Hitachi NAS Platform
5000 Series Hardware Reference

Release 14.9 or higher

Legal Notices

Contents

Contents

Contents

Preface

This guide provides an overview of the Hitachi NAS Platform and the Hitachi Unified Storage File Module hardware. This guide explains how to install and configure the hardware and software for the 5200 and 5300 server models, and how to replace faulty components.

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

> **Note:** The use of clustering in a production environment is required for data availability. Any deferences herein to "single node" are taken in the context of a cluster of 2 or more nodes.

Accessing product documentation

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

Getting help

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

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

Comments

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

Thank you!

Chapter 1: About this guide

This guide provides an overview of the NAS Platform Series 5000 hardware, how to install and configure the hardware and software, and how to replace faulty components. This guide provides information on the 5200 and 5300 server models.

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

Audience

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

Conventions

The following conventions are used throughout this document:

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

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

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

Før du starter (DANSK)

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

Bemærk: "Bemærk" indikerer informationer, som skal bemærkes.

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

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

Vorbereitung (DEUTSCH)

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

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

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

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

Antes de comenzar (ESPAÑOL)

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

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

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

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

Avant de commencer (FRANÇAIS)

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

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

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

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

Operazioni preliminari (ITALIANO)

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

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

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

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

Vóór u aan de slag gaat (NEDERLANDS)

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

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

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

Antes de começar (PORTUGUÊS)

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

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

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

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

Ennen kuin aloitat (SUOMI)

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

Huomautus: Huomautus sisältää tietoja, jotka tulee ottaa huomioon.

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

Chapter 2: Safety information

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

Electrostatic discharge precautions

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

- Wear an anti-static wrist or ankle strap.

- Observe all standard electrostatic discharge precautions when handling plug-in modules or components that have been removed from any anti-static packaging.

- Avoid contact with backplane components and module connectors.

Safety and handling precautions

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

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

> ⚠ **Caution:** There is a risk that a cabinet could fall over suddenly. To prevent this from occurring:
> - If your system comes with a rack stabilizer plate, install it.
> - Fill all expansion cabinets including all storage enclosures from the bottom to the top.
> - Do not remove more than one unit from the rack at a time.

Electrical precautions

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

- Provide a suitable power source with electrical overload protection to meet the power requirements of the entire system (the server/cluster and all storage systems and switches).

- Provide a power cord suitable for the country of installation (if a power cord is not supplied).

- Power cords supplied with this server or system may be less than 1.5m in length. These cords are for use with a power distribution unit (PDU), which is mounted inside the 19-inch rack. If you require longer cables, contact your Hitachi representative.

- Provide a safe electrical ground connection to the power cord. Check the grounding of an enclosure before applying power.

- Only operate the equipment from nominal mains input voltages in the range 100 - 240Vac, 6A max, 50/60Hz.

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

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

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

Chapter 3: Mandatory regulations

The following sections provide the mandatory regulations governing the installation and operation of the system. Adhere to these instructions so that regulatory compliance requirements are met.

International standards

Safety

The safety standards include:

- IEC 62368-1:2014 (Second Edition)

EMC

The EMC standards are as follows:

- EN 55032:2015
- FCC/CFR 47:Part 15
- Canadian Standard ICES-003:Issue 6
- AS/NZS CISPR 22
- EN 61000-3-2:2019
- EN 61000-3-3:2013 inc A1:2019
- EN 55035:2017
- NRRA Notice 2018-17
- VCCI-CISPR32:2016

Certification for approval marks

Certification for the following approval marks have been granted:

- European Union CE mark, including RoHS and WEEE
- China: CCC
- Russia: Eurasia (CU) - EAC & RoHS
- Taiwan: BSMI
- Argentina: IRAM
- Mexico: NOM and CONUEE
- South Africa: NRCS and SABs
- Israel: SII
- Ukraine: UKrSEPR & RoHS
- UK: UKCA

Federal Communications Commission (FCC)

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

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

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

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

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

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

European Union (EU) Statement

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

- 89/336/EEC Electromagnetic Compatibility Directive

- 73/23/EEC Low Voltage Directive

- 93/68/EEC CE Marking Directive

- 2015/863/EU amending Annex II of Directive 2011/65/EU Restriction in the use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) - This product is 10/10 (fully) compliant.

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

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

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

Korea Certification (KC) Statement

The VGA, Serial, and USB ports are for setup purposes only and are not used when the unit is in normal working operation.

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 Compulsory Statement

China Compulsory Certificate Statement

声明此☒ A ☒☒品，在生活☒境中，☒☒品可能会造成无☒☒干☒。在☒种情况下，可能需要用☒☒其干☒采取切☒可行的措施。

Chinese RoHS Compliance Statement

有毒有害物质名称标识
Toxic and Hazardous Substances Table

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

O：表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 规定的限量要求以下
O : Indicates that the toxic or hazardous substances contained in all of the homogeneous materials for this part is below this limit requirement in SJ/T 11363-2006.

X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 规定的限量要求
X : Indicates that the toxic or hazardous substances contained in at least one of the homogeneous materials used for this part is above the limit requirement in SJ/T 11363-2006.

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

Figure 1 Chinese RoHS Compliance Statement

Chapter 4: Hitachi NAS Platform server components

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

System components

Component	Description
HNAS server	The system contains several servers that operate as a cluster. Clusters that use more than two servers include two 10 Gbps Ethernet switches. Hitachi Vantara supports two switches for redundancy.
NAS Manager	The NAS Manager is the management component for the other components in a system. The NAS Manager 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 NAS Manager does not move data between the network client and the servers. In clustered systems, the NAS Manager provides the management functionality.
Storage systems	A Hitachi NAS Platform system or a Hitachi Unified Storage File Module system can control several storage enclosures. The maximum number of storage enclosures in a rack depends on the model of storage enclosures being installed. Refer to the *Storage Subsystem Administration Guide* for more information on supported storage systems.
Fibre Channel (FC) switches	The server supports FC switches that connect multiple servers and storage systems. See Hitachi Vantara Support Connect for information about which FC switches are supported.
External 10 Gigabit Ethernet (10 GbE) switches	All cluster configurations require an external Ethernet switch. See Hitachi Vantara Support Connect for information about the 10 GbE switches that have been qualified for use with the system, and to find out about the availability of those switches.
10 GbE switches	The server connects to a 10 GbE switch for connection with the public data network (customer data network). Also, a 10 GbE switch is required for internal cluster communications for clusters of three or more nodes. See Hitachi Vantara Support Connect for information about the 10 GbE switches that have been qualified for use with the server, and to find out about the availability of those switches. Hitachi Vantara requires dual 10 GbE switches for redundancy. In a dual-switch configuration, if one switch fails, the cluster nodes remain connected through the second switch.

Server components

The NAS Platform Series 5000 has a chassis that is 3U (5.25 inches) high, 480 millimeters (19 inches) wide, rack mountable, and a maximum of 686 millimeters (27 inches) deep, excluding the bezel. The chassis contains:

- Front bezel

- NAS Platform Series 5000 Base Server

- Dual hot-swappable fan assemblies

- Dual hot-swappable power supplies

- Dual hot-swappable 2.5" O/S disk drive

If there is an issue with the NAS Platform Series 5000 Base Server, the server must be returned for repair. Some of the other components can be replaced in the field, and some are hot-swappable (they can be changed without shutting down the server).

Field replaceable units (FRUs) include power supplies, fan assemblies, and disk drives.

New FRUs supported include:

- SX325151 – FRU HNAS 5000 SERVER (without PSUs, bezel, and rail kit)

- SX325152 – FRU HNAS 5000 (495W) PSU

- SX325155 – FRU HNAS 5000 SSD MODULE

- SX170320 – MODULE SFP+ 16GBIT TRANSCEIVER

Existing FRUs supported include:

- SX325116 – FRU HNAS 5000 FAN TRAY (Fan ID: 1)

- SX325142 – FRU HNAS 5000 CLIP-IN RAIL KIT

- SX325150 – FRU HNAS SERVER BEZEL KIT

Server specifications

Physical:

- Weight: 23 kg (51 lb.) including 3 kg rail kit assemblies and metal bezel.

- Height: 132 mm. (5 in.)

- Depth (bezel to PSU): 725 mm. (28.6 in.)

- Width: 440 mm. (17.3 in.)

- Rack space required: 3U (5.25 in.)

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

The power and cooling information is shown as follows:

📄 **Note:** The power supplies and cooling fans are hot-swappable.

Table 1 Power and cooling details

Power or cooling detail	Hitachi NAS Platform
Voltage range (Ave./Max.)	100 VAC – 2.1/2.6A 110 VAC – 1.9/2.4A 200 VAC – 1.0/1.3A 208 VAC – 1.0/1.3A 230 VAC – 0.9/1.2A
Power supply rating	495W
Average thermal (BTU/hour)	710
Max. thermal (BTU/hour)	887
Max. power usage	260W
Heighth/width/depth	3U, 5.2 in. (132mm)/ 17.3 in. (440mm)/28.6 in. (725mm)
Weight	Weight 51 lbs. (23kg) incl. rail kit assemblies.
Compliance	RoHS 6 China RoHS Compliant EU RoHS Compliant Safety EU: EN62368-1: 2nd edition Canada: CAN/CSA-C22.2 No.60950-1-07 2nd edition US: UL 62368-1 EMC EU: EN62368-1: 2nd edition Canada: CAN/CSA-C22.2 No.60950-1-07 2nd edition US: UL 62368-1

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

Ventilation

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

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

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

Server front panel

The following figure shows the front panel of the server:
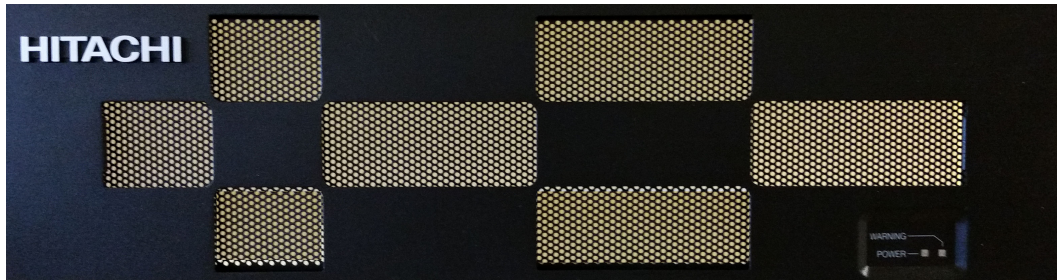
Figure 2 Server front panel metal bezel

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

Figure 3 Server model 5200 / 5300 front panel components (bezel removed)
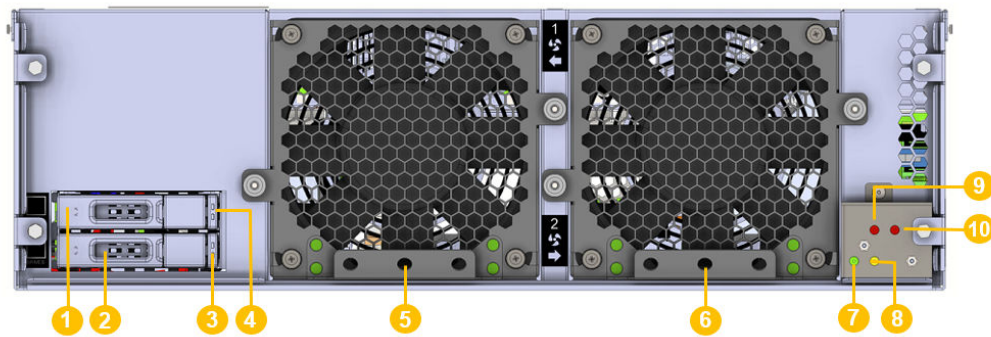
The following table shows the server front panel component descriptions:

Table 2 Server front panel component descriptions

Item	Description
1	O/S disk drive A (top)
2	O/S disk drive B (bottom)
3	Disk B status LED
4	Disk A status LED
5	Fan 1
6	Fan 2
7	Power status LED
8	Server status LED
9	Fan 1 status LED
10	Fan 2 status LED

LED status indicators

The following figure shows the LED status indicators for the 5200 and 5300 server models.
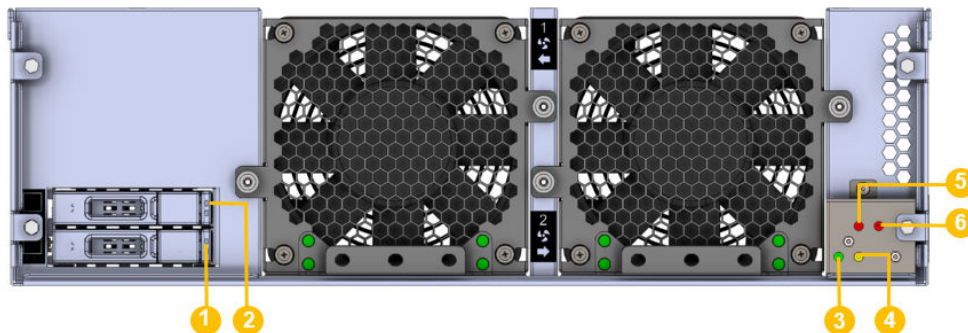
Figure 4 Model 5200 / 5300 status LEDs

The following table describes each numbered LED in the preceding diagram:

Table 3 LED descriptions

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

The following table describes the various power status LEDs.

Table 4 Power status LED (green)

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

LEDs	Meaning
Fast flash (five flashes per second)	The server is rebooting.
Off	The server is not powered up.

The following table describes the various server status LEDs:

Table 5 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.

The following table describes the varius fan status LEDs:

Table 6 Fan status LEDs

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

The following table describes the O/S disk activity and status LEDs:

Table 7 O/S disk activity and status LEDs

LEDs	Meaning
Blue	If this LED is on and blue, the disk is operating normally and no problems have been detected. If the LED is flashing blue, this indicates disk activity. If the LED is on but not flashing, there is currently no disk activity.

Chapter 4: Hitachi NAS Platform server components

LEDs	Meaning
Red	If this LED is on immediately after installing a new O/S disk, this indicates that the RAID configuration for the server is being rebuilt. The LED turns off after the RAID configuration is restored. The amount of time it takes for the RAID configuration to be rebuilt after a new disk drive is installed depends on the amount of user and system configuration data stored. If this LED is on during the course of normal operation (not after installing a new O/S disk), either the disk has failed or the server's RAID configuration has been degraded.

O/S drives

O/S drives are located behind the bezel on the left side of the chassis.

> 📄 **Note:**
>
> - Failed O/S drives are hot-swappable, which means that a failed drive can be replaced without shutting down the server. However, there are serious risks in trying to swap a drive that has not failed. It is strongly recommended that you avoid performing replacement procedures during busy periods to minimize the risk of any disruption caused by the procedure.
>
> - Do not attempt to replace or recover a O/S drive without the assistance of Hitachi Vantara Customer Support.

The O/S drive A and B status and activity status LEDs of the 5200 and 5300 server models are shown as follows:
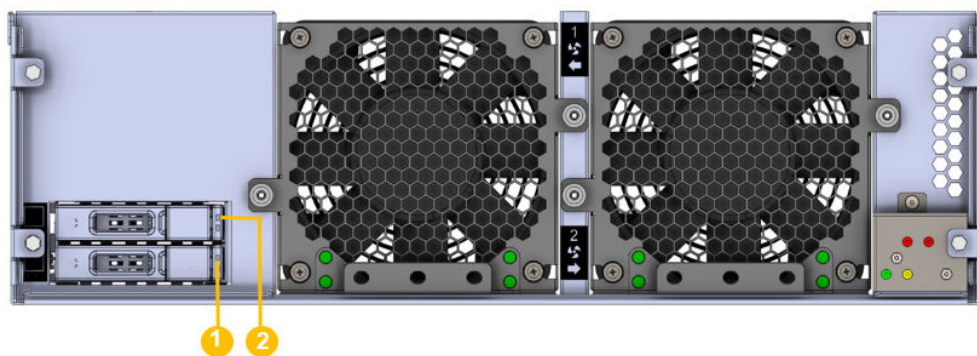
Table 8 Drive A and B status and activity LEDs

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

Table 9 O/S disk activity and status LEDs

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

Fans

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

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

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

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

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

Two fan status LEDs provide fan status information. These LEDs are located behind the bezel on the right side of the chassis.
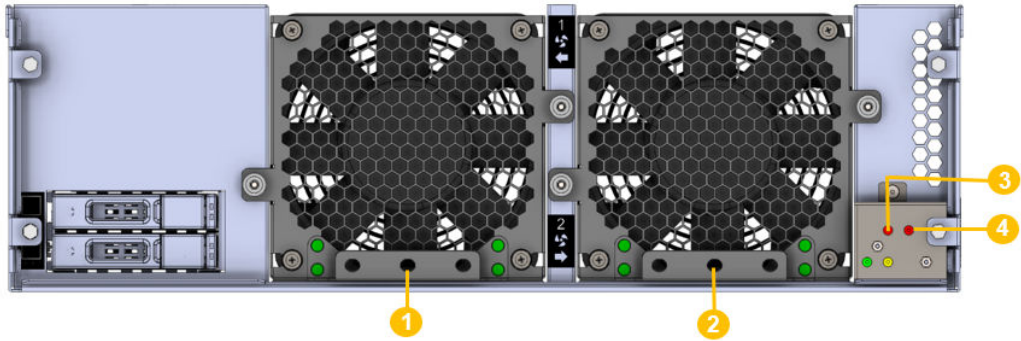
Item	Description
1	Fan 1 (left)
2	Fan 2 (right)
3	Fan 1 status LED
4	Fan 2 status LED

Table 10 Fan status LEDs

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

Server rear panel

The following figure shows the rear panel components for the 5200 and 5300 server models:
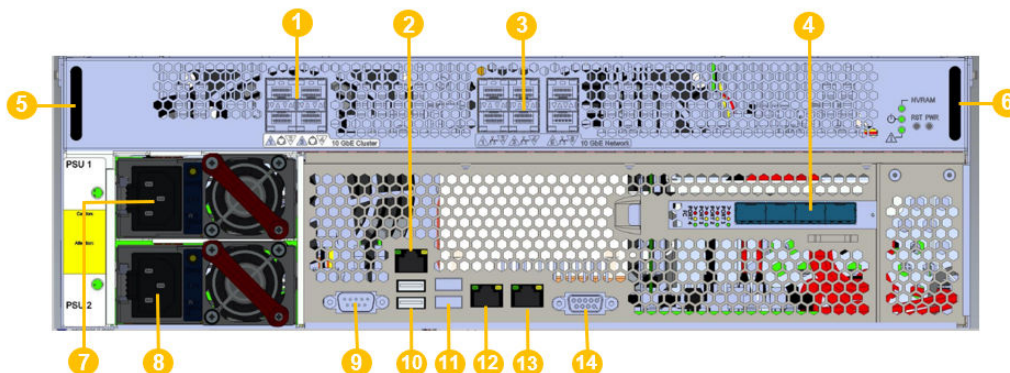
Figure 5 Server rear panel components for models HNAS 5200 / 5300

The following table shows the ports and connectors on the server rear panel:

📄 **Note:** Do not use any ports or connectors that are not described in this table without guidance from technical support.

Item	Connectivity	Qty	Description
1	Clustering ports 10 GbE	4	For cluster management and heartbeat, connect to: ▪ Two-way configuration: Connect to the corresponding cluster server ports (left port to left port and right port to right port). ▪ N-way configuration: Connect to the 10 GbE switch.
2	IPMI port	1	Connection to the internal Ethernet switch of the rack
3	10 GbE network ports	6	Connection to external 10 Gbps Ethernet data network
4	Storage or FC switch	4	Connection to disk systems or (where present) to the FC switches
5&6	n/a	3	Plastic handles Caution: Do not lift the server by these handles.
7	PSU 1	1	Power Supply Unit 1

Item	Connectivity	Qty	Description
8	PSU 2	1	Power Supply Unit 2
9	RS-232	2	Management interface. *(Reserved for Customer Service Engineer access only.)*
10	USB Ports	1	USB port. *(Reserved for Customer Service Engineer access only.)*
11	USB Ports 3.0	1	USB 3.0 port. *(Reserved for Customer Service Engineer access only.)*
12	ETH0 1000baseT Ethernet	1	External system management. Connect to the customer's management switch.
13	ETH1 1000baseT Ethernet	1	Management port. Connect to the internal Ethernet switch of the rack.
14	Video port	1	Video management interface port. *(Reserved for Customer Service Engineer access only.)*

Rear panel LED state descriptions

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

The following tables describe the various power status LEDs.

Table 11 NVRAM status LED (green/amber)

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

Table 12 Power status LED (green)

LEDs	Meaning
Green	Normal operational mode of an active cluster node.

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

Table 13 Server status LED (amber)

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

10 gigabit cluster ethernet interconnect ports

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

Do *not* use the 10 GbE cluster interconnect ports to connect to the customer data network (also known as the public data network).
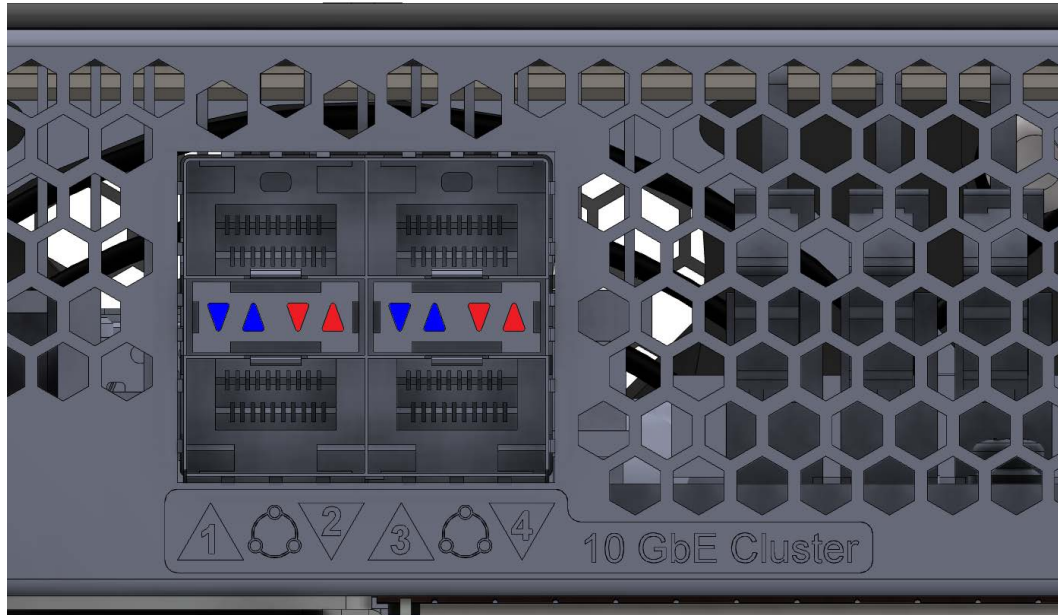
Figure 6 10 GbE cluster interconnect ports

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

Table 14 Status and activity per port

Status/Activity (per port)		Meaning
Status	Blue on, not flashing	10 Gbps link present
	Blue off	No link
	Red on	Fault with 10GbE cluster port. Check SFP (laser fault, not 10Gb or Copper SFP used)
	Red off	No fault with 10GbE cluster port
Activity	Blue flashing	10GbE cluster port activity

Rear panel server LED and button locations

Figure 7 Rear panel server LEDs and buttons
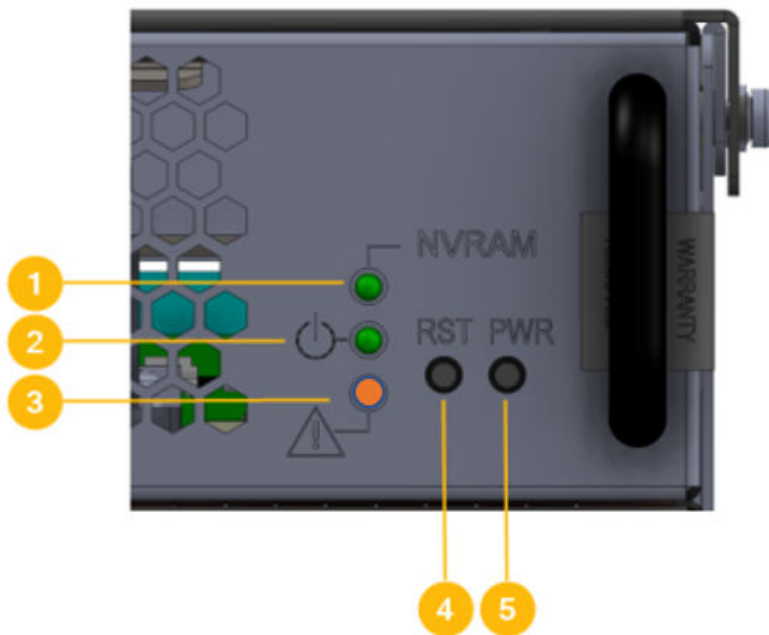
Figure 8 Rear panel server LEDS and buttons

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

Power button (PWR)

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

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

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

Reset button (RST)

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

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

> ⚠ **Caution:** If the server is non-responsive, see Restarting an unresponsive server. Do not pull the power cord. Pulling the power cord does not produce a dump.

Fibre channel storage ports

The four FC ports operate at speeds of 4/8/16 Gbps. 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 10GbE Network SFP+ and the 16 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. Refer to the table in Chapter 9 for more information.

Figure 9 Fibre Channel storage ports label

Chapter 4: Hitachi NAS Platform server components

Table 15 Status and Activity (per port) descriptions

Status/Activity (per port)		Meaning
Status	Green (solid on)	Server booting
	Green off	Link down
Activity	Top Green LED(flashes for activity, other speed LEDs off)	16G FC link
	Middle Green LED (flashes for activity, other speed LEDs off)	8G FC link
	Bottom Green LED (flashes for activity, other speed LEDs off)	4G FC link
	HBA fault(LEDs flash in sequence)	Host Bus Adapter faulted

10 gigabit ethernet customer data network ports

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

There are six 10 GbE ports that use enhanced small form factor pluggable (SFP+) optical connectors, shown as follows:
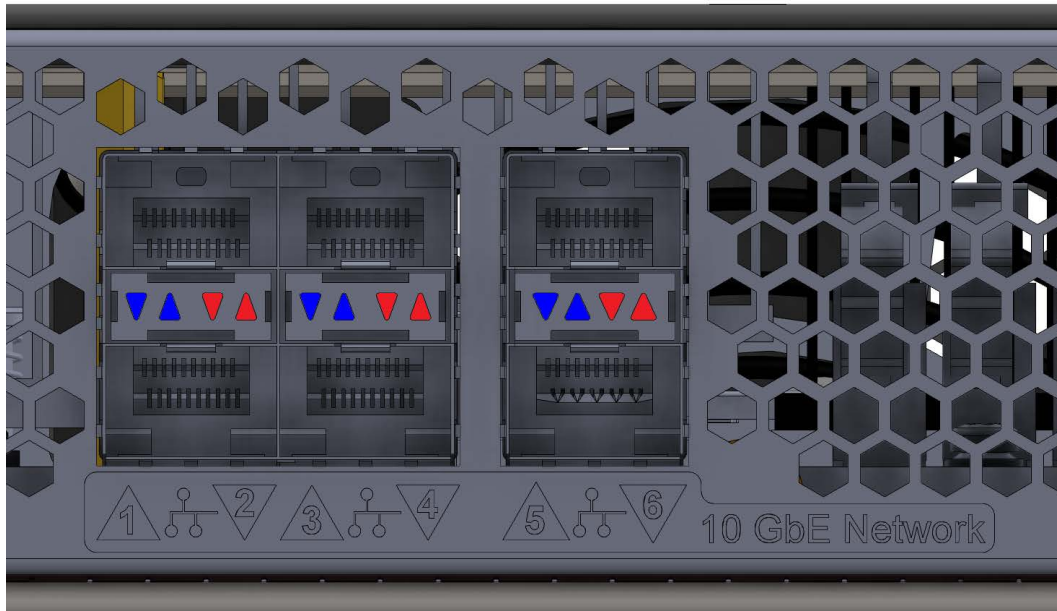
Figure 10 10 gigabit ethernet customer data network ports

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

Status/Activity (per port)		Meaning
Status	Blue on, not flashing	10 Gbps link present
	Blue off	No link
	Red on	Fault with 10GbE port. Check SFP (laser fault, not 10 Gb or Copper SFP >5m used)
	Red off	No fault with 10GbE port
Activity	Blue flashing	10 Gbps link activity

Power supply units

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

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

Power supply unit details
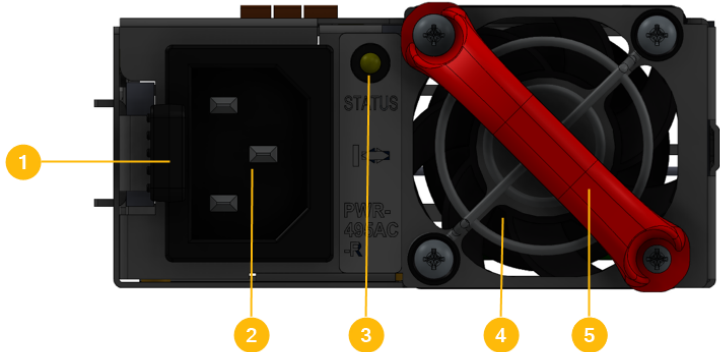
Item	Description
1	PSU retention latch
2	Power cord connector
3	PSU status LED
4	PSU fan exhaust
5	PSU handle

📄 **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 45) for information about replacing a power supply.

Table 16 Power status LED

Status	Meaning
Green	DC output operating normally
Flashing Green	No AC power or DC output fault
Off	Standby power fault or neither PSU is powered from AC mains
Flashing Amber	Internal PSU fault (over voltage, over-current, over temperature or fan failure)

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

If the amber status LED is flashing, unplug the power cable, wait 10 minutes, then reconnect the cable. If the PSU Status LED remains off, the PSU has failed and must be replaced. See Replacing a power supply unit (on page 45) for more information on replacing a PSU.

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 48). Do not pull the power cord.

Ethernet management ports 0 and 1

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

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

Refer to the following tables for more information.

Table 17 eth0/eth1 Activity LED (Right) LED State

LED Color	Status	Definition
Green	Flashing	Active

Table 18 eth0/eth1 Activity LED (Left) LED State

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

Serial port

A standard serial (RS-232) port, used to connect to the server for management purposes. See RS-232 serial management port for more information.

USB ports

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

Valid USB devices include:

- Flash drives

- External hard drives

- USB keyboards

Valid operations include:

- Management

- Install

- Upgrade

- Update

- Repair

> **Note:** The USB ports should not be used without guidance from Hitachi Vantara customer support.

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

IPMI port

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

Table 19 IPMI LAN LEDs

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

Management interfaces
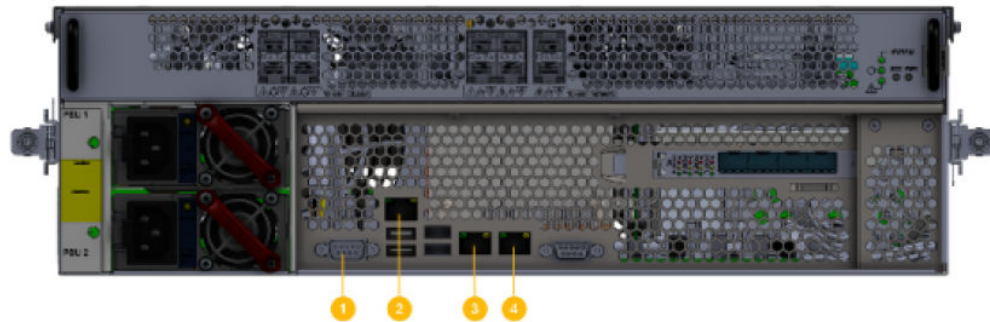
Management interface ports on rear panel.

Table 20 Management interface ports and descriptions

Item	Description
1	Serial management port (RS-232 DB-9 connector)
2	IPMI port
3	External system management port 0 for customer facing management (RJ45 connector)
4	Internal system management port 1 for private management (RJ45 connector)

RS-232 serial management port

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

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

Table 21 Host setting values

Terminal	Requirement
Connection	Crossover (null modem) cable
Emulation	VT100

Terminal	Requirement
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 server's SMU and use SSH to access the server's CLI.

10/100/1000 Ethernet management ports

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

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

Ethernet cables

CAT6 cables that fully comply with the CAT6 SF/UTP standard for the 1000Base-T GE Ethernet network ports are required.

Chapter 5: Replacing server components

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

Field replaceable units

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

FRUs include the following components:

- Whole node (except rail kit, bezel, and PSU)
- SSDs
- Fans
- Bezel
- Power Supply Units (PSUs)
- SFP+ port adapters

Hot-swappable components

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

Before replacing a component that is not hot-swappable, you must shut down and power off the server. See Rebooting or shutting down a server for details.

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.

Replacing a fan

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

Procedure

1. Remove the front bezel. The fan assemblies are now visible.
2. Identify the fan to be replaced.

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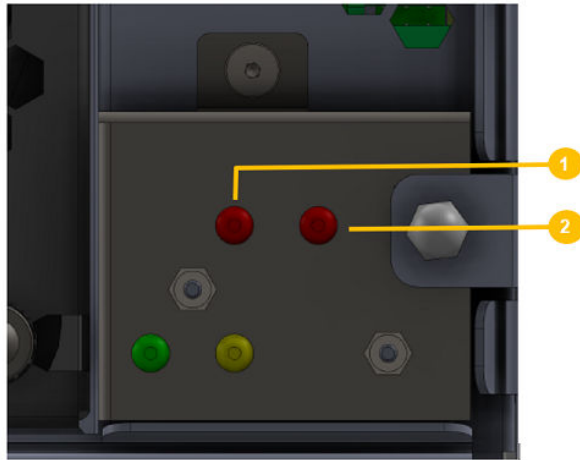

Figure 11 Fan status LEDs

Table 22 Fan status LED descriptions

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

3. Remove the faulty fan by loosening the thumbscrews (turning them counter-clockwise) until they are loose, then pulling the fan unit straight out of the chassis. (The fan lead connector disengages automatically as you remove the fan assembly.)
4. Put the new fan assembly into place.
5. Gently press the fan assembly back into the chassis. The fan electrical connector is aligned automatically when the fan is fully inserted into the chassis.
6. Secure the fan assembly in position by tightening the thumbscrews (turning them clockwise).
7. Replace the front bezel.

Recovering or replacing a drive

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

> **Important:** Do not attempt to replace or recover a drive without the assistance of Hitachi Vantara Customer Support.

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

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

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

> **Important:** Before you consider replacing a drive, note the following points:
>
> - Failed drives are hot-swappable, so a failed drive can be replaced without shutting down the server. However, there are serious risks in trying to swap a drive that has not failed.
>
> - Do not assume that because the red LED is illuminated that a drive is faulty. Under a RAID rebuild/recovery, the red LED is illuminated. If the drive fails and must be replaced, remove it from the server.
>
> - If the drive shows signs of failure (through warning events in the event log), the drive can be replaced as it is hot-swappable.
>
> - Do not pull out a drive that is in a known good configuration. Doing so can potentially lead to data corruption.
>
> - Unless you are certain the drive has failed, perform a disk recovery.
>
> - Drive redundancy is unsupported if the drive is removed from the server.
>
> - The new drive does not require the same capacity as the drive being replaced.

> **WARNING:** It is strongly recommended that you perform drive replacement procedures during a maintenance window to minimize risk of any disruption caused by the procedure and to allow for the movement of EVSs and other unexpected events that may occur.

Replacing a power supply unit

You can replace a power supply unit (PSU) as a hot-swappable server component. The server can operate on a single PSU if necessary, making it possible to replace a failed PSU without shutting down the server. If a PSU fails, it must 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.

> **Note:** Refer to the section on Power supply units (on page 37) for more information.

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 main power circuit is live and that the other end of the power cable is connected to a live outlet.

Chapter 6: Rebooting, shutting down, and powering off

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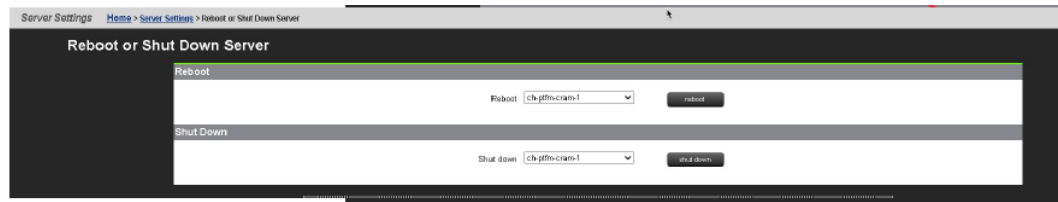
Rebooting or shutting down a server or cluster

Procedure

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

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

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

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

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

Restarting an unresponsive server

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

Procedure

1. Connect to the SMU using the SSH software.

2. From the siconsole, select the server.

   ■ If the system fails to respond, go to step 3.

   ■ If the system takes you to the server OS console, issue the **bt active** command, so you can view the display.

   ■ If you are still at the siconsole, select **q**, press `Return`, and then perform the following steps:

      a. Connect directly to the CMB as manager using SSH.
      b. If the connection succeeds, you are taken to the server OS console, where you issue the **bt active** command.
      c. If the connection fails, continue to step 4.

3. Connect to the system with a serial null modem cable, and perform the following steps: See if you need details.

   a. Log in as manager or you will get the Linux prompt, not the server OS.

      If you use root, use the **ssc localhost** command.

   b. Issue the command: **bt active**.

4. If you are still unable to get to the server OS, perform the following steps:

   a. Ensure that the NAS CLI is booting successfully.

    b. Log in through the serial cable connection.

    c. Tail **`/var/opt/mercury-main/logs/dblog`**.

    d. Search the log for the entry

        `MFB.ini not found run nas-preconfig.`

- If the entry is present, the system has been unconfigured by either running the **`unconfig`** script or by 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 process 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

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

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

Procedure

1. From the NAS Platform operating system console, enter the command: `shutdown --powerdown`

2. Wait until the rear panel LEDs turn off.

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

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

Powering on the server or cluster

To start/power on a server or cluster:

Procedure

1. Verify that all servers are switched off.

2. Start all storage systems, beginning with the expansion enclosures.

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

3. For a cluster configuration, verify the SMU has been installed and configured in the customer VMware or HyperV environment.
   Wait one minute to allow the external SMU to start.

4. If you are starting a cluster, wait 5 - 10 seconds before powering on the next node in the cluster.

Recovering from power stand-by

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

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

- The `shutdown --powerdown` command has been issued.

- The PWR button is pressed when the server is running.

- The server has shut down automatically due to an over-temperature condition.

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

- Press the PWR button.

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

Chapter 7: Server replacement procedures

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

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

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

Replacement procedure overview

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

Server replacement requirements

Consider the following server replacement requirements:

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

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

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

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

Swapping components

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

The components that can be swapped include:

- Power supplies

- Bezel

- Rack mounting guides

MAC ID and license keys

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

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

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

Previous backups

A system backup preserves two critical components of information:

- SMU configuration

- Server configuration

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

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

Upgrades

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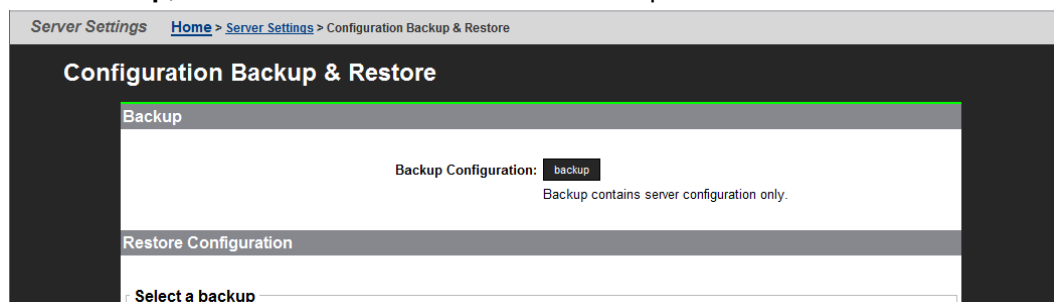
Replacing a server

Obtaining backups, diagnostics, firmware levels, and license keys

On the old server:

Procedure

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

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

3. For a node in a cluster, backup the Node Registry.
4. For a node in a cluster, migrate the EVSs to an alternate node.
5. Navigate to **Home** > **Status & Monitoring** > **Download Diagnostics**.
6. Click **download** to retrieve the diagnostic test results.

> **Note:** Unless the SMU is actively managing Brocade Fibre Channel switches, un-check the Fibre Channel Switches box.

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

The server firmware version on the new server must match the failed server otherwise the server cannot properly restore from the backup file. See the Release Notes for release-specific requirements.

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

9. Record the following information:

- IP addresses for Ethernet ports 0 and 1

- Gateway

- Domain name

- Host name

Shutting down a server that you are replacing

On the server that you are replacing:

Procedure

1. From the server console, enter the **shutdown --powerdown** command.
2. 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.

3. Unplug the power cords from the power supplies.
4. For a node in a cluster, once the node is shut down, go to **Home** > **Server Settings** > **Cluster Configuration** and delete the entry for the node that you are replacing.
5. Use the following rear panel figure and table to identify and label the cabling placement on the existing server.
6. If cables are not labeled, label them before removing them from the server.
7. Remove all cables from the server, and remove the server from the rack.
8. Remove the rail mounts from the old server, and install them on the new server.
9. Remove the power supply from the old server, and install it in the new server.
10. Remove the bezel from the old server, and install it on the new server.
11. 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.

IP addresses are required for the following:

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

For a single NAS server, 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 to be managed.

The reconfigured settings are:

- 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.

   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.
5. Use a keyboard, video, and mouse (KVM) device or a serial cable to connect to the serial port. 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
6. Log in as `root`, and enter the `ssc localhost` command to access the command prompt.
7. If using SAN attached, and/or host group security, update this to reflect the changes that are being made to the WWN, as described in Capturing information from the existing node.
8. Add the new node as a managed server on the SMU.
9. Enter `evs list` to see the IP configuration for the server.
10. Using a supported browser, launch the NAS Manager using either one of the IP addresses acquired from the EVS list output.
11. Click **Yes** to proceed past the security alert, and log in as `admin`.
12. Verify and, if necessary, convert the new server to the model profile required.

    This step requires a separate process, training, and license keys. Contact Hitachi Vantara if the incorrect model arrives for replacement.
13. Navigate to **Home** > **Server Settings** > **Firmware Package Management** to verify and, if necessary, upgrade the new server to the latest SU release.
14. When replacing a server in a cluster only, navigate to **Home** > **Server Settings** > **Cluster Wizard**, and promote the node to the cluster.
    a. Enter the cluster name, cluster node IP address, subnet, and select a quorum device. Note that the node reboots several times during this process.
    b. When prompted, add the second node to the cluster.

Chapter 7: Server replacement procedures

    c. Enter the physical node IP address, log in as `supervisor`, and click **finish**. Wait for the system to reboot.

    d. Enter **`smu-uninstall`** to uninstall the embedded SMU.

15. For all servers, navigate to **Home** > **Server Settings** > **Configuration Backup & Restore**, select the required backup file, and then click **restore** to restore the system from that backup file.

16. When replacing a server in a cluster only, 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.

17. Navigate to **Home** > **Server Settings** > **License Keys** to load the license keys.

18. Reboot the server.

19. Reconnect the data cables to the server.

Finalizing and verifying the replacement server configuration

The maximum Fibre Channel (FC) link speed on the NAS Platform Series 5000 is 16 Gbps.

On the replacement server:

Procedure

1. Navigate to **Home** > **Server Settings** > **License Keys** to load the license keys.

2. Remove the previous license keys in the backup file, then 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. Modify zoning and switches with the new WWPN, if you are using WWN-based zoning. If you are using port-based zoning, no modifications are necessary for the switch configurations.

5. Open Device Manager - Storage Navigator and re-configure the 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.

6. If the server does not recognize the system drives, enter **`fc-link-reset`** to reset the fiber paths.

7. Enter the **`sdpath`** command to display the path to the devices (system drives) and the port and storage port that are used.

8. Enter the **`sd-list`** command to verify the system drive statuses are OK and that access is allowed.

9. Use the 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
```

10. Enter `span-list` to verify the storage pools (spans) are accessible.

    > **Note:** In this instance, cluster is synonymous with the stand-alone server.

11. Enter the `span-list-cluster-uuids` `span_label` command to display the cluster serial number (UUID) to which the storage pool belongs.
    The UUID is written into the storage pool 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 the `span-assign-to-cluster` `span_label` command to assign all the spans to the new server.

13. If EVS mapping or balancing is required, select the EVS to migrate, assign it to the preferred node, then click **migrate**.
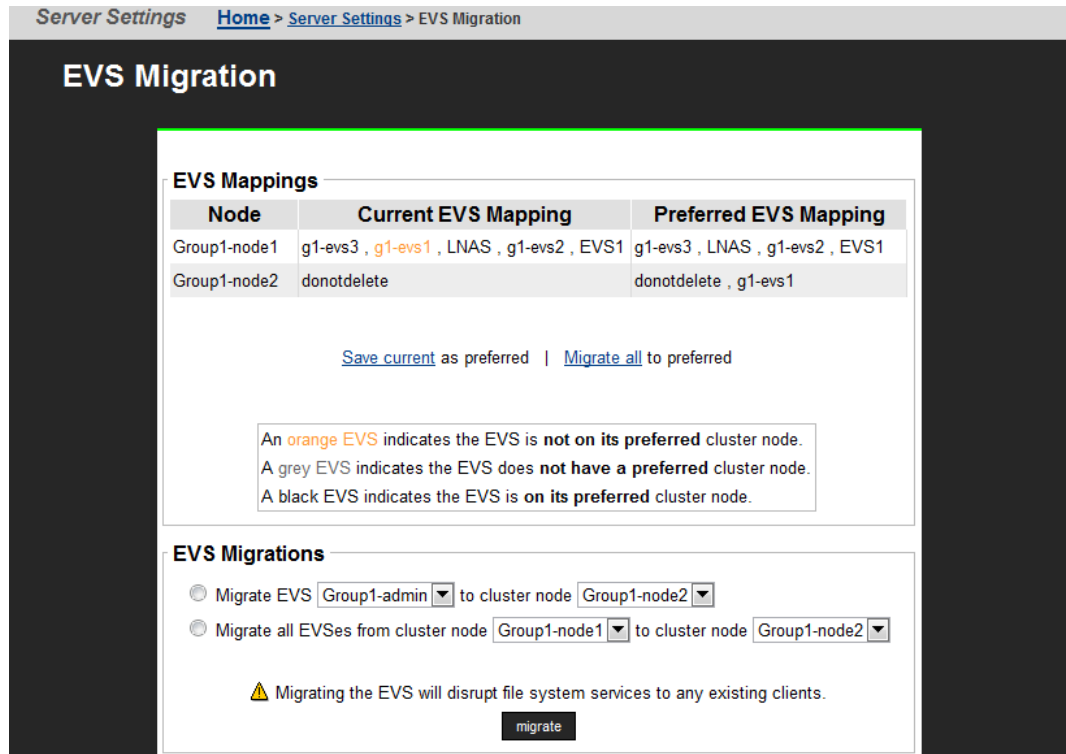
14. To set the preferred node for any remaining EVSs, navigate to **Home** > **Server Settings** > **EVS Management** > **EVS Details**.
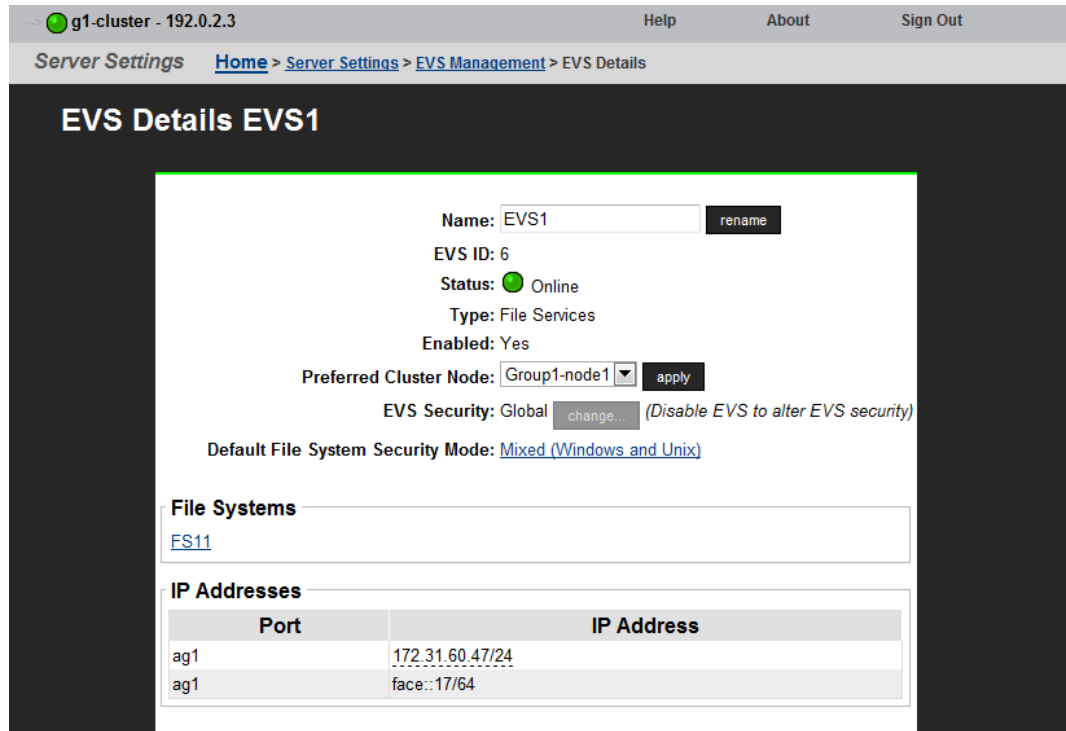
15. Select the node from the Preferred Cluster Node list, then click **apply**.

16. Reconfigure any required tape backup application security.

17. Navigate to **Home** > **Status & Monitoring** > **Event Logs**, and click **Clear Event Logs**.

18. 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, then download another diagnostic to support. Permanent license keys for the replacement server are normally provided within seven days.

    ▪ If the server is not operating normally for any reason, contact Customer Support for assistance.

19. Navigate to **Home** > **Server Settings** > **Cluster Configuration** to verify the cluster configuration status. Verify the cluster is shown as Online and Robust and has the correct number of nodes.

20. 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 must all be confirmed as working, and all file systems and storage pools must be online.

Chapter 8: Accessing the server CLI

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

Chapter 9: Parts list for NAS Platform Series 5000

Parts for NAS Platform Series 5000 servers

Part number	Description	Notes
SX325151	Server	Does not include PSUs, bezel, or rail kit
SX325152	PSU	80 Plus Platinum rated
SX325155	SSD	2 per server
SX170320	Fibre Channel SFP+	
SX325116	Fan tray	2 per server
SX325142	Clip in rail kit	
SX325150	Bezel	

Switch Parts

Part number	Description	Notes
ICX6430-24	Managed 24-port Ethernet 10/100/1000 Base-Tnotes – Used for private management network when desired	
BR-VDX6740-24-F(or R)	▪ Brocade VDX 6740 ▪ 10GbE Switch, 16 ports ▪ SFP+, AC, "F" for front side or "R" for rear side exhaust ▪ Exhaust AF	

Part number	Description	Notes
10G-SFP-SR	▪ Brocade VDX 6740 ▪ Cisco Nexus 3524-X or XL ▪ SW 10GbE SFP+	
N3K-C3524P-10GX N3K-C3524P-XL	▪ Cisco Nexus 3524-X or XL switch ▪ 10GbE Switch 24 ports enabled, but upgradeable to 48 ports ▪ Port-side exhaust is default	

Optics used with NAS Platform Series 5000 servers

Part number	Description	Notes
FTLX8574D3BCL-HD	▪ SFP+ 10GbE 400 meters ▪ 850 nm. multi-mode ▪ 3.3v	Supported in: ▪ 6 x 10GbE network ports ▪ 4 x cluster ports Not supported in 4 x Fibre Channel ports
AFBR-710SMZ-HT1/ FTLX8574D3BCL-HD/ PLRXPL-SC-S43-HT1	▪ SFP+ 10GbE 300 meters ▪ 850 nm. multi-mode ▪ 3.3v	Supported in: ▪ 6 x 10GbE network ports ▪ 4 x cluster ports Not supported in: 4 x Fibre Channel ports
SFP16-SR-SP	SFP+ 16GbE FC 100 meters 850nm Fibre Channel 4.25-14.025 Gbps	Supported in: 4 x Fibre Channel ports Not supported in: ▪ 6 x 10GbE network ports ▪ 4 x cluster ports

Part number	Description	Notes
FTLX1475D3BCV	▪ SFP + 10GbE 10km ▪ 1310 nm. single-mode ▪ 3.3v	Supported in: ▪ 6 x 10GbE network ports ▪ 4 x cluster ports Not supported in: 4 x Fibre Channel ports

Copper cables used with NAS Platform Series 5000 servers

Part number	Description	Notes
SFP-H10GB-CU1M	▪ Copper cable - SFP+ ▪ 10GbE passive twinax, for 10GbE network ports, 1 meter	▪ Supported in 6 x 10GbE network ports ▪ Not supported in 4 x cluster ports ▪ Not supported in 4 x Fibre Channel ports
SFP-H10GB-CU3M	▪ Copper cable - SFP+ ▪ 10GbE passive twinax, for 10GbE network ports, 3 meters	▪ Supported in 6 x 10GbE network ports ▪ Not supported in 4 x cluster ports ▪ Not supported in 4 x Fibre Channel ports
SFP-H10GB-CU5M	▪ Copper cable - SFP+ ▪ 10GbE passive twinax, for 10GbE network ports, 5 meters	▪ Supported in 6 x 10GbE network ports ▪ Not supported in 4 x cluster ports ▪ Not supported in 4 x Fibre Channel ports

Hitachi Vantara