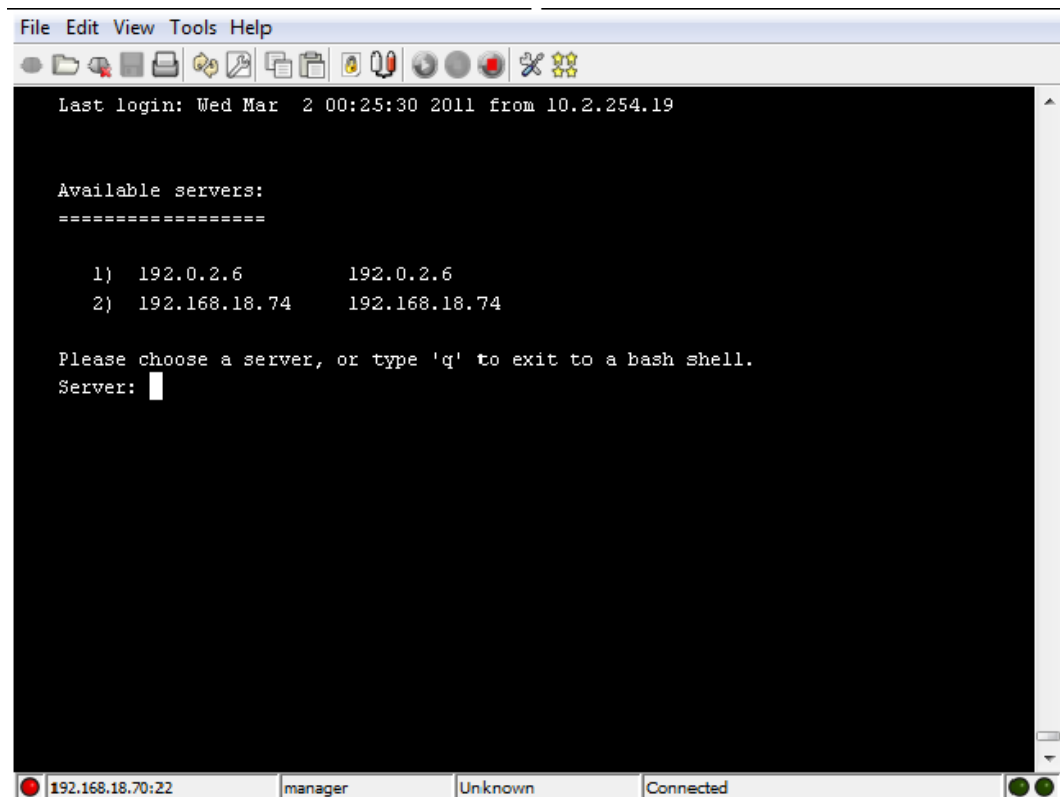
unused devices: <none>
Group5-node1:~#
```

## Step 2: Gathering information about the server or node

Before shutting down the server/node to replace disks, you must gather and record information about the related IP addresses and check the status and synchronization of the devices. To obtain this information:

### Procedure

1. Log in to the Bali console. See [Accessing Linux on the server and node on page 81](#).
2. Select the server or node that has the disks you want to replace.



3. Record the IP Address of the system you choose.
4. Run the `evs list` command.
  - For a single-node cluster or a standalone server, record the administrative services EVS IP address.



- For a multi-node cluster, record all cluster node IP addresses.

```

File Edit View Tools Help
Available servers:
=====

1) 192.0.2.3      192.0.2.3

Please choose a server, or type 'q' to exit to a bash shell.
Server: 1

Bali Console
Server name : Group1-model
MAC ID : D4-28-DD-99-3C-A4
Group1-model:~$ evs list

Node EVS ID   Type      Label Enabled Status      IP Address Port
-----
1      0   Cluster  Group1-model  Yes Online   192.0.2.200 eth1
1      0   Admin   Group1-admin  Yes Online   192.0.2.3   eth1
                        192.168.18.49 ag1
1      1   Service  G1-EVS1      Yes Online   192.168.18.41 ag1
1      2   Service  G1-EVS-target Yes Online   192.168.18.42 ag1
2      0   Cluster  Group1-node2  Yes Online   192.0.2.201 eth1

Group1-model:~$

```

5. Run the `chassis-drive-status` command
6. Review the values in the **Status** and **% Rebuild** columns for each device.

The response to the command should be similar to the following:

Device	Status	% Used	Size (4k blks)	Used (4k blks)
% Rebuild				
0	Good	32	3846436	1266962
Synchronized				
1	Good	3	12302144	463572
Synchronized				
2	Good	0	0	0
Synchronized				
Success				

For each device, the **Status** should be “Good” and the **%Rebuild** should be “Synchronized.”

- If the values are correct, repeat the health check, as described in [Step1: Performing an Internal Drive Health Check on page 83](#).
- If the values are not correct, run the `trouble chassis-drive` command. If the command response displays “No faults found,” repeat the health check, as

described in [Step1: Performing an Internal Drive Health Check on page 83](#). If the command response displays issues, resolve them if possible, or contact technical support for assistance.

## Step 3: Backing up the server configuration

Backing up the server's configuration for an internal or external SMU saves the server's configuration, including the SI configuration. When backing up a server with an internal SMU, the configuration backup also includes a ZIP file of the SMU configuration.

### Procedure

1. Connect your laptop to the management Ethernet switch using an Ethernet cable.
2. Log in to Web Manager.
3. Navigate to **Home > Server Settings > Configuration Backup & Restore**.
4. Click **backup** to save the configuration file to your laptop.
5. Verify that the backup file is complete and make sure the file size is not 0 bytes

## Step 4: Locating the server

Before shutting down the server/node to replace disks, you must physically locate the server.

### Procedure

1. Run the `led-identify-node X` command.  
where *X* is the number of cluster node (the pnode-id) to identify.

The result of this command is that the server's fault and power LEDs (located on the left side of the server's rear panel) flash simultaneously.



2. Physically locate the server that has the disks to be replaced. After you have identified the server, press any key to stop the LEDs from flashing.

## Step 5: Save the preferred mapping and migrate EVSs (cluster node only)

If replacing the hard disks in a standalone server, skip this step. If replacing the hard disks in a cluster node, before shutting down the node to replace disks, migrate the EVSs to another node. You can migrate an individual EVS to a different node within the same cluster, or you can migrate all EVSs to another server or another cluster.

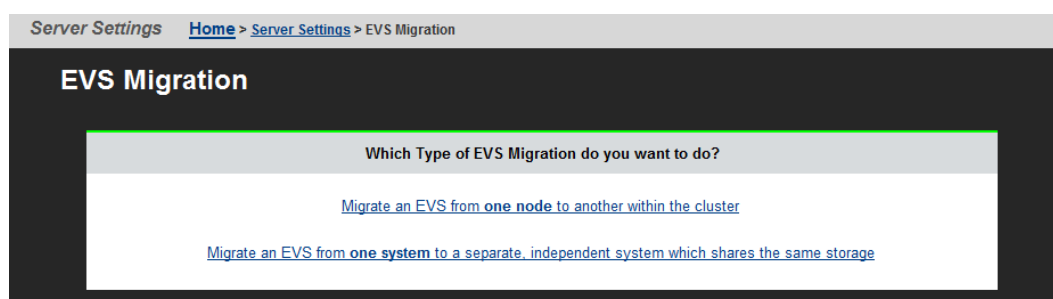
The current mapping of EVSs to cluster nodes can be preserved, and the saved map is called a preferred mapping. Saving the current EVS-to-cluster configuration as the preferred mapping helps when restoring EVSs to cluster nodes. For example, if a failed cluster node is being restored, the preferred mapping can be used to restore the original cluster configuration.

### Procedure

1. Connect your laptop to the customer's network.
2. Using a browser, go to `http://[SMU_IP_Address]/` where `[SMU_IP_Address]` is the IP address of the SMU (System Management Unit) managing the cluster
3. Log into Web Manager as user manager. By default, the password is nasadmin but this password may have been changed.
4. Navigate to **Home > Server Settings > EVS Migration** to display the EVS Migration page.

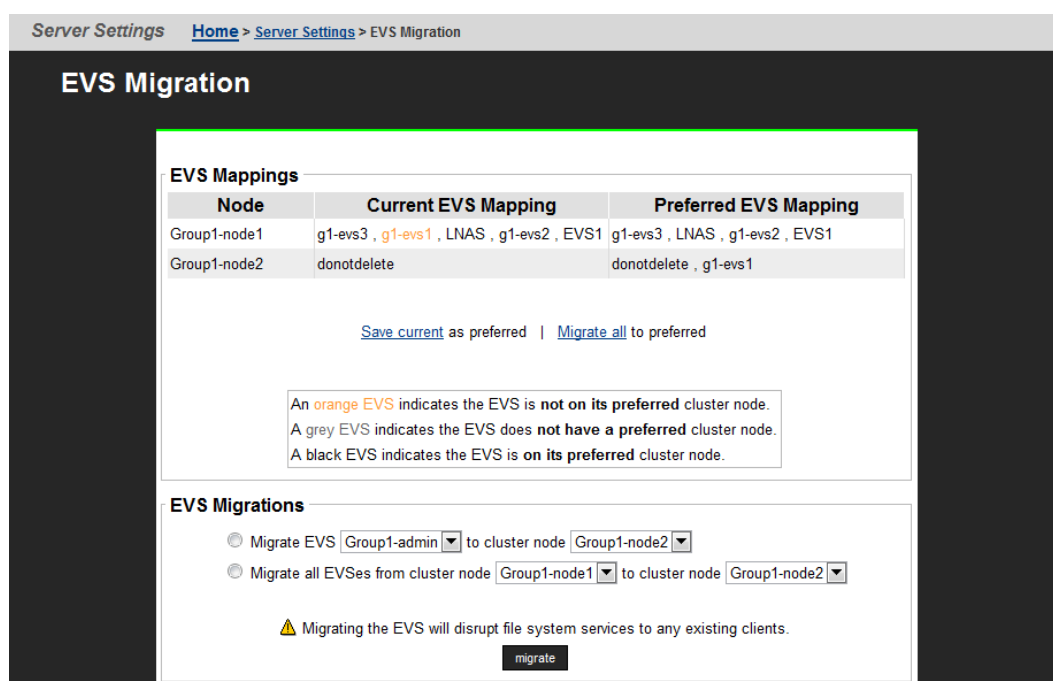


**Note:** If the SMU is currently managing a cluster and at least one other cluster or standalone server, the following page appears:



If this page does appear, click **Migrate an EVS from one node to another within the cluster** to display the main EVS Migration page.

If the SMU is managing one cluster and no standalone servers, the main EVS Migration page appears:



5. Migrate the EVSs between the cluster nodes until the preferred mapping has been defined. The current mapping is displayed in the Current EVS Mappings column of the EVS Mappings section of the page.
6. Save the current EVS-to-cluster node mapping by clicking **Save current as preferred** in the EVS Mappings section.
7. Migrate EVSs as required:
  - To migrate all EVSs between cluster nodes:
    - a. Select Migrate all EVS from **cluster node** \_\_\_\_ **to cluster node** \_\_\_\_.

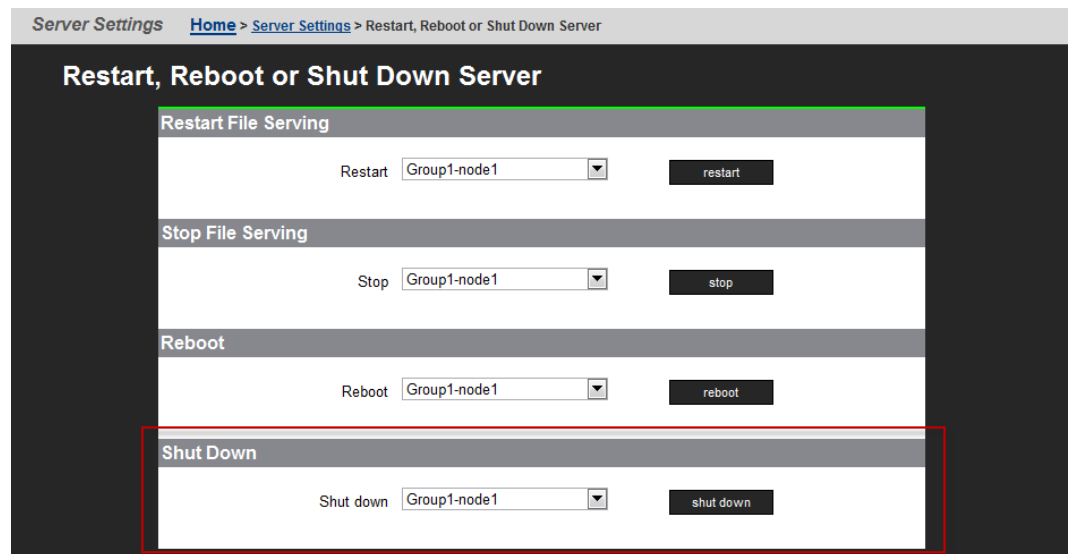
- b. From the first drop-down list, select the cluster node from which to migrate all EVS.
- c. From the second drop-down list, select the cluster node to which the EVSs will be migrated.
- d. Click **Migrate**.
  - To migrate a single EVS to a cluster node:
    - a. Select **Migrate EVS \_\_\_\_ to cluster node \_\_\_\_**.
    - b. From the first drop-down list, select the cluster node to migrate.
    - c. From the second drop-down list, select the cluster node to which the EVS will be migrated.
    - d. Click **Migrate**.

## Step 6: Replacing a Server's Internal Hard Disk

Because physically replacing hard disks is not a hot-swap operation, you must shut down the server and disconnect the power cables from the PSUs before beginning physical replacement.

### Procedure

1. Shut down the server.  
Using Web Manager, go to the Server Settings page, and:
  - For a cluster node, navigate to **Home > Restart, Reboot or Shutdown Server > Shutdown**.



- For a standalone server, navigate to **Home > Restart, Reboot or Shutdown Server > Shutdown**.
- Using the CLI, shut down the server using the following command:  
`shutdown --powerdown --ship -f`

2. Wait for the status LEDs on the rear panel of the server to stop flashing, which may take up to five (5) minutes.  
If the LEDs do not stop flashing after five minutes, make sure the Linux operating system has shut down by looking at your terminal emulator program. If Linux has not shut down, enter the `shutdown now` command.



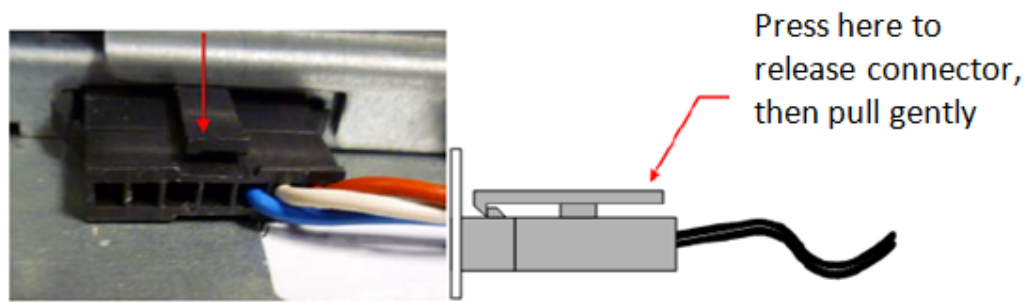
3. Remove the power cables from the PSUs.
4. Remove the fascia. See [Bezel removal on page 50](#) for details.
5. Remove the fan.

Typically, hard disk "B" is replaced before hard disk "A." Hard disk "B" is behind fan assembly number 2 (the center fan), Hard disk "A" is behind fan assembly number 1 (the left fan).

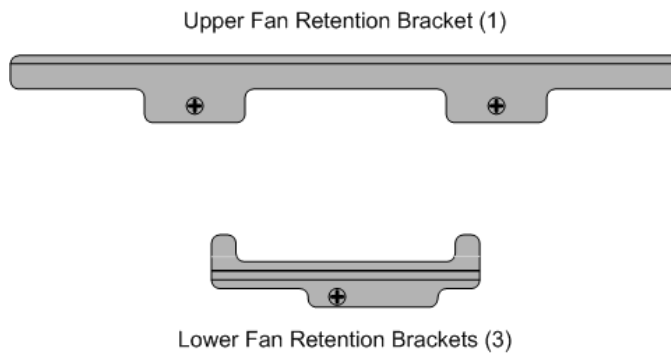


**Caution:** After one hard disk is replaced, you must restart the server and resynchronize its internal RAID subsystem before replacing the second hard disk. See [Step 7: Synchronizing server's new disk on page 100](#) for more information.

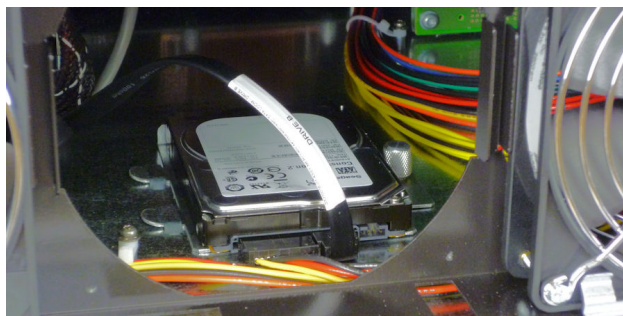
6. Disconnect the fan power connector by pressing down on the connector's retention latch and gently pulling the connector apart.



7. Remove the upper and lower fan retention brackets.

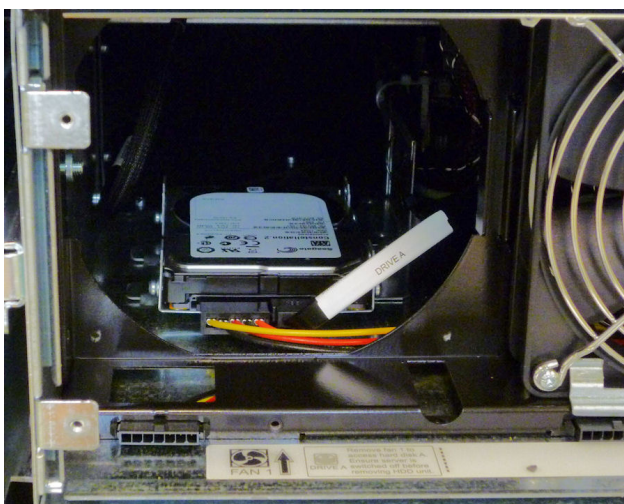


- When replacing hard disk B, remove the upper fan retention bracket and the lower fan retention bracket under fan assembly 2 (the center fan assembly).
  - When replacing hard disk A, remove the upper fan retention bracket and the lower fan assembly bracket under fan assembly 1 (the left fan assembly).
8. Remove the fan assembly covering the disk you want to replace.

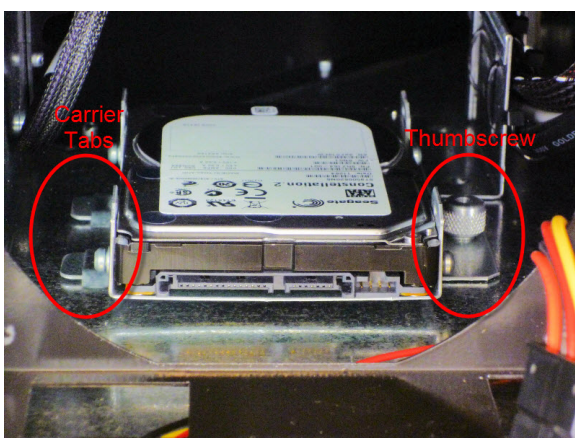


When replacing hard disk B, remove fan assembly 2 (the center fan assembly). Hard disk B should now be visible.





The hard disk is in a carrier (bracket) held to the bottom of the chassis by a thumbscrew on the right side and tabs that fit into slots on the chassis floor on the left side.



**Note:** The carrier used for replacement hard disks may be different than the carrier holding the old hard disks. The new carriers fit into the same place and in the same way as the older carriers.



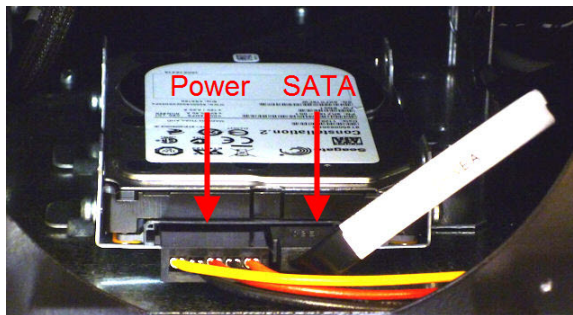
- Old carrier: the hard disk is mounted through tabs on the sides of the carrier.



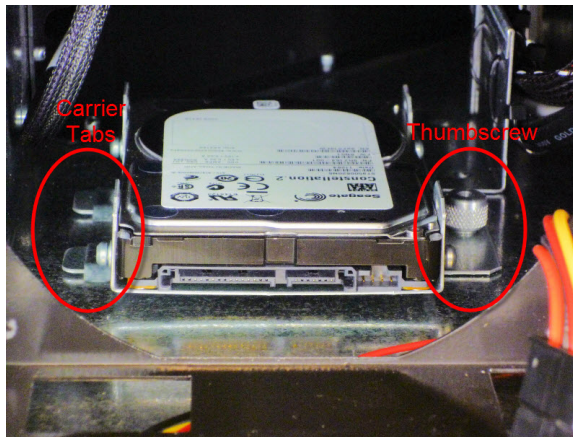
- New carrier: the hard disk is mounted through the bottom plate of the carrier.



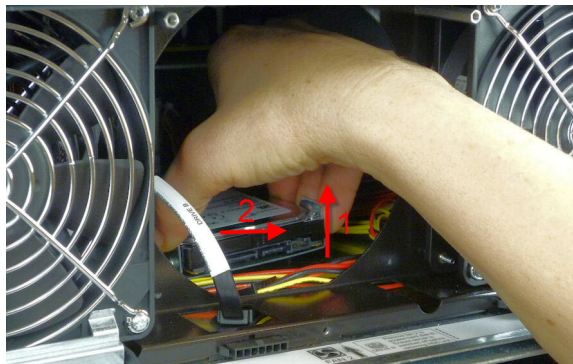
- 
9. Disconnect the power and SATA cables from the hard disk.



10. Loosen the thumbscrew on the right side of the hard disk carrier. Note that the thumbscrew cannot be removed from the carrier.



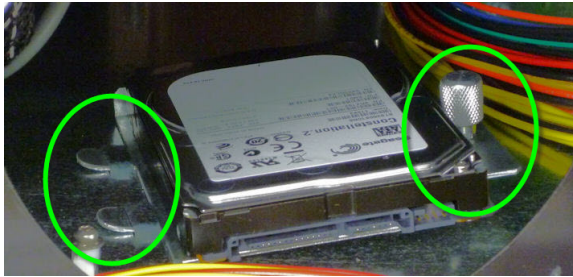
- 11.** Gently lift the right side of the hard disk carrier and slide it to the right to disengage the tabs on the left side of the carrier.



- 12.** Once the disk carrier is completely disengaged from the chassis, remove it from the server, label it appropriately (for example, "server X, disk A"), and store it in a safe location.
- 13.** To install the replacement hard disk, lift the right side of the carrier until you can insert the tabs on the left side of the disk carrier into the slots on the floor of the server chassis.



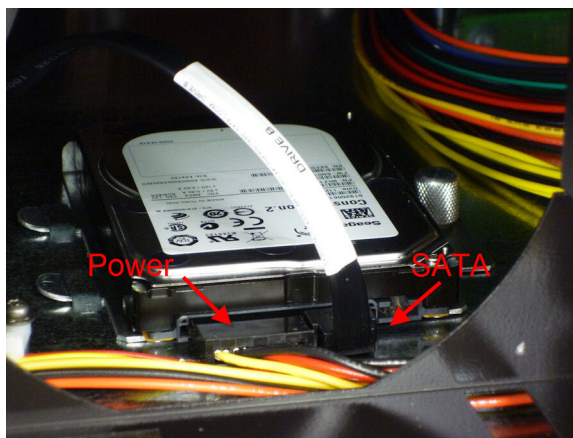
- 14.** Move the carrier to the left until the ends of the tabs are visible and the thumbscrew is aligned to fit down onto the threaded stud.



- 15.** Tighten the thumbscrew to secure the disk carrier. Do not over tighten the thumbscrew.



- 16.** Connect the power and SATA cables to the replacement hard disk.



- 17.** Reinstall the fan in the mounting slot, with the cable routed through the chassis cut-out.



18. Reinstall the fan retention brackets. Do not over tighten the screws.
19. Reconnect the fan cable.
20. If you replaced only the first hard disk, continue with the next step. If you have replaced both disks, reinstall the fascia.
21. Reconnect the power cables to the PSUs.  
When the server starts, the LEDs on the front of the server flash quickly, indicating that the server is starting up.

## Step 7: Synchronizing server's new disk

After replacing a hard disk, the new disk in the server's internal RAID subsystem must be synchronized with the older disk.

### Procedure

1. Wait until the LEDs on the front of the server slow to indicate normal activity.
2. Use a serial cable connected to the serial (console) port of the server to access the Bali console.
3. Once you have successfully logged in, select the server or node that has the disks you want to synchronize.
4. Run the `chassis-drive-status` command, and look at the values in the **Status** and **% Rebuild** columns for each device.
  - The values in the **Status** column should be "Invalid."
  - The **% Rebuild** column should not display any values.
5. Run the script `/opt/raid-monitor/bin/recover-replaced-drive.sh`. This script partitions the replacement disk appropriately, updates the server's internal RAID configuration, and initiates rebuilding the replaced disk.  
The RAID system rebuilds the disk as a background operation, which takes approximately 50 minutes to complete. Events are logged as the RAID partitions rebuild and become fully fault tolerant.
6. Monitor the rebuilding process by running the `chassis-drive-status` command, and check the values in the **Status** column for each device. The values in the **Status** column should be:
  - "Good" for synchronized volumes.
  - "Rebuilding" for the volume currently being synchronized.
  - "Degraded" for any volume(s) that have not yet started the synchronization process.

7. Once the rebuild process has successfully completed, run the trouble `chassis-drive` command.  
  
If the command response displays issues, resolve them if possible, or contact technical support for assistance.  
  
If the command response displays "No faults found," continue the disk replacement process by replacing the second hard disk.
8. Shut down the server.

## Step 8: Replacing the server's second disk

Once the server's first hard disk has been replaced and synchronized, replace the second disk. Refer to [Step 6: Replacing a Server's Internal Hard Disk on page 93](#) for the steps required to replace the server's second hard disk.

## Step 9: Synchronizing the second new disk

Once the server's second hard disk has been replaced, synchronize the server's second hard disk to restore the integrity of the server's internal RAID subsystem. Refer to [Step 7: Synchronizing server's new disk on page 100](#) for the steps required to synchronize the server's second hard disk.

Once the second hard disk is synchronized, log out by entering the `exit` command or pressing the Ctrl+D keys.

## Step 10: Restore EVSs (cluster node only)

If replacing the hard disks in a standalone server, skip this step. If replacing the hard disks in a cluster node, return each of the EVSs to its preferred node (the node with the replaced disks).

The preferred mapping of EVSs to cluster nodes should have been saved in [Step 5: Save the preferred mapping and migrate EVSs \(cluster node only\) on page 91](#). To return each EVSs to its preferred node using the preferred mapping:

### Procedure

1. Connect your laptop to the customer's network.
2. Using a browser, go to `http://[SMU_IP_Address]/` where `[SMU_IP_Address]` is the IP address of the SMU (System Management Unit) managing the cluster
3. Log into Web Manager as user manager. By default, the password is nasadmin but this password may have been changed.
4. Navigate to **Home > Server Settings > EVS Migration** to display the EVS Migration page.





**Note:** If the SMU is currently managing a cluster and at least one other cluster or standalone server, the following page appears:

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

## EVS Migration

Which Type of EVS Migration do you want to do?

[Migrate an EVS from one node to another within the cluster](#)

[Migrate an EVS from one system to a separate, independent system which shares the same storage](#)

If this page does appear, click **Migrate an EVS from one node to another within the cluster** to display the main EVS Migration page.

If the SMU is managing one cluster and no standalone servers, the main EVS Migration page appears:

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

## EVS Migration

### EVS Mappings

Node	Current EVS Mapping	Preferred EVS Mapping
Group1-node1	g1-eva3 , g1-eva1 , LNAS , g1-eva2 , EVS1	g1-eva3 , LNAS , g1-eva2 , EVS1
Group1-node2	donotdelete	donotdelete , g1-eva1

[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  to cluster node

☐ Migrate all EVSes from cluster node  to cluster node

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

5. To return all EVSs to their preferred nodes:
  - If the preferred mapping was saved in [Step 5: Save the preferred mapping and migrate EVSs \(cluster node only\) on page 91](#), click **Migrate all to preferred** in the EVS Mappings section.
  - If the preferred mapping was not saved, migrate EVSs as required:

6. Migrate EVSs as required:
- To migrate all EVSs between cluster nodes:
    - a. Select Migrate all EVS from **cluster node** \_\_\_\_ **to cluster node** \_\_\_\_.
    - b. From the first drop-down list, select the cluster node from which to migrate all EVS.
    - c. From the second drop-down list, select the cluster node to which the EVSs will be migrated.
    - d. Click **Migrate**.
  - To migrate a single EVS to a cluster node:
    - a. Select **Migrate EVS** \_\_\_\_ **to cluster node** \_\_\_\_.
    - b. From the first drop-down list, select the cluster node to migrate.
    - c. From the second drop-down list, select the cluster node to which the EVS will be migrated.
    - d. Click **Migrate**.





## 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:

- Single stand-alone server using an embedded SMU for management
- Single stand-alone server using an external SMU for management
- 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](#)
- ☐ [Manually installing an internal SMU \(if necessary\)](#)
- ☐ [Replacing a single server with an embedded SMU](#)
- ☐ [Replacing a single server with an external SMU](#)
- ☐ [Replacing a node within a cluster](#)
- ☐ [Replacing all servers within a cluster](#)

## Replacement procedure overview

This section highlights the requirements and considerations when replacing nodes.

### Requirements

*Any personnel attempting the following procedures must have completed the necessary training before proceeding. Much of the process required for a server replacement is the same process covered in installation and configuration training. No personnel should attempt to replace a unit without adequate training and authorization.*

Determine which replacement scenario is being encountered in advance. The replacement process is different for each scenario.

Acquire the temporary license keys before arriving onsite to expedite the server replacement. The license keys are necessary because they are based on the unique MAC ID for the server or cluster. New license keys are not required when replacing one server in a cluster.



**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.

---

You can use a KVM (keyboard, video, and mouse) device or a serial cable to connect to the serial port. Bring both devices with you just in case both 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 the replacement server that you receive. You must remove those components from the original server and use them in the replacement server. There are a minimum of four parts to be reused in the replacement server.

The components that can be swapped include:

- Battery
- Bezel
- Rack mounting guides

**Note:**

- New power supplies are shipped installed in the server, and do not need to be swapped.
- 

## Model selection

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.

The upgrade process is outside the scope of this document and documented separately. Contact Hitachi Data Systems Support Center for upgrade information.

## MAC ID and license keys

The replacement server will have a new MAC ID. The new ID forces the need for new license keys regardless whether it is a single node or complete cluster replacement.

As part of a field replacement process, Hitachi Data Systems recommends that temporary keys be obtained to enable quick delivery and implementation. However, any temporary keys used 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 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, then a manual recovery process is required to reestablish 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 internal SMU (if necessary)

HNAS 3080/3090 spare or replacement units are shipped without the internal 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 internal 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 internal 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 internal SMU on the replacement node, but it is recommended to fully uninstall the internal 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 TISC or the support portal.

---

## 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.



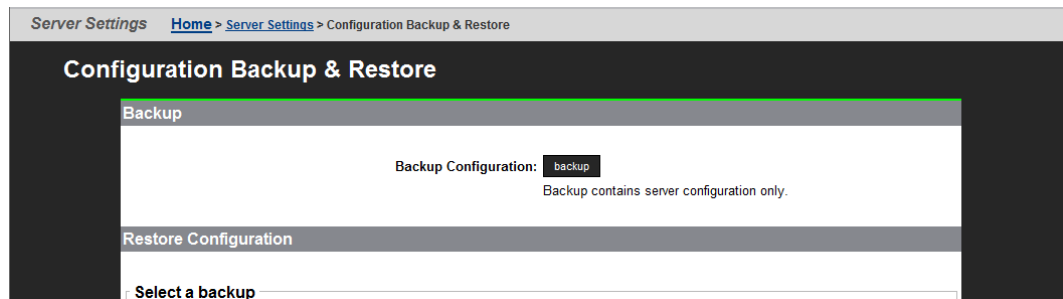
**Important:** Set expectations up front with the customer that this will delay time to recovery, and that some aspects of the systems configuration might never be recovered.

## Obtaining backups, diagnostics, firmware levels, and license keys

On the old server:

### Procedure

1. If the server is online, using Web Manager (SMU GUI), 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 showall.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 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 %)	<a href="#">details</a>
2 (Group1-node2)	Online	12.1.3600.00	12.1.3600.00	297.36 GB (97 %)	<a href="#">details</a>

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

Package View		
Package	Present On Cluster Nodes	Install Status
<input type="radio"/> nas-11.3.3434.01.tar	1, 2	OK
<input type="radio"/> nas-11.2.3319.06.tar	1, 2	OK
<input type="radio"/> nas-11.2.3319.09.tar	1, 2	OK
<input type="radio"/> nas-11.1.3225.00.tar	1, 2	OK
<input type="radio"/> nas-12.1.3600.00.tar	1, 2	OK
<input type="radio"/> nas-12.0.3525.00.tar	1, 2	OK
<input type="radio"/> 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.
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

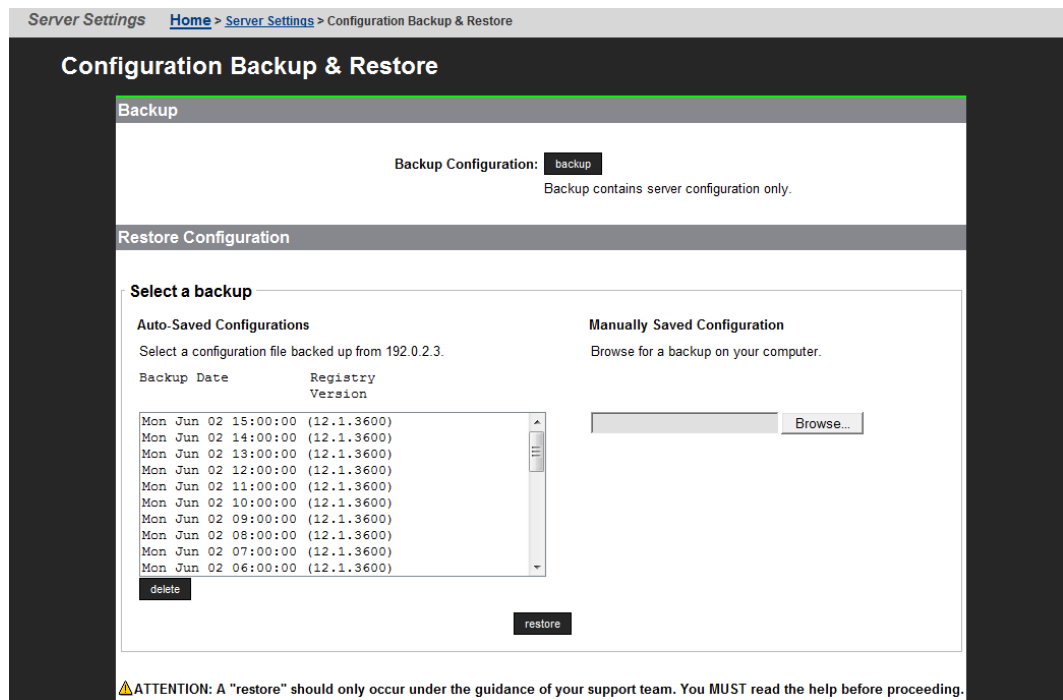
On the replacement server:

### 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` (default password: `nasadmin`), 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 Web Manager (SMU GUI) using either of the IP addresses acquired from the EVS list output.
9. Click **Yes**, and log in as `admin` (default password: `nasadmin`).
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 Data Systems Support Center 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 3080 and 3090	4 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:
  - a. Enter `fc-link-speed` to display the current settings.
  - b. Enter `fc-link-speed -i port_number -s speed` for each port.
  - c. Enter `fc-link-speed` to verify the settings.
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.



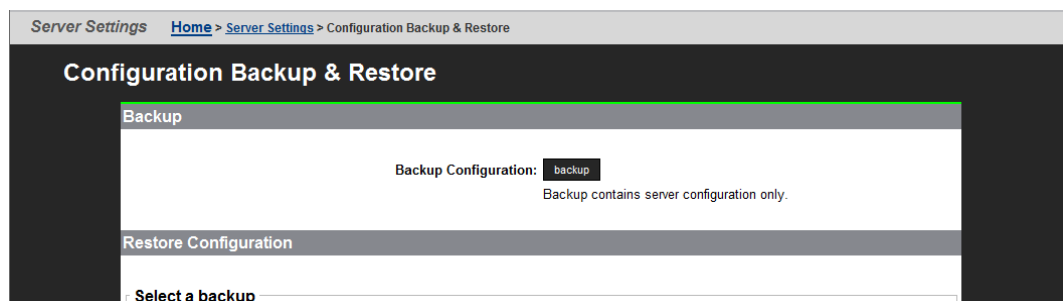
**Important:** Set expectations up front with the customer that this will delay time to recovery, and that some aspects of the systems configuration might never be recovered.

## Obtaining backups, diagnostics, firmware levels, and license keys

On the old server:

### Procedure

1. If the server is online, using Web Manager (SMU GUI), 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.

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

### Firmware Package Management

Filter
☐ Include System Patch Packages

Node View

Cluster Node ID (Name)	Status	Current Package	Default Package	Free Space	
1 (G400-442060-1)	Online	12.6.4128.00	12.6.4128.00	Not available	<a href="#">details</a>
2 (G400-442060-2)	Online	12.6.4128.00	12.6.4128.00	71.09 GB (87 %)	<a href="#">details</a>

Actions: [reboot cluster](#) [reboot node](#) | [upload package](#)

Package View

Package	Present On Cluster Nodes	Install Status
<a href="#">nas-12.6.4124.00.tar</a>	1	<span style="color: green;">●</span> OK
<a href="#">nas-12.6.4126.00.tar</a>	1, 2	<span style="color: green;">●</span> OK
<a href="#">nas-12.6.4119.00.tar</a>	1, 2	<span style="color: green;">●</span> OK
<a href="#">nas-12.6.4128.00.tar</a>	1, 2	<span style="color: green;">●</span> OK
<a href="#">nas-12.6.4127.00.tar</a>	1, 2	<span style="color: green;">●</span> OK
<a href="#">mcy-12.6.4123.00.20151023.tar</a>	1, 2	<span style="color: green;">●</span> OK

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

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.
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` (default password: `nasadmin`), 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 Web Manager (SMU GUI) 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` (default password: `nasadmin`).
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 Data Systems Support Center 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.

Server Settings [Home](#) > [Server Settings](#) > Configuration Backup & Restore

## Configuration Backup & Restore

### Backup

Backup Configuration: **backup**

Backup contains server configuration only.

### Restore Configuration

**Select a backup**

**Auto-Saved Configurations**

Select a configuration file backed up from 192.0.2.3.

Backup Date	Registry Version
Mon Jun 02 15:00:00	(12.1.3600)
Mon Jun 02 14:00:00	(12.1.3600)
Mon Jun 02 13:00:00	(12.1.3600)
Mon Jun 02 12:00:00	(12.1.3600)
Mon Jun 02 11:00:00	(12.1.3600)
Mon Jun 02 10:00:00	(12.1.3600)
Mon Jun 02 09:00:00	(12.1.3600)
Mon Jun 02 08:00:00	(12.1.3600)
Mon Jun 02 07:00:00	(12.1.3600)
Mon Jun 02 06:00:00	(12.1.3600)

**delete**

**Manually Saved Configuration**

Browse for a backup on your computer.

**Browse...**

**restore**

⚠ ATTENTION: A "restore" should only occur under the guidance of your support team. You MUST read the help before proceeding.

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 3080 and 3090	4 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:
  - a. Enter **fc-link-speed** to display the current settings.
  - b. Enter **fc-link-speed -i port\_number -s speed** for each port.
  - c. Enter **fc-link-speed** to verify the settings.
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. From TISC, download 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

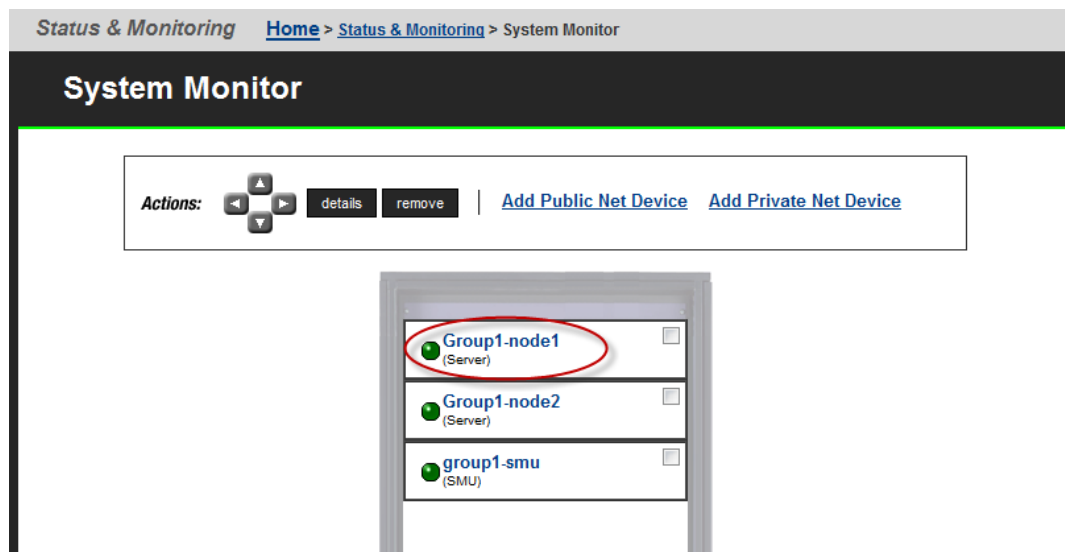
1. Physically rack the new node into the place of the old node.
2. Connect the cables to the new node, according your labelling.
3. Power up the new node and ensure that BALI loads again.
4. If the customer is using SAN attached, and/or host group security, update this to reflect the changes that are 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 > Sever 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

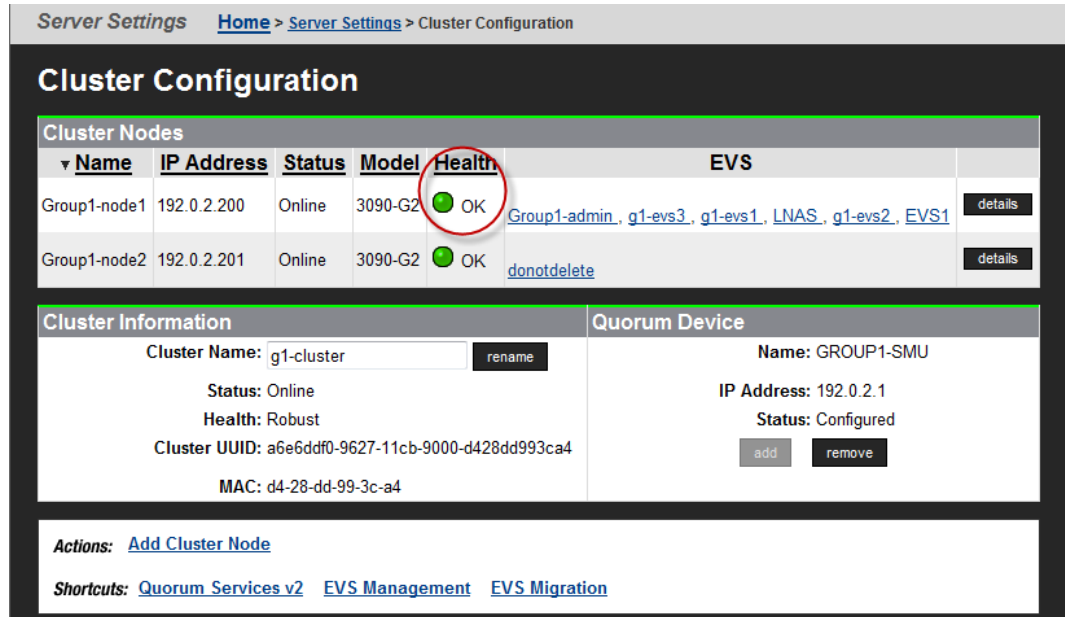
On the new server:

### 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.



3. 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

4. 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-eva3 , g1-eva1 , LNAS , g1-eva2 , EVS1	g1-eva3 , LNAS , g1-eva2 , EVS1
Group1-node2	donotdelete	donotdelete , g1-eva1

[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**

5. 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:  [rename](#)

EVS ID: 6

Status: ● Online

Type: File Services

Enabled: Yes

Preferred Cluster Node:  [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

6. Select the node from the Preferred Cluster Node list, and then click **apply**.
7. 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.



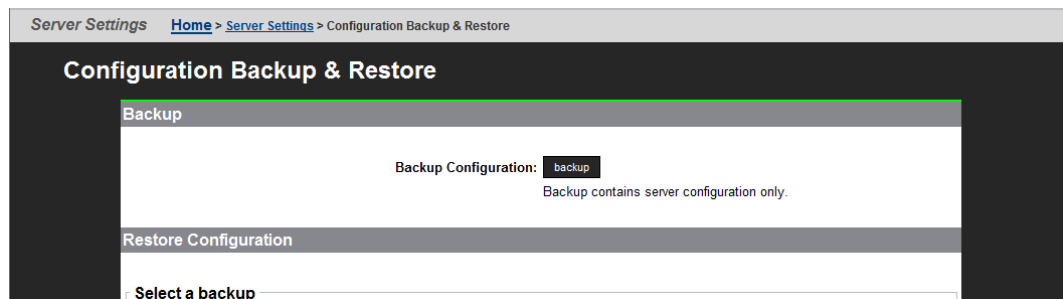
**Important:** Set expectations up front with the customer that this will delay time to recovery, and that some aspects of the systems configuration might never be recovered.

## Obtaining backups, diagnostics, firmware levels, and license keys

On the old server:

### Procedure

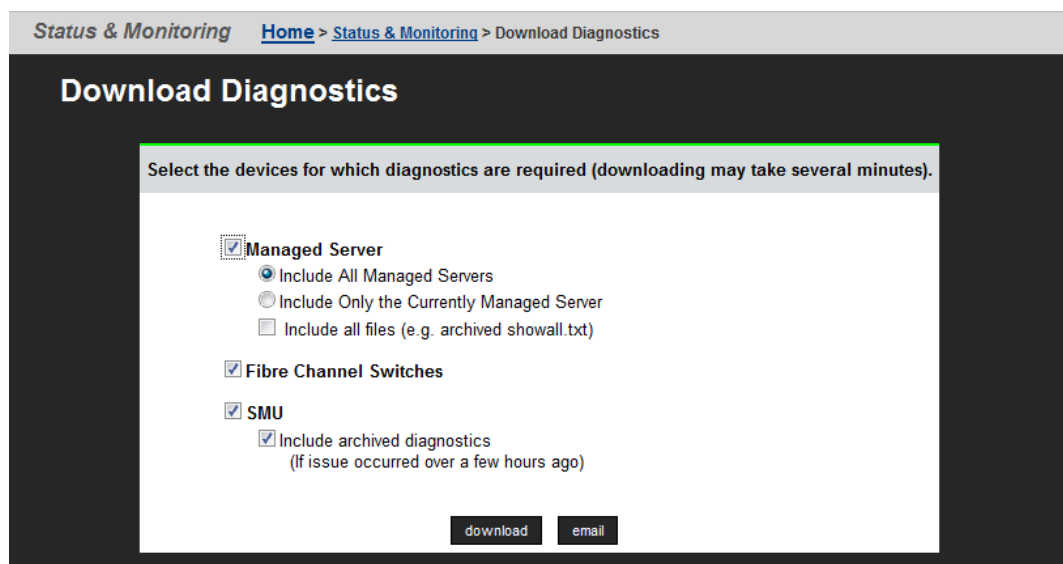
1. If the server is online, using Web Manager (SMU GUI), navigate to **Home > Server Settings > Configuration Backup & Restore**, click **backup**, and then select a location to save the backup file.



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.



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.

- 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

- 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.
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` (default password: `nasadmin`), 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 Web Manager (SMU GUI) 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` (default password: `nasadmin`).
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 Data Systems Support Center 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` (default password: `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 name

The SMU should recognize the node as the same and allow it to be managed.

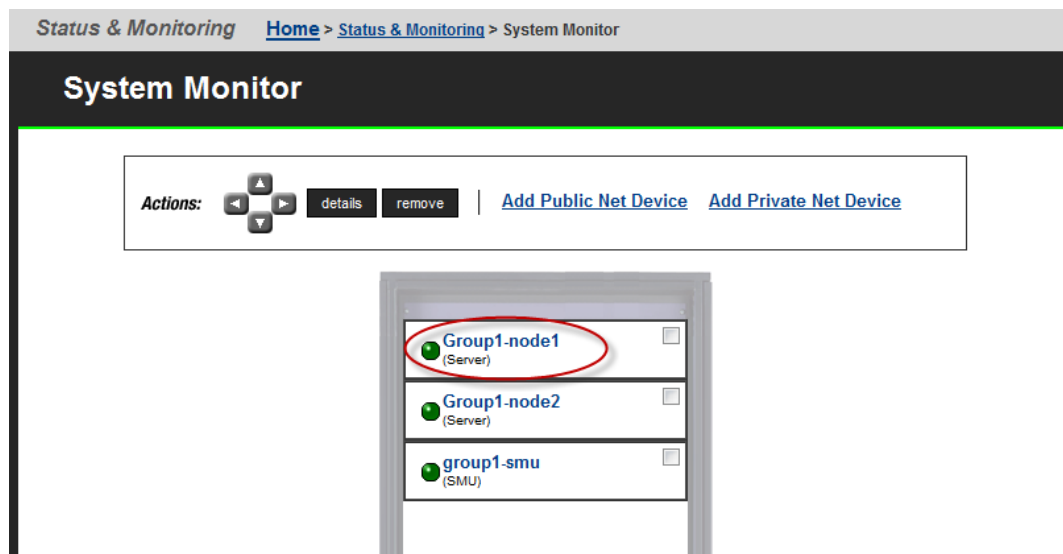
19. Navigate to **Home > Server Settings > License Keys** to load the license keys.
20. Repeat steps for any other replacement servers to be configured.

## 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.



# Parts list for 3080/3090 G1 servers

## Parts for 3080/3090 servers

Part number	Description	Notes
SX325074	PSU Module-450W	
SX325075	Fan Module (each)	
SX325118	MK1.5 Hard Disk (250GB)	Replaces SX325076
SX325120	Server w/250GB HDD (no battery)	Replaces SX325087, this part number should be used whenever possible
SX320164	USB Configure Tool	Included in part number SX325104
SX325130	PSU- 450W	<ul style="list-style-type: none"> <li>RoHS 2013</li> <li>Required for EMEA</li> <li>RoHS 2013 spares are required for EMEA units start with a S/N starting with M2SEKW13 or higher</li> </ul>
SX325097	MK1 Battery Module ea	

## System Management Unit (SMU) parts

Part number	Description	Notes
SX325094	SMU300 w/CentOS 4.4	<ul style="list-style-type: none"> <li>No SMU code</li> <li>RoHS5</li> </ul>
SX325121	SMU300 HDS Branded, CentOS6.2	No SMU code
SX325134	SMU300 HDS Branded, CentOS6.2	<ul style="list-style-type: none"> <li>no SMU code</li> <li>RoHS 2013 (Required for EMEA)</li> <li>RoHS 2013 spares are required for EMEA units start with a S/N starting with M2SEKW13 or higher</li> </ul>
SX345278	System Management Unit 300 (SMU300)	<ul style="list-style-type: none"> <li>Required for Cluster (current)</li> <li>Can use SX325121</li> </ul>

## 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)	
HD-TI-24X-AC	TurboIron 24 Port switch (10GbE/1GbE, SFP+)	This switch is required for configurations that include 3 or more nodes
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	
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	
SX222096	Copper cable - SFP+ 10GE passive twinax, Cluster & 10GbE, 1 meter, RoHS 6	

Part number	Description	Notes
SX222097	Copper cable - SFP+ 10GE passive twinax, Cluster & 10GbE, 3 meters, RoHS 6	
SX222098	Copper cable - SFP+ 10GE passive twinax, Cluster & 10GbE, 5 meters, RoHS 6	
SX222099	Copper cable - SFP+ 10GE passive twinax, Cluster & 10GbE, 7 meters, RoHS 6	

### Optics parts

Part number	Description	Notes
HD-10G-SFPP-SR	10GBASE-SR, SFP+ optic (LC), target range 300m over MMF	This SFP is used in the TurboIron switch (part number HD-TI-24X-AC)
SX350004	SFP 1000BaseT Copper	Manufacturer part number is FCMJ-8521-3
SX350000	SFP - Multi-Mode Fiber - 2 Gbps	Manufacturer part number is FTRJ8519P1BNL
SX350010	SFP - Multi-Mode Fiber - 4 Gbps	Manufacturer part number is FTLF8524P2BNV
SX350011	XFP - 10G 850NM 1-Pk for Cluster only	Manufacturer part number is FTLX8511D3
FTLX1412D3BCL	Multi-source XFP 10Gbps; Single Mode 1310nm; LC 3.3v	Substitute part number FTLX1411D3
FTLX1411D3	XFP - 10G LWL 10km Finisar 1-Pk	Can use FTLX1412D3BCL







## **Hitachi Data Systems**

### **Corporate Headquarters**

2845 Lafayette Street  
Santa Clara, California 95050-2639  
U.S.A.  
[www.hds.com](http://www.hds.com)

### **Regional Contact Information**

#### **Americas**

+1 408 970 1000  
[info@hds.com](mailto:info@hds.com)

#### **Europe, Middle East, and Africa**

+44 (0) 1753 618000  
[info.emea@hds.com](mailto:info.emea@hds.com)

#### **Asia Pacific**

+852 3189 7900  
[hds.marketing.apac@hds.com](mailto:hds.marketing.apac@hds.com)



**MK-92HNAS016-10**

**October 2016**