

Hitachi Advanced Server HA800 G2 Series

Troubleshooting Guide

This document describes common procedures and solutions for the many levels of troubleshooting servers. This document is intended for the person who installs, administers, and troubleshoots servers and server blades. Hitachi Vantara assumes you are qualified to service computer equipment and are trained in recognizing hazards in products with hazardous energy levels.

2021 Hitachi, Ltd. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

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

Preface

This document describes common procedures and solutions for the many levels of troubleshooting servers. This document is intended for the person who installs, administers, and troubleshoots servers and server blades. Hitachi Vantara assumes you are qualified to service computer equipment and are trained in recognizing hazards in products with hazardous energy levels.

Please read this document carefully to understand how to use these products, and maintain a copy for your reference.

Accessing product documentation

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

Getting help

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

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

Thank you!

Contents

Using this guide	9
Getting started	9
Supported servers	10
Additional troubleshooting resources	10
Troubleshooting preparation.....	11
Prerequisites for server troubleshooting	11
Important safety information	12
Symbols on equipment	12
Warnings and cautions	13
Electrostatic discharge	15
Collecting symptom information.....	15
Preparing the server for diagnosis.....	15
Processor troubleshooting guidelines.....	16
Breaking down the server to the minimum hardware configuration.....	17
Common issue resolution	19
Resolving loose connections.....	19
Searching for service notifications.....	19
Firmware updates	19
Server updates with an Trusted Platform Module and BitLocker enabled	20
DIMM handling guidelines	20
DIMM and NVDIMM population information	21
Intel Xeon Scalable Processors supported on G2 servers	21
DIMM-processor compatibility	21
NVDIMM-processor compatibility.....	21
Component LED definitions	21
Storage	21
Front panel LED and buttons.....	26
Front panel LED power fault codes	29
Controller and energy pack cables	31
Remote troubleshooting	32
Remote troubleshooting tools	32
Using iLO for remote troubleshooting of servers	32
Diagnostic flowcharts	34
Diagnostic steps	34
Gather important information before you begin	34
Troubleshooting flowcharts.....	34
Using the Diagnostic flowcharts	34
Initial diagnosis	34
Remote diagnosis flowchart	35
Power-on issues flowchart	36
POST issues flowchart	38
OS boot issues flowchart.....	43

Intelligent Provisioning issues flowchart.....	44
Controller issues flowchart.....	46
Energy pack issues for smart array controllers	48
Physical drive issues flowchart.....	51
Fault indications flowchart	55
NIC issues flowchart.....	57
General diagnosis flowchart.....	60
Hardware issues	62
Procedures for all Advanced Server products	62
Power issues	62
Server does not power on.....	62
Power source issues	62
Power supply issues	63
UPS issues.....	65
General hardware issues	67
New hardware issues	67
Unknown issue.....	68
Third-party device issues.....	69
Drive issues (hard drives and solid state drives)	70
Drives are failed.....	70
Drives are not recognized	71
Data is inaccessible	72
Server response time is slower than usual.....	72
SmartDrive icons or LEDs illuminate errors for the wrong drive or an error message is displayed in POST, SSA, or SSADUCLI	73
SSD Smart Wear error	73
Diagnosing array problems	74
Storage controller issues	74
General controller issues.....	74
Controllers are no longer redundant.....	75
Data located on drives accessed in RAID mode is not compatible with data accessed from non-RAID mode	76
The smart array controller does not show logical drives after moving drives to a new server or JBOD	76
Data failure or disk errors on a server with a 10 SFF drive backplane or a 12 LFF drive backplane	77
Smart array S100i SR G2 drives are not found when RAID mode is disabled.....	77
Smart array S100i SR G2 drives are not recognized.....	78
Fan and thermal issues.....	78
General fan issues	78
Fans running at a higher than expected speed.....	79
Excessive fan noise (high speeds).....	80
Excessive fan noise (low speeds)	80
Hot-plug fan issues	81
Memory issues.....	81
General memory issues	81
Server is out of memory.....	82
DIMM configuration errors	83
Server fails to recognize existing memory	84
Server fails to recognize new memory	85
Uncorrectable memory error	86
Correctable memory error threshold exceeded	86

Persistent Memory issues	87
Persistent Memory module percentage remaining alerts	87
For more information, see the user guide for your server.	87
Persistent Memory Module configuration errors	87
Persistent Memory Module goal configuration errors	88
Persistent Memory module memory health errors	89
NVDIMM issues	90
NVDIMM population errors	90
NVDIMMs are disabled	90
The persistent memory drive does not appear in the OS	91
The persistent memory drive is read only	92
The persistent memory drives lose persistency.....	93
Scalable Persistent Memory issues	94
The persistent memory drive does not appear in the OS	94
The persistent memory drive is read only	95
The persistent memory drives lose persistency.....	97
Scalable Persistent Memory backup and restore failure	97
Unable to configure Scalable Persistent Memory	99
Processor issues	99
Troubleshooting the processor.....	99
Uncorrectable machine check exception	100
Trusted Platform Module issues	101
TPM fails or is not detected	101
System battery is low or lost power	102
System board and power backplane issues	102
microSD card issues	103
The system does not boot from the microSD card	103
USB drive key issues	103
System does not boot from the USB drive key	103
Graphics and video adapter issues.....	104
Troubleshooting general graphics and video adapter issues	104
Video issues	104
The screen is blank for more than 60 seconds after you power up the server	104
Monitor does not function properly with energy saver features	106
Video colors are wrong	106
Slow-moving horizontal lines are displayed	106
Mouse and keyboard issues.....	107
Expansion board issues	107
System requests recovery method during expansion board replacement	107
Network controller or FlexibleLOM issues.....	108
Network controller or FlexibleLOM is installed but not working.....	108
Network controller or FlexibleLOM has stopped working.....	108
Network controller or FlexibleLOM stopped working when an expansion board was added ..	109
Network performance or virtual machine performance issues with G2 servers with AMD processors	110
Energy pack issues	110
Energy pack support in G2 servers.....	111
The energy pack might lose charge when shelved for long periods of time	111
Energy pack configuration error.....	111
Energy pack failure.....	112
Cable issues	112
Drive errors, retries, timeouts, and unwarranted drive failures occur when using an older Mini SAS cable	112
USB device not recognized, an error message is displayed, or the device does not power on when	

connected to an SUV cable	113
Software issues	114
Operating system issues and resolutions	114
Operating system issues.....	114
Updating the operating system	114
Reconfiguring or reloading software.....	115
Linux resources	115
Application software issues	116
Software locks up	116
Errors occur after a software setting is changed.....	116
Errors occur after the system software is changed	116
Errors occur after an application is installed	117
ROM issues.....	117
Remote ROM flash issues	117
Boot issues.....	120
Software and configuration utilities.....	122
Server mode.....	122
Active Health System.....	122
iLO Federation.....	124
iLO Service Port	124
iLO RESTful API	125
RESTful Interface Tool	125
Intelligent Provisioning.....	125
Intelligent Provisioning operation	125
Management security	126
UEFI System Utilities	126
Selecting the boot mode	127
Secure Boot.....	127
Launching the Embedded UEFI Shell.....	128
Smart Storage Administrator	129
USB support.....	129
External USB functionality.....	129
Redundant ROM support	129
Safety and security benefits	129
Keeping the system current.....	130
Updating firmware or system ROM	130
Drivers	132
Software and firmware.....	132
Operating system version support.....	132
Reports and logs	133
Reports and Logs overview.....	133
Active Health System Log	133
Active Health System Log download methods	133
Intelligent Provisioning diagnostic tools	139
Performing a Diagnostics task using SSA.....	139
Smart Storage Administrator Diagnostics Utility CLI	140
Installing the utility	140
Launching the utility in CLI mode.....	140

Diagnostic report procedures	140
SmartSSD Wear Gauge report procedures	141
Linux reports	141
Symptom information checklist.....	142

Using this guide

Getting started

NOTE: For common troubleshooting procedures, the term "server" is used to mean servers.

This guide provides common procedures and solutions for troubleshooting a Hitachi Advanced Server product- from the most basic connector issues to complex software configuration issues.

To understand the sections of this guide and to identify the best starting point for an issue, review the following descriptions:

- **Troubleshooting preparation**

This section provides information on how to prepare to begin troubleshooting the server, including important safety information, tips on how to gather symptom information, how to prepare your server to begin diagnosis, and other pre-diagnostic information.

- **Common issue resolution**

Many server issues are caused by loose connections, outdated firmware, and other issues. Use this section to perform basic troubleshooting for common issues.

- **Remote troubleshooting**

This section provides a list of the tools and processes to begin troubleshooting a server from a remote location.

- **Diagnostic flowcharts**

If a server exhibits symptoms that do not immediately pinpoint the issue, use this section to begin troubleshooting. The section contains a series of flowcharts that provide a common troubleshooting process for Hitachi Advanced Server products. The flowcharts identify a diagnostic tool or a process to help solve the issue.

- **Hardware issues**

If the symptoms point to a specific component, use this section to find solutions for issues with power, general components, system boards, system open circuits and short circuits, and external devices.

- **Software issues**

If you have a known, specific software issue, use this section to identify and solve the issue.

- **Software and configuration utilities**

Use this section as a reference for software tools and utilities.

- **Reports and logs**

Use this section for more information about the reports and logs you can generate during the troubleshooting process or prior to contacting Hitachi Vantara Support.

- **Resources for troubleshooting**

When additional information becomes necessary, use this section to identify websites and supplemental documents that contain troubleshooting information.

Supported servers

The Troubleshooting Guide for G2 Servers focuses on troubleshooting procedures for the following:

- HA800 servers
- HA800 G2 servers

Additional troubleshooting resources

Additional troubleshooting resources are available for G2 server products in the following documents:

- Error Message Guide for Hitachi Advanced Server HA800 G2 servers provides a list of error messages and information to assist with interpreting and resolving error messages.
- Error Message Guide for Hitachi Advanced Server HA800 servers provides a list of error messages and information to assist with interpreting and resolving error messages.
- Troubleshooting Guide for Hitachi Advanced Server HA800 G2 servers provides associated troubleshooting information to resolve critical and cautionary events.

To access troubleshooting resources for your product, see the Hitachi Vantara Website:

- For G2 servers, see https://knowledge.hitachivantara.com/Documents/Servers/Advanced_Server.

Troubleshooting preparation

Prerequisites for server troubleshooting



WARNING: To avoid potential issues, ALWAYS read the warnings and cautionary information in the product documentation before removing, replacing, reseating, or modifying system components.



IMPORTANT: This document provides information for multiple server products. Some information might not apply to the server you are troubleshooting. For information on procedures, hardware options, software tools, and operating systems supported by the server, see the server documentation.

Procedure

2. Before you change the server, gather and record symptom information. If the server powers on or if auxiliary power is available, download the Active Health System Log and obtain the OS logs.

The OS logs are available only when the system has power.

For more information, see the iLO User Guide on the [Hitachi Vantara website](#).

To obtain OS logs, see the OS documentation.

If you choose to not download the Active Health System Log, you must gather all symptom information, including the following:

- POST error messages
- OS logs
- Physical symptoms (LED behavior, physical state, and so on)

For more information about gathering symptom information, see the Symptom information checklist.

3. If it is necessary to contact customer support.
4. Prepare the server for diagnosis.
5. To begin the diagnostic process, see Initial diagnosis.

More information

[Important safety information](#)

[Symptom information checklist](#)

[Preparing the server for diagnosis](#)

[Initial diagnosis](#)

Important safety information

Familiarize yourself with the safety information in the following sections before troubleshooting the system.



Important safety information

Symbols on equipment

The following symbols might be found on the equipment to indicate the presence of potentially hazardous conditions.



This symbol indicates the presence of hazardous energy circuits or electric shock hazards. Refer all servicing to qualified personnel.

WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure. Refer all maintenance, upgrades, and servicing to qualified personnel.



This symbol indicates the presence of electric shock hazards. The area contains no user or field serviceable parts. Do not open for any reason.

WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure.



This symbol on an RJ-45 receptacle indicates a network interface connection.

WARNING: To reduce the risk of electric shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



This symbol indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



weight in kg

weight in lb

This symbol indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.



These symbols, on power supplies or systems, indicate that the equipment is supplied by multiple sources of power.

WARNING: To reduce the risk of injury from electric shock, remove all power cords to disconnect power from the system completely.

Warnings and cautions



WARNING: Only authorized technicians trained by Hitachi Vantara should attempt to repair this equipment. All troubleshooting and repair procedures are detailed to allow only subassembly/module-level repair. Because of the complexity of the individual boards and subassemblies, no one should attempt to make repairs at the component level or to make modifications to any printed wiring board. Improper repairs can create a safety hazard.



WARNING: To reduce the risk of personal injury or damage to the equipment, consult the safety information and user documentation provided with the server before attempting the installation.

Some servers contain high energy circuits, high current circuits, moving parts, or any combination of these hazards, that may be exposed if covers are removed while the product is connected to a power source. These products are intended to be serviced only by qualified personnel who have been trained to deal with these hazards. Do not remove enclosures or attempt to bypass any interlocks designed to guard against these hazardous conditions.



WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling feet are extended to the floor.
- The full weight of the rack rests on the leveling feet.
- The stabilizing feet are attached to the rack if it is a single-rack installation.
- The racks are coupled together in multiple-rack installations.
- Only one component is extended at a time. A rack may become unstable if more than one component is extended for any reason.



- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply to disconnect power to the equipment.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.



WARNING: To reduce the risk of personal injury or damage to the equipment:

weight

in kg

weight

in lb

- Observe local occupation health and safety requirements and guidelines for manual handling.
 - Obtain adequate assistance to lift and stabilize the chassis during installation or removal.
 - The server is unstable when not fastened to the rails.
 - When mounting the server in a rack, remove the power supplies and any other removable module to reduce the overall weight of the product.
-

⚠ CAUTION: To properly ventilate the system, you must provide at least 7.6 cm (3.0 in) of clearance at the front and back of the server.

⚠ CAUTION: The server is designed to be electrically grounded (earthed). To ensure proper operation, plug the AC power cord into a properly grounded AC outlet only.

Electrostatic discharge

Preventing electrostatic discharge

To prevent damaging the system, be aware of the precautions you must follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

Procedure

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding methods to prevent electrostatic discharge

Several methods are used for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part. For more information on static electricity or assistance with product installation, contact an authorized reseller.

Collecting symptom information

Before troubleshooting a server issue, collect the symptom information.

For more information about collecting symptom information, use the Symptom information checklist.

More information

[Symptom information checklist](#)

Preparing the server for diagnosis

Procedure

1. Be sure the server is in the proper operating environment with adequate power, air conditioning, and humidity control.
For more information, see the server user guide.
2. Record any error messages displayed by the system.
3. Remove all CDs, DVD-ROMs, USB drive keys, or SD cards that are not bootable devices.
4. Collect all tools and utilities necessary to troubleshoot the issue. Items you might need include a Torx screwdriver, loopback adapters, ESD wriststrap, and software utilities.
 - You must have the appropriate support software installed on the server.
 - Hitachi Vantara recommends that you have access to the server documentation for server-specific information.
5. Determine if the server will be diagnosed offline or online:
 - If you will diagnose the server online, complete steps 6 and 8.
 - If you will diagnose the server offline, complete steps 7 and 8.
6. To diagnose the server online, review and collect the following information:
 - a. Review the iLO information on both the **Overview** and the **System Information** pages.
 - b. Review the **Diagnostics** page.
 - c. If the OS is operating is installed, then review the operational status.
 - d. Download the Active Health System Log.
 - e. Record survey data.
7. To diagnose the server offline, power down the server and peripheral devices. If possible, always perform an orderly shutdown:
 - a. Exit any applications.
 - b. Exit the operating system.
 - c. Power down the server.
8. Disconnect any peripheral devices not required for testing (any devices not necessary to power up the server).

More information

[Active Health System Log](#)

User guide for your Server

Processor troubleshooting guidelines

CAUTION: When reducing the server to a minimum configuration for troubleshooting, do not remove additional processors. Processors and heatsinks are not designated for customer self repair. The processor and heatsink must be removed and replaced by an authorized service provider.

Before performing any troubleshooting steps that involve processors, review the following guidelines:

- Be sure that only authorized personnel perform the troubleshooting steps that involve installation, removal, or replacement of a processor.
- Always complete all other troubleshooting procedures before an authorized service provider removes or replaces a processor.

Breaking down the server to the minimum hardware configuration

During the troubleshooting process, you might be asked to break the server down to the minimum hardware configuration. A minimum configuration consists of only the components required to boot the server and successfully complete POST.

 **CAUTION:** When reducing the server to a minimum configuration for troubleshooting, do not remove additional processors. Processors and heatsinks are not designated for customer self repair. The processor and heatsink must be removed and replaced by an authorized service provider.

Prerequisites

Before removing the components, be sure to determine the minimum configuration for each component and follow all guidelines in the server user guide. Always use the recommended minimum configuration before removing any DIMMs.

Procedure

1. When requested to break down the server to the minimum configuration, uninstall the following components, if installed:
 - All additional cooling fans, if applicable
For the minimum fan configuration, see the server user guide or the chassis setup and installation guide.
 - All additional power supplies, if applicable (leave one installed)
 - All hard drives and SSDs
 - All optical drives (DVD, CD, and so forth)
 - All optional mezzanine cards
 - All expansion boards
2. If the issue cannot be isolated with the minimum configuration, then remove all but the minimum number of associated DIMMs for each processor as directed by the Hitachi Vantara Support Center.

Common issue resolution

Resolving loose connections

- Be sure that all power cords are securely connected.
- Be sure that all cables are properly aligned and securely connected for each external and internal component.
- Remove and check all data and power cables for damage. Be sure that no cables have bent pins or damaged connectors.
- If a cable routes through air baffles or other components, be sure the cords and cables connected to the server are routed correctly through the baffle.
- Be sure that each device is properly seated. Avoid bending or flexing circuit boards when reseating components.
- If a device has latches, be sure that they are completely closed and locked.
- Check any interlock or interconnect LEDs that might indicate that a component is not connected properly.
- If issues continue to occur, remove, and reinstall each device, checking the connectors and sockets for bent pins or other damage.

Searching for service notifications

Service notifications are created to provide solutions for known issues. Check to see if your issue is covered by an existing service notification.

Procedure

1. See the [Hitachi Vantara website](#).
2. Enter the product name or number, and then press **Enter**.
3. To show the documents available for your product, select **Documents**.
4. To narrow the results, select from the available options to filter by document type.

Some of the document types you may include are as follows:

- **Advisory**—Provides a problem and solution to an issue or a workaround.
- **Bulletin or Security Bulletin**—Provides information about a potential product safety or security vulnerability.
- **Notice**—Provides general information, announcements, or best practices.

Firmware updates

Many common issues can be resolved by updating the firmware. Firmware updates and additional information can be found in the following ways:

- SPV: Update the firmware by downloading SPV from the website (<https://support.hitachivantara.com/en/user/answers/downloads.html#hardware-download>).
- Hitachi Vantara Support Center website: Update the firmware by downloading the most recent version of a particular server or option firmware from the Hitachi Vantara Support Center website (<https://support.hitachivantara.com/en/user/answers/downloads.html#hardware-download>).
- Subscription services: Hitachi Vantara offers a subscription service that can provide notification of firmware updates.

More information

Service Pack for Advanced Server

Server updates with an Trusted Platform Module and BitLocker enabled

When a TPM is installed and enabled in UEFI System Utilities, and when the Microsoft Windows BitLocker Drive Encryption feature is enabled, always disable BitLocker before performing any of the following procedures:

- Restarting the computer for maintenance without a PIN or startup key
- Updating firmware when a TPM is installed
- Upgrading critical early boot components
- Replacing the system board
- Replacing the system board to replace or remove the TPM
- Disabling or clearing the TPM
- Moving a BitLocker-protected drive to another server
- Adding an optional PCI device, such as a storage controller or network adapter

For more information, see [Hitachi Vantara website](#)

DIMM handling guidelines



CAUTION: Failure to properly handle DIMMs can cause damage to DIMM components and the system board connector.

When handling a DIMM, observe the following guidelines:

- Avoid electrostatic discharge.
- Always hold DIMMs by the side edges only.
- Avoid touching the connectors along the bottom of the DIMM.
- Never wrap your fingers around a DIMM.
- Avoid touching the components on the sides of the DIMM.
- Never bend or flex the DIMM.

When installing a DIMM, observe the following guidelines:

- Before seating the DIMM, open the DIMM slot and align the DIMM with the slot.
- To align and seat the DIMM, use two fingers to hold the DIMM along the side edges.
- To seat the DIMM, use two fingers to apply gentle pressure along the top of the DIMM.

For more information, contact customer support.

DIMM and NVDIMM population information

For specific DIMM and NVDIMM population information,

Intel Xeon Scalable Processors supported on G2 servers

Depending on the server, a server supports either first or second-generation Intel Xeon Scalable processors.

To determine the generation, look at the four-digit processor model number.

- If the second digit is a 1 (X1XX), you have a first-generation Intel Xeon Scalable processor.
- If the second digit is a 2 (X2XX), you have a second-generation Intel Xeon Scalable processor.

 **IMPORTANT:** Existing G2 server products containing first-generation Intel Xeon Scalable processors may not be upgraded to second-generation Intel Xeon Scalable processors at this time.

DIMM-processor compatibility

The installed processor determines the type of DIMM that is supported in the server:

- First-generation Intel Xeon Scalable processors support DDR4-2666 DIMMs.
- Second-generation Intel Xeon Scalable processors support DDR4-2933 DIMMs.

Mixing DIMM types is not supported. Install only the supported DDR4-2666 or DDR4-2933 DIMMs in the server.

NVDIMM-processor compatibility

16GB NVDIMMs are only supported in servers with first-generation Intel Xeon Scalable processors installed.

Component LED definitions

[Hitachi Vantara website.](#)

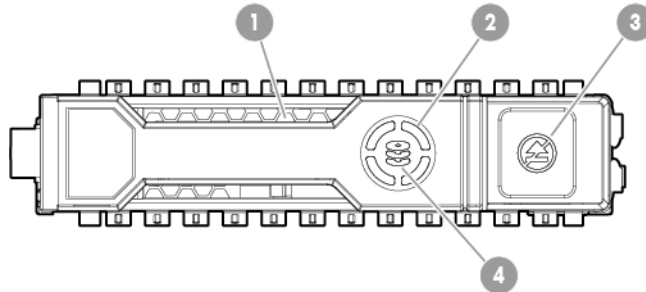
Storage

SAS, SATA, and SSD drive guidelines

When adding drives to the server, observe the following general guidelines:

- Drives must be of the same capacity to provide the greatest storage space efficiency when drives are grouped in the same drive array.
- Drives in the same logical volume must be of the same type. SSA does not support mixing SAS, SATA, and SSD drives in the same logical volume.

Hot-plug drive LED definitions

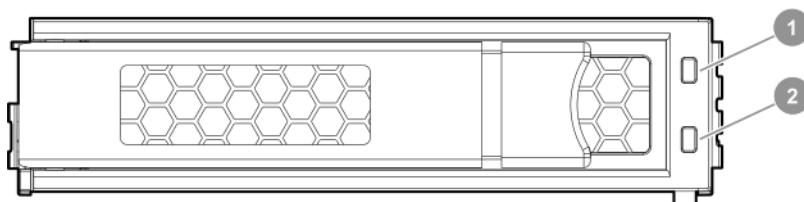


Item	LED	Status	Definition
1	Locate	Solid blue	The drive is being identified by a host application.
		Flashing blue	The drive carrier firmware is being updated or requires an update.
2	Activity ring	Rotating green	Drive activity
		Off	No drive activity
3	Do not remove	Solid white	Do not remove the drive. Removing the drive causes one or more of the logical drives to fail.
		Off	Removing the drive does not cause a logical drive to fail.
4	Drive status	Solid green	The drive is a member of one or more logical drives.
		Flashing green	The drive is doing one of the following: · Rebuilding · Performing a RAID migration · Performing a strip size migration · Performing a capacity expansion · Performing a logical drive extension · Erasing · Spare part activation
		Flashing amber/green	The drive is a member of one or more logical drives and predicts the drive will fail.
		Flashing amber	The drive is not configured and predicts the drive will fail.

Table Continued

Item	LED	Status	Definition
		Solid amber	The drive has failed.
		Off	The drive is not configured by a RAID controller or a spare drive.

Low-profile LFF drive LED definitions

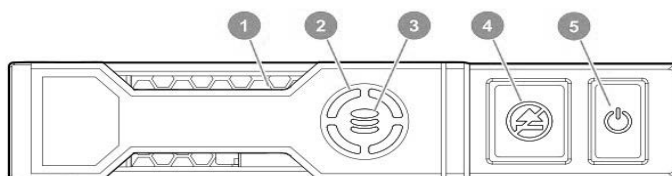


Item	LED	Status	Definition
1	Fault Locate	Solid amber	The drive has failed.
		Solid blue	The drive is operating normally and being identified by a management application.
		Flashing amber/blue (1 flash per second)	The drive has failed, or a predictive failure alert has been received for this drive; it also has been identified by a management application.
		Flashing amber (1 flash per second)	A predictive failure alert has been received for this drive. Replace the drive as soon as possible.
2	Online Activity	Solid green	The drive is online and has no activity.
		Flashing green (4 flashes per second)	The drive is operating normally and has activity.
		Flashing green (1 flash per second)	The drive is doing one of the following: - Rebuilding - Performing a RAID migration - Performing a strip size migration - Performing a capacity expansion - Performing a logical drive extension - Erasing - Spare part activation
		Off	The drive is not configured by a RAID controller or a spare drive.

NVMe SSD LED definitions

The NVMe SSD is a PCIe bus device. A device attached to a PCIe bus cannot be removed without allowing the device and bus to complete and cease the signal/traffic flow.

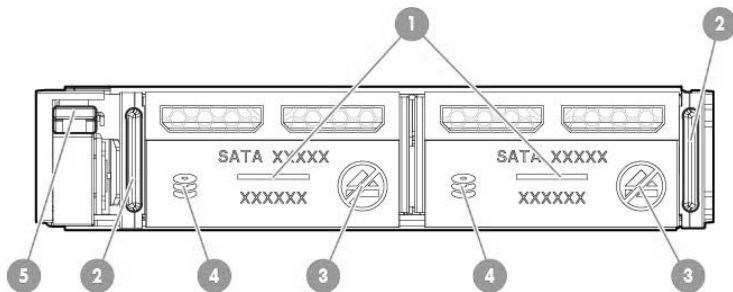
⚠ CAUTION: Do not remove an NVMe SSD from the drive bay while the Do not remove LED is flashing. The Do not remove LED flashes to indicate that the device is still in use. Removing the NVMe SSD before the device has completed and ceased signal/traffic flow can cause loss of data.



Item	LED	Status	Definition
1	Locate	Solid blue	The drive is being identified by a host application.
		Flashing blue	The drive carrier firmware is being updated or requires an update.
2	Activity ring	Rotating green	Drive activity
		Off	No drive activity
3	Drive status	Solid green	The drive is a member of one of more logical drives.
		Flashing green	The drive is done one of the following: • Rebuilding • Performing a RAID migration • Performing a stripe size migration • Performing a capacity expansion • Performing a logical drive extension • Erasing
		Flashing amber/green	The drive is a member of one or more logical drives and predicts the drive with fail.
		Flashing amber	The drive is not configured and predicts the drive with fail.
		Solid amber	The drive has failed.
		Off	The drive is not configured by a RAID controller.
4	Do not remove	Solid white	Do not remove the drive. The drive must be ejected from the PCIe bus prior to removal.
		Flashing White	The drive ejection request is pending.

Item	LED	Status	Definition
		Off	The drive has been ejected.
5	Power	Solid green	Do not remove the drive. The drive must be ejected from the PCIe bus prior to removal.
		Flashing green	The drive ejection request is pending.
		Off	The drive has been ejected.

SFF flash adapter components and LED definitions



Item	Component	Description
1	Locate	Off—Normal
		Solid blue—The drive is being identified by a host application.
		Flashing blue—The drive firmware is being updated or requires an update.
2	uFF drive ejection latch	Removes the uFF drive when released.
3	Do not remove LED	• Off—OK to remove the drive. Removing the drive does not cause a logical drive to fail.
		• Solid white—Do not remove the drive. Removing the drive causes one or more of the logical drives to fail.

Table Continued

Item	Component	Description
4	Drive status LED	- Off—The drive is not configured by a RAID controller or a spare drive. - Solid green—The drive is a member of one or more logical drives. - Flashing green (4 Hz)—The drive is operating normally and has activity. - Flashing green (1 Hz)—The drive is rebuilding, erasing, or performing a RAID migration, stripe size migration, capacity expansion, logical drive extension, or spare activation. - Flashing amber/green (1 Hz)—The drive is a member of one or more logical drives that predicts the drive will fail. - Solid amber—The drive has failed. - Flashing amber (1 Hz)—The drive is not configured and predicts the drive will fail.
5	Adapter ejection release latch and handle	Removes the SFF flash adapter when released.

System power LED definitions

The system power LED is on the Power On/Standby button and each status is defined as shown in the following table.

System power LED	Definition
Off (Server)	System has no power.
Off	If the Health Status LED bar is off, then the system has no power. If the Health Status LED bar is flashing green, then the Power On/Standby Button service is being initialized.
Solid amber	System is in standby, Power On/Standby Button service is initialized.
Flashing green	System is waiting to power on, Power On/Standby button is pressed.
Solid green	System is powered on.

Front panel LED and buttons

Standard descriptions for most G2 servers are provided in this section.

Description	Status
UID LED/button	Solid blue = Activated Off = UID is deactivated and iLO Service Port is ready for use. Flashing blue: 1 Hz/cycle per sec = Remote management or firmware upgrade in progress 4 Hz/cycle per sec = iLO manual reboot sequence initiated

Table Continued

- 8 Hz/cycle per sec = iLO manual reboot sequence in progress
- 1 fast flash and then off for 3 seconds = iLO Service Port status is Complete.
- 4 medium flashes and then off for 1 second = iLO Service Port status is Busy.
- 8 fast flashes and then off for 1 second = iLO Service Port status is Error.

Power On/Standby button and system power LED	Solid green = System on Flashing green (1 Hz/cycle per sec) = Performing power on sequence Solid amber = System in standby Off = No power present
Health LED	Solid green = Normal Flashing green (1 Hz/cycle per sec) = iLO is rebooting. Flashing amber = System degraded Flashing red (1 Hz/cycle per sec) = System critical
NIC status LED	Solid green = Link to network Flashing green (1 Hz/cycle per sec) = Network active Off = No network activity

More information

See the user guide for your server.

Front panel LED notations

For more information about LED combinations and LED definitions, review the following:

- When all four front panel LEDs flash simultaneously, a power fault has occurred.
- The server UID also flashes to indicate the status of the iLO Service Port.

For more information, see the iLO documentation on the [Hitachi Vantara website](#)

- When the system power LED is off, one of the following is true:

- Facility power is not present.
 - The power cord is not attached.
 - Power supplies are not seated properly.
 - No power supplies are installed.
 - A power supply failure has occurred.
 - The power backplane, if installed, is not seated properly.
 - The PDU has issues.
 - The Power On/Standby Button cable is disconnected.
- If the health LED indicates a degraded or critical state, use iLO to review the system health status.

More information

[Front panel LED power fault codes](#)

Using the Server Health Summary

You can use iLO to display the Server Health Summary on an external monitor when the server is powered on or off. Use this feature for troubleshooting when the server will not start up. This feature can also be used to view the server IP address and other health information.

Prerequisites

- The server has a UID button.
- An external monitor is connected.
- The **Show Server Health on External Monitor** feature is enabled on the **Access Settings** page.

Procedure

1. Press the UID button on the server.



CAUTION: Press and release the UID button. Holding it down at any time for more than 5 seconds initiates a graceful iLO reboot or a hardware iLO reboot. Data loss or NVRAM corruption might occur during a hardware iLO reboot.

The Server Health Summary screen is displayed on the external monitor.

2. Press the UID button again to close the Server Health Summary screen.

Server Health Summary details

Server screen thumbnail

A thumbnail image of the server screen.

Server Power

The server power status.

Product Name

The server model.

Serial Number

The server serial number.

Product ID

The product with which this iLO processor is integrated.

iLO Firmware

The installed iLO Firmware version.

System ROM

The installed system ROM version.

Backup ROM

The backup system ROM version.

iLO CPLD

The installed iLO CPLD version.

System CPLD

The installed system CPLD version.

Embedded smart array

The installed smart array firmware version. This value is displayed only if server POST has successfully completed since the last auxiliary power cycle.

iLO IPv4

The iLO IPv4 address. This value is displayed only if **Show iLO IP during POST** is enabled on the **Access Settings** page.

iLO IPv6

The iLO IPv6 address. This value is displayed only if **Show iLO IP during POST** is enabled on the **Access Settings** page.

iLO Hostname

The iLO hostname.

Front panel LED power fault codes

When a power fault occurs, the following front panel LEDs flash simultaneously:

- System power LED
- Health LED
- NIC LED
- UID LED

For more information about the LED locations on your server, see the user guide for your server.

The number of flashes in each sequence corresponds to the subsystem impacted by the power fault. The following table provides a list of power fault codes, and the subsystems that are affected. Not all power faults are used by all servers.

Subsystem	Front panel LED behavior
System board	1 flash
Processor	2 flashes
Memory	3 flashes

Riser board PCIe slots	4 flashes
FlexibleLOM	5 flashes
Removable Flexible smart array controller/Smart SAS HBA controller	6 flashes
System board PCIe slots	7 flashes
Power backplane or storage backplane	8 flashes
Power supply	9 flashes

Controller and energy pack cables

When an energy pack and smart array P-class SR or MR G2 controllers are installed in the server, be sure to install and properly seat all required cables.

Energy pack cable

The energy pack cable is a cable connected to each energy pack and can be either 145mm or 260mm in length. When an energy pack is installed, always verify that the energy pack cable is connected properly. For more information about installing and cabling the energy pack, see the server user guide.

Controller backup power cable

The controller backup power cable is a cable that provides backup power to controllers installed in PCIe slots and the DIMM slots on the system board. If a smart array P-class SR or MR G2 controller is installed in a PCIe slot, be sure to install the controller backup power cable. For more information about installing and cabling the controller backup power cable, see the server user guide.

More information

Server user guide

Remote troubleshooting

Remote troubleshooting tools

Hitachi Vantara provides several options that help IT administrators troubleshoot a server from remote locations.

iLO

iLO enables the monitoring and controlling of servers from remote locations. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely.

For more information about iLO features (which may require a specific iLO license), see the iLO documentation on the [Hitachi Vantara website](#)

Active Health System

The Active Health System monitors and records changes in the server hardware and system configuration. The Active Health System assists in diagnosing issues and delivering rapid resolution when server failures occur. The ActiveHealth System log, in conjunction with the system monitoring provided by Agentless Management or SNMP Pass-thru, provides continuous monitoring of hardware and configuration changes, system status, and service alerts for various server components.

If you are unable to resolve the issues, submit a support case through [Hitachi Vantara website](#).

More information

[iLO 5](#)

[Active Health System](#)

[Using the CLI](#)

Using iLO for remote troubleshooting of servers

Prerequisites

For more information about the information in this section, see the iLO User Guide on the Hitachi Vantara (<https://knowledge.hitachivantara.com/Documents/Servers>).

Procedure

1. Log in to the iLO web interface.
2. Review the initial **Overview** screen for status and health.
Observe the following fields on the Overview screen:
 - System ROM
 - iLO Firmware Version
 - System Health
 - Server Power
 - SD-Card Status
3. To display the Summary tab, click **System Information** in the navigation tree.

- a. Review all installed Subsystems and Devices and verify that all devices show the OK status with a green icon.
 - b. If any degraded subsystems or devices exist, then click the degraded subsystems or device to review the current status.
4. From the System Information page, select the **Storage** tab.
 - a. Verify that all storage devices show the OK status with a green icon.
 - b. If any degraded subsystems or devices exist, then click the degraded subsystems or device to review the status.
5. To review firmware and OS information, click **Firmware & OS Software** in the navigation tree.

The Firmware tab is displayed.
6. Review the iLO Event Log for possible hardware faults on power-on or boot up issues when the server is not booting properly.
 - a. To access the logs, click **Information** in the navigation tree.
 - b. Click the **iLO Event Log**.
7. Click **Information** in the navigation tree, and then select the **Diagnostics** tab.

From this page, you can do the following depending on your server:

 - Verify the status of the iLO Self-Test results.
 - Use the **Reset** button to reset iLO.
 - If a memory dump recording is required, use the **Generate NMI to System** button to Initiate NMI for a memory dump recording.
 - Boot to system safe mode.
 - Boot to Intelligent Diagnostics mode.
 - Restore the default manufacturing settings.
 - Restore the default system settings.
8. Be sure the **Power On** and **Health status** icons in the top right on the iLO web interface pages are green.

Diagnostic flowcharts

Diagnostic steps

To effectively troubleshoot an issue, Hitachi Vantara recommends that you start with Initial diagnosis, and follow the appropriate diagnostic path.

If the other flowcharts do not provide a troubleshooting solution, follow the diagnostic steps in the General diagnosis flowchart. The General diagnosis flowchart is a generic troubleshooting process to be used when the issue is not server-specific or is not easily categorized into the other flowcharts.

More information

[Initial diagnosis](#)

[General diagnosis flowchart](#)

Gather important information before you begin

Before you begin troubleshooting the issue, gather the following information for use during troubleshooting and for use if the issue requires contacting Hitachi Vantara support:

- Active Health System log
- OS logs
- Symptom information
- POST error messages
- Other

More information

[Active Health System](#)

[Symptom information checklist](#)

[Using the CLI](#)

[Reports and Logs overview](#)

Troubleshooting flowcharts

Using the Diagnostic flowcharts

Some information provided in the flowcharts can be further explained in conjunction with other sources of information provided on the Hitachi Vantara website and in other sections of this document. To locate the appropriate information, see the references following the flowchart. Each reference corresponds to the underlined text in the flowchart.

Initial diagnosis

This section helps you decide which flowchart can help you with your issue.

- Remote diagnosis flowchart—To diagnose the issue from a remote location.
- Server power-on issues flowchart DL series servers— Advanced Server G2 series server does not power on.
- POST issues flowchart—An overview that directs you to the correct flowchart when your server does not complete POST.
- POST issues—Server hang or reboot during POST flowchart—A server hangs or reboots during the boot process.
- POST issues—No boot, no video flowchart—A server does not boot and has no video.
- POST issues—Boot, no video flowchart—A server boots, but has no video.
- OS boot issues flowchart—A server does not boot to the OS.
- Intelligent Provisioning issues flowchart—A server does not boot to Intelligent Provisioning.
- Controller issues flowchart—A controller is not shown during POST or if your controller shows errors.
- Energy pack issues for smart array controllers — An energy pack is not recognized or is not charging.
- Physical drive issues flowchart—Physical drives are not shown or if errors are displayed during POST.
- Logical drive issues flowchart—Logical drives are not shown or if errors are displayed during POST.
- Server fault indications flowchart for non-blade servers—A nonblade server has Insight Management Agent faults or faults indicated by LEDs.
- NIC issues flowchart—A NIC is not working.
- General diagnosis flowchart—All other issues.

Remote diagnosis flowchart

❗ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

To troubleshoot a server from a remote location, use iLO. If the issue still exists, contact customer support.

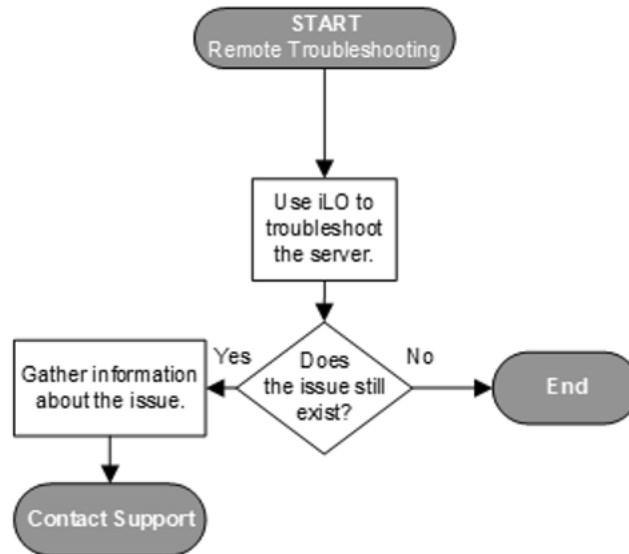


Figure 1: Remote troubleshooting flowchart

More information

[Active Health System](#)

[Using iLO for remote troubleshooting of servers](#)

Power-on issues flowchart

Server power-on issues flowchart and DL series servers

Symptom

- The server does not power on.
- The server does not respond when the power button is pressed.
- The system power LED is off or solid amber.
- The health LED is solid red, flashing red, solid amber, or flashing amber.
- All front panel LEDs flash in unison.

Cause

- Improperly seated or faulty power supply
- Loose or faulty power cord
- Power source issue
- Improperly seated component or interlock issue

❗ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

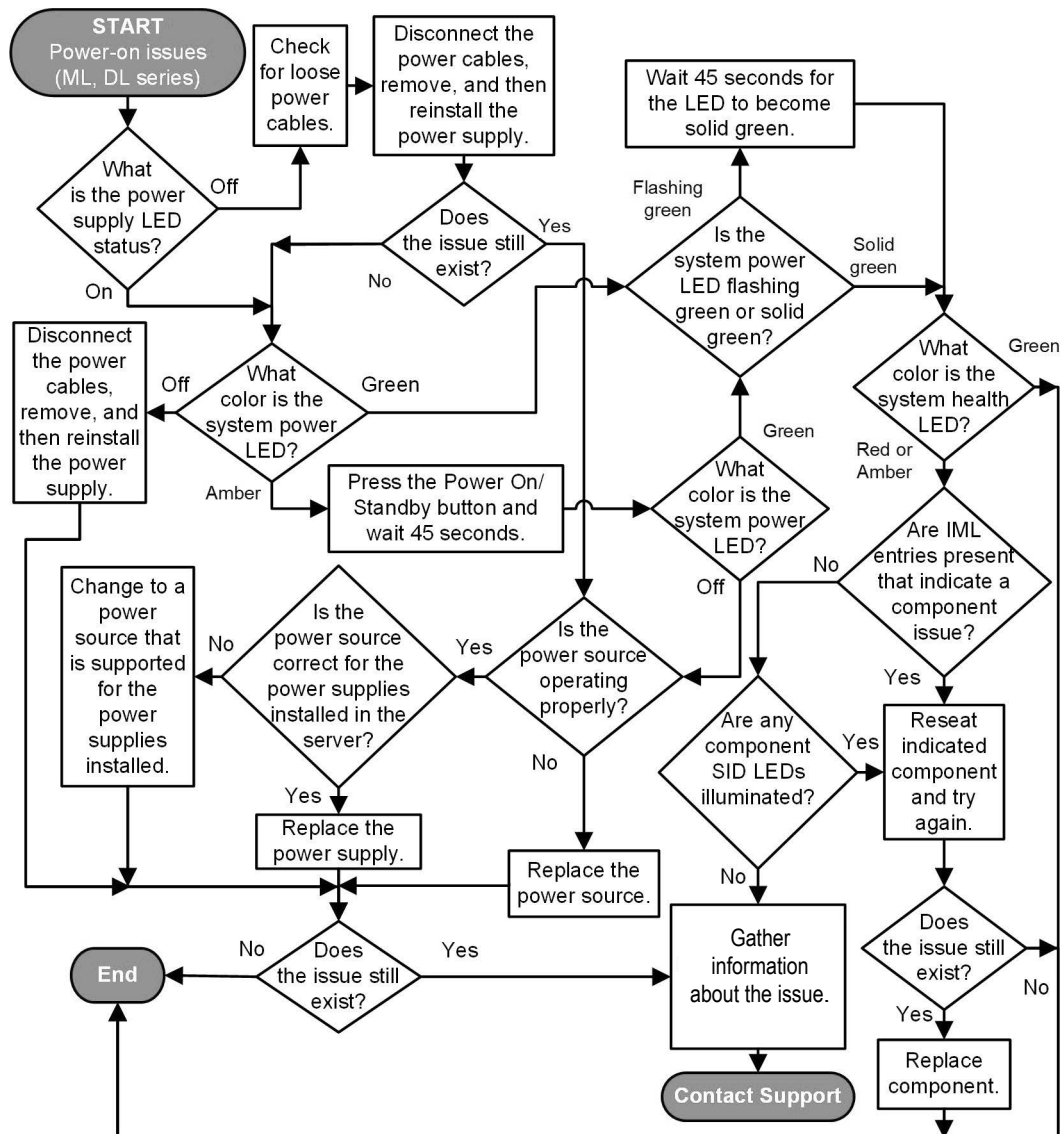


Figure 2: Server power-on issues flowchart and DL series servers

For the location of server LEDs and information on their statuses, see the user guide for your server).

For removal and replacement procedures, see the server maintenance and service guide for your server.

More information

[System power LED definitions](#)

[Resolving loose connections](#)

[Front panel LED and buttons](#)

[Power source issues](#)

POST issues flowchart

Symptom

- The server does not complete POST
- The server completes POST with errors

Cause

- Improperly populated memory
- Outdated firmware on adapter options
- Unsupported adapter
- Improperly seated or faulty internal component

ⓘ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

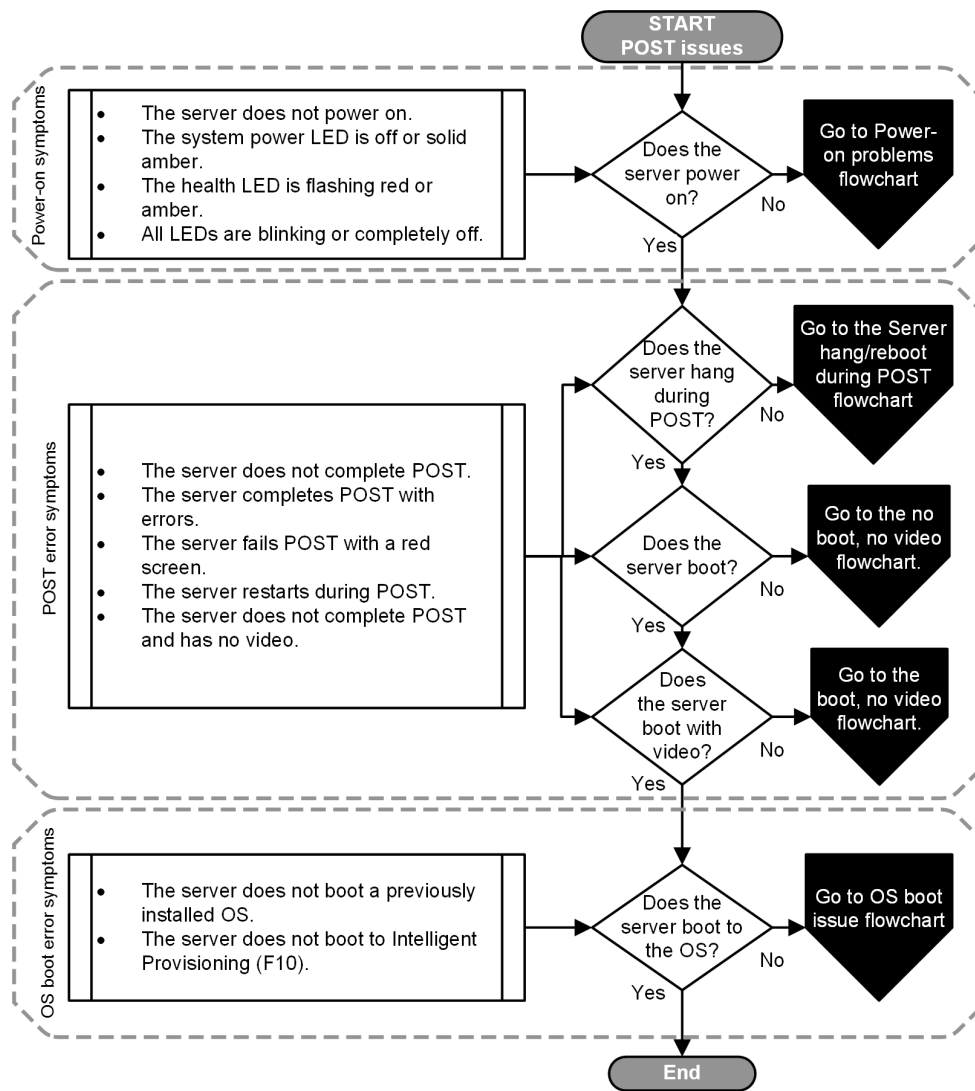


Figure 6: POST issues flowchart

More information

[Power-on issues flowchart](#)

[POST issues—Server hang or reboot during POST flowchart](#)

[POST issues—Boot](#)

[OS boot issues flowchart](#)

POST issues—Server hang or reboot during POST flowchart

Symptom

The server hangs or reboots during POST and does not boot.

Action

To resolve the issue, follow the steps in the flowchart.

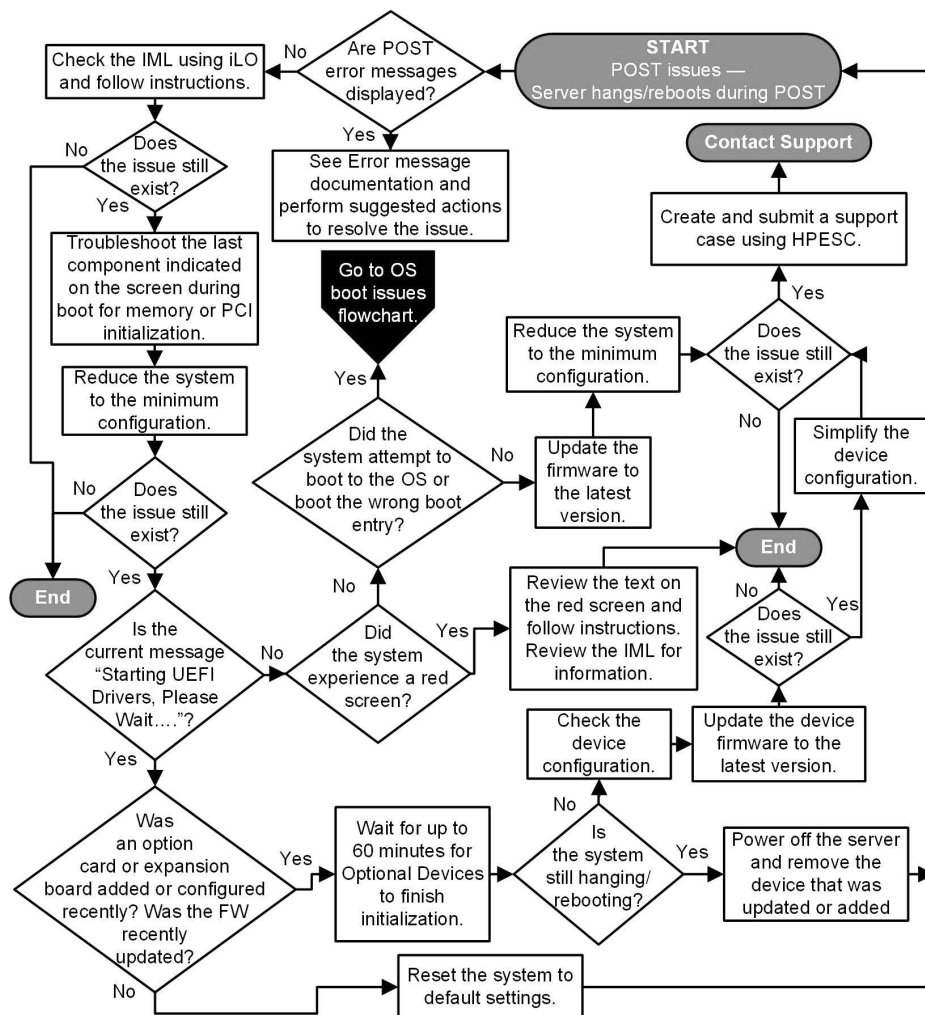


Figure 7: POST issues—Server hangs or reboots during POST flowchart

For the location of server LEDs and information on their statuses, see the user guide for your server.

For removal and replacement procedures, see the user guide for your server

For more information about error messages, see the error message guide on the [Hitachi Vantara website](#)

More information

[Active Health System](#)

[Firmware updates](#)

[OS boot issues flowchart](#)

POST issues—No boot

Symptom

The server will not boot.

Action

To resolve the issue, follow the steps in the flowchart.

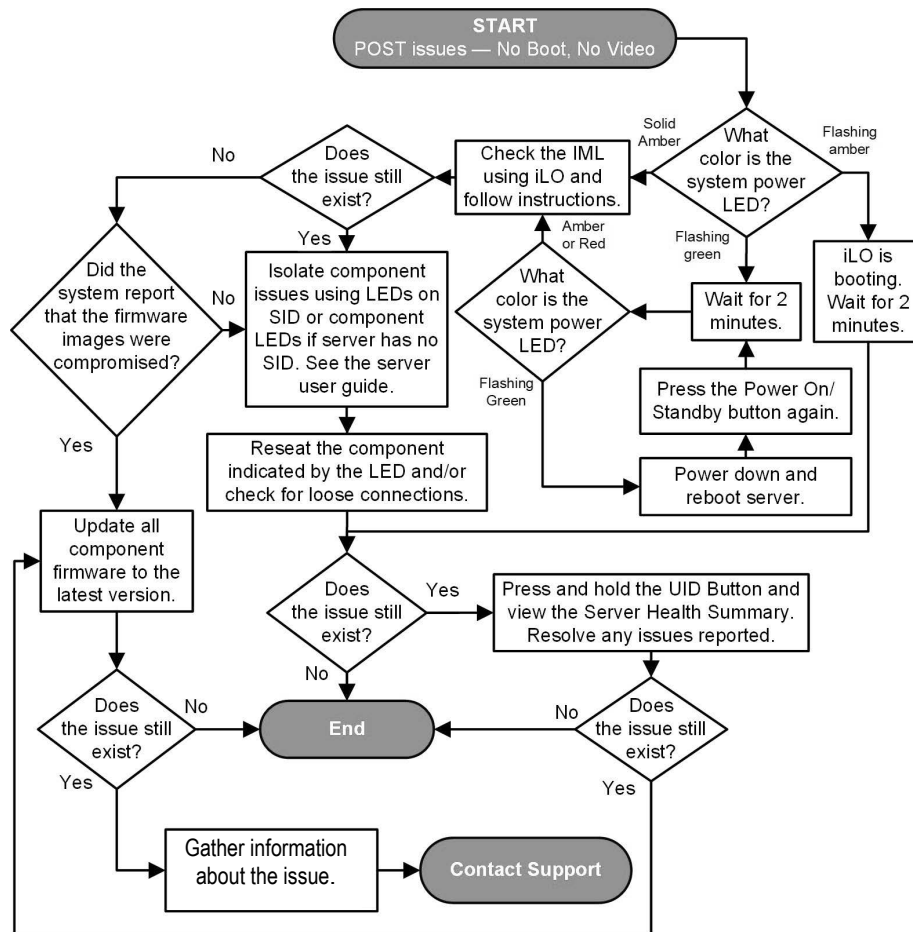


Figure 8: POST issues—No boot

For the location of server LEDs and information on their statuses, see the user guide for your server.
user guide for your server.

More information

[System power LED definitions](#)

[Resolving loose connections](#)

[Using the Server Health Summary](#)

[Component LED definitions](#)

[Firmware updates](#)

POST issues—Boot

Symptom

The server boots, but has no video output.

Action

To resolve the issue, follow the steps in the flowchart.

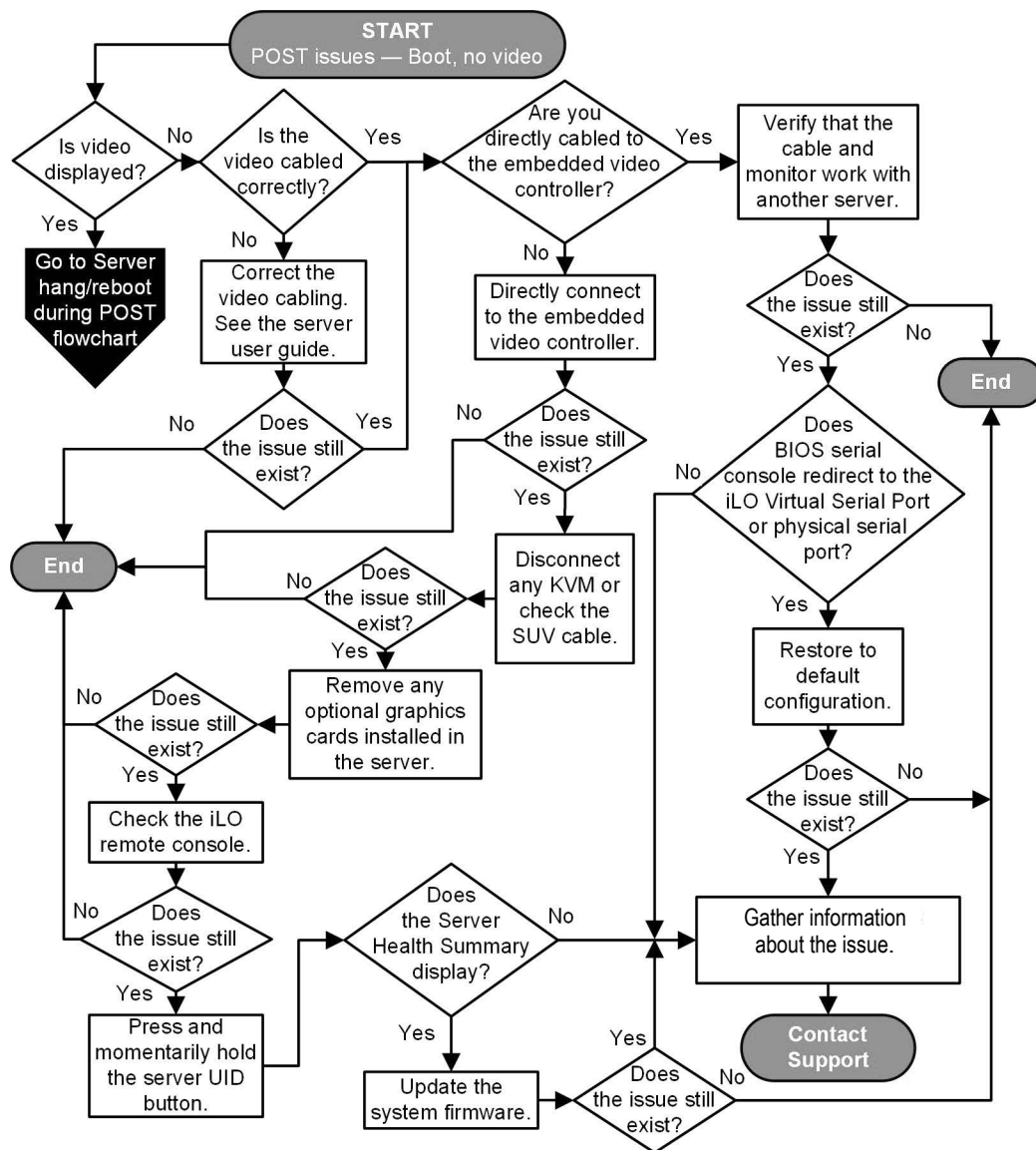


Figure 9: POST issues—Boot, no video flowchart

For the location of server LEDs and information on their statuses, see the server user guide for your server.
For removal and replacement procedures, see the user guide for your server.

More information

[POST issues—Server hang or reboot during POST flowchart](#)

[POST issues—No boot](#)

OS boot issues flowchart

Symptom

The server does not boot a previously installed OS.

Cause

- Corrupted OS
- Drive subsystem issue
- Incorrect setting in UEFI System Utilities
- Issue with the boot order
- An item in the boot order failed or was removed
- Set for UEFI boot mode versus Legacy boot mode



IMPORTANT: Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

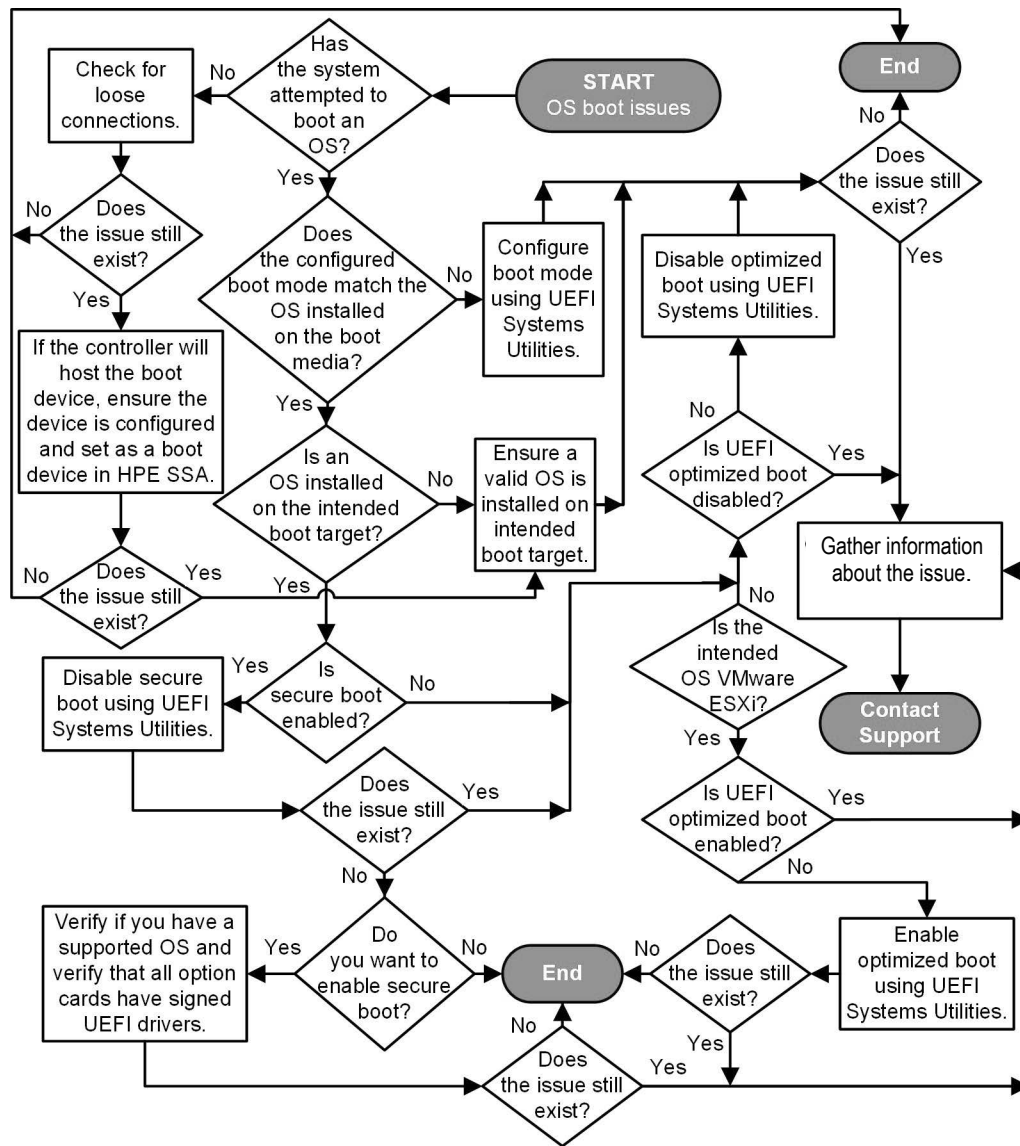


Figure 10: OS boot issues flowchart

For more information about UEFI System Utilities, see the UEFI System Utilities documentation on the [Hitachi Vantara website](#)

More information

[PXE boot guidelines for UEFI servers](#)

[UEFI System Utilities documentation](#)

[Resolving loose connections](#)

Intelligent Provisioning issues flowchart

Symptom

The server does not boot to Intelligent Provisioning (F10).

Cause

- Corrupted installation of Intelligent Provisioning
- Drive subsystem issue
- Incorrect setting in UEFI System Utilities

❗ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

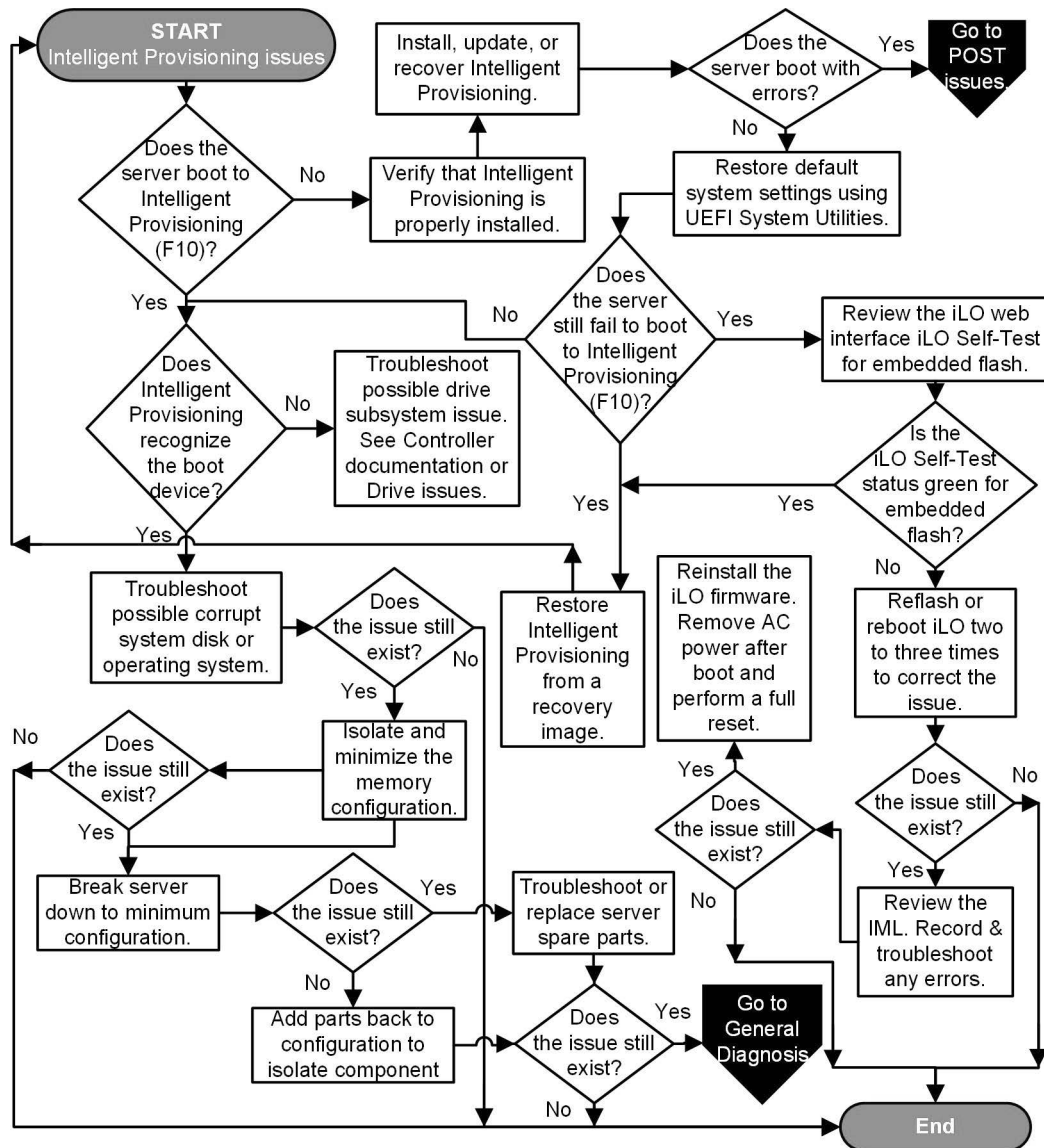


Figure 11: Intelligent Provisioning issues flowchart

For more information about Intelligent Provisioning, see the Intelligent Provisioning documentation on the [Hitachi Vantara website](#)

For more information about UEFI System Utilities, see the UEFI System Utilities documentation on the [Hitachi Vantara website](#)

For removal and replacement procedures, see the user guide for your server.

More information

[Drive issues \(hard drives and solid state drives\)](#)

[Operating system issues and resolutions](#)

[Isolating and minimizing the memory configuration](#)

[Breaking down the server to the minimum hardware configuration](#)

[POST issues flowchart](#)

[General diagnosis flowchart](#)

Controller issues flowchart

Symptom

- The controller is not displayed in UEFI System Utilities.
- The controller is not displayed in SSA.

Cause

- The hardware is physically damaged.
- The controller is not supported on the server.
- The controller is faulty.
- The processor is not installed for the PCIe slot where the controller is installed.
- The firmware is outdated.

 **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

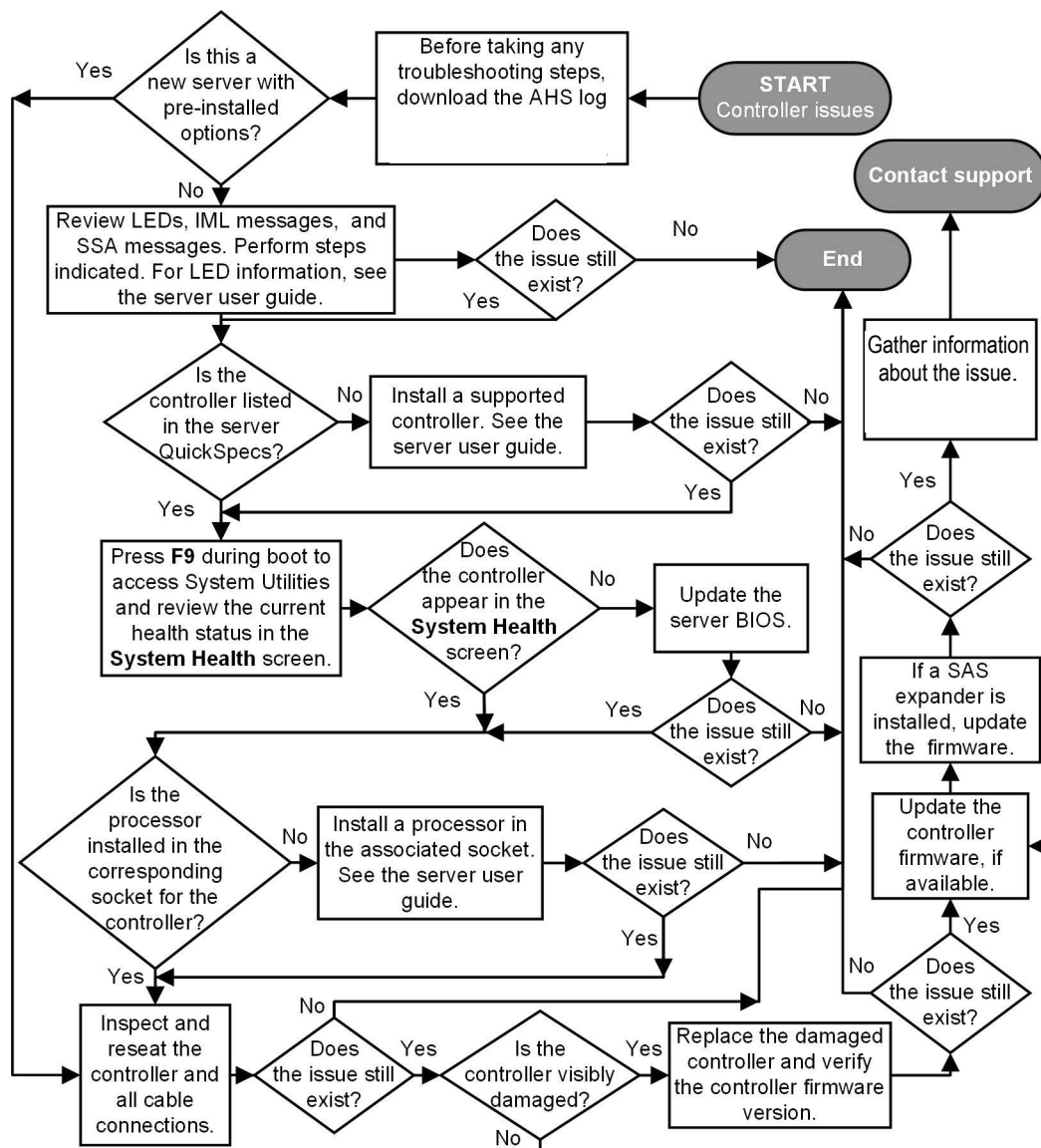


Figure 12: Controller issues flowchart

For more information about error messages, see the error message guide on the [Hitachi Vantara website](#)

For removal and replacement procedures, see the user guide for your server.

For installation procedures, see the user guide for your server.

More information

[Updating firmware or system ROM](#)

[Gather important information before you begin](#)

[Controller and energy pack cables](#)

Energy pack issues for smart array controllers

Symptom

- The energy pack is not recognized.
- The energy pack is not charging.
- The energy pack is reported as failed.

Cause

- The energy pack is unsupported on this server.
- The energy pack cable connector is not connected properly.
- The controller backup power cable is not connected properly or is not installed.
- The energy pack is faulty.

IMPORTANT: Before you make changes to your system, always download the Active Health System log.



Action

-
- !** **IMPORTANT:** Before you begin the steps, verify that the firmware for the controller and the firmware for iLO are the latest versions.
-

1. To resolve the issue, follow the steps in the flowchart.

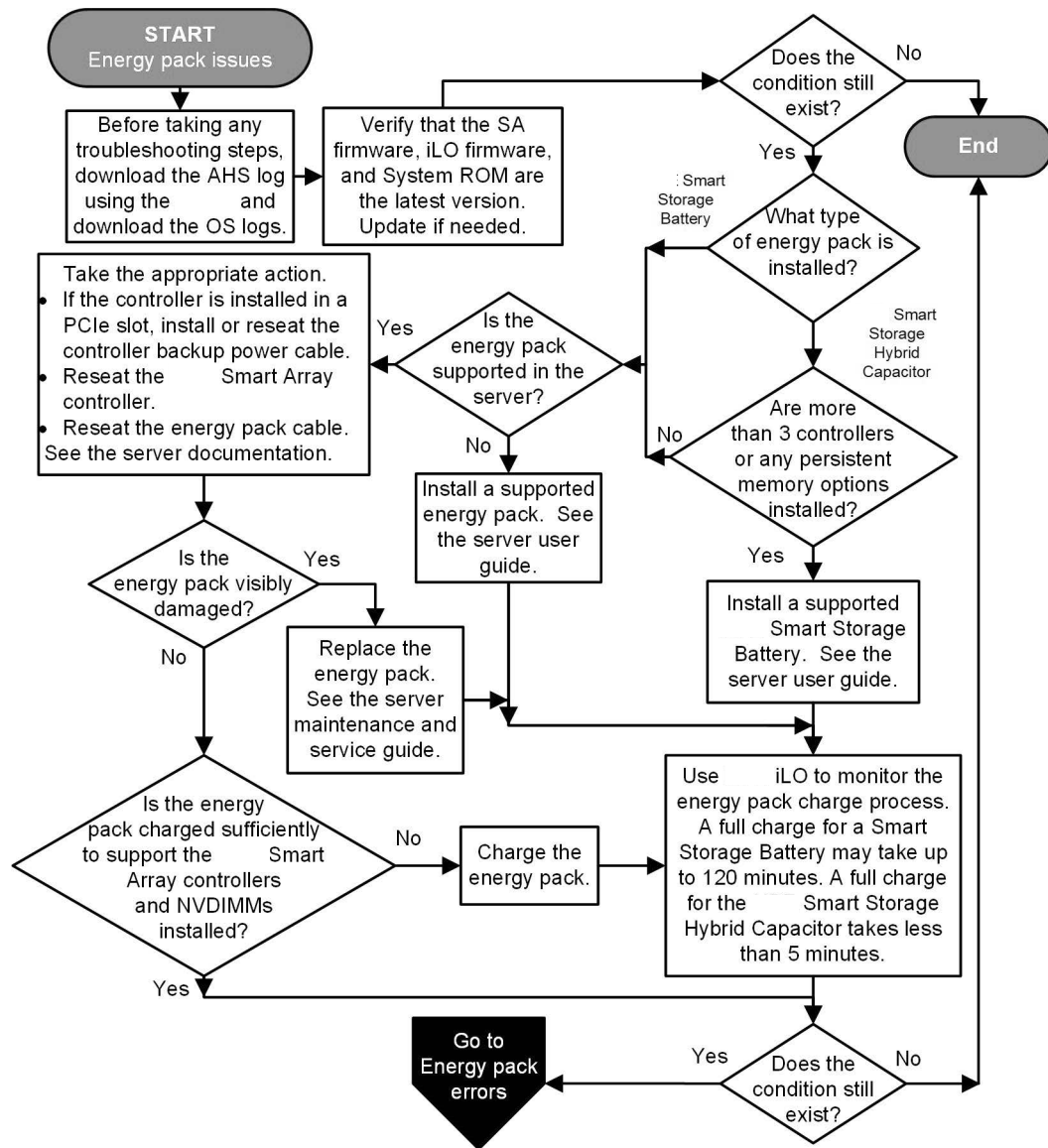


Figure 13: Energy pack issues flowchart

For installation procedures, see the user guide for your server.

For removal and replacement procedures, see the user guide for your server.

2. If the energy pack issues did not resolve the issue, follow the steps in the following flowchart.

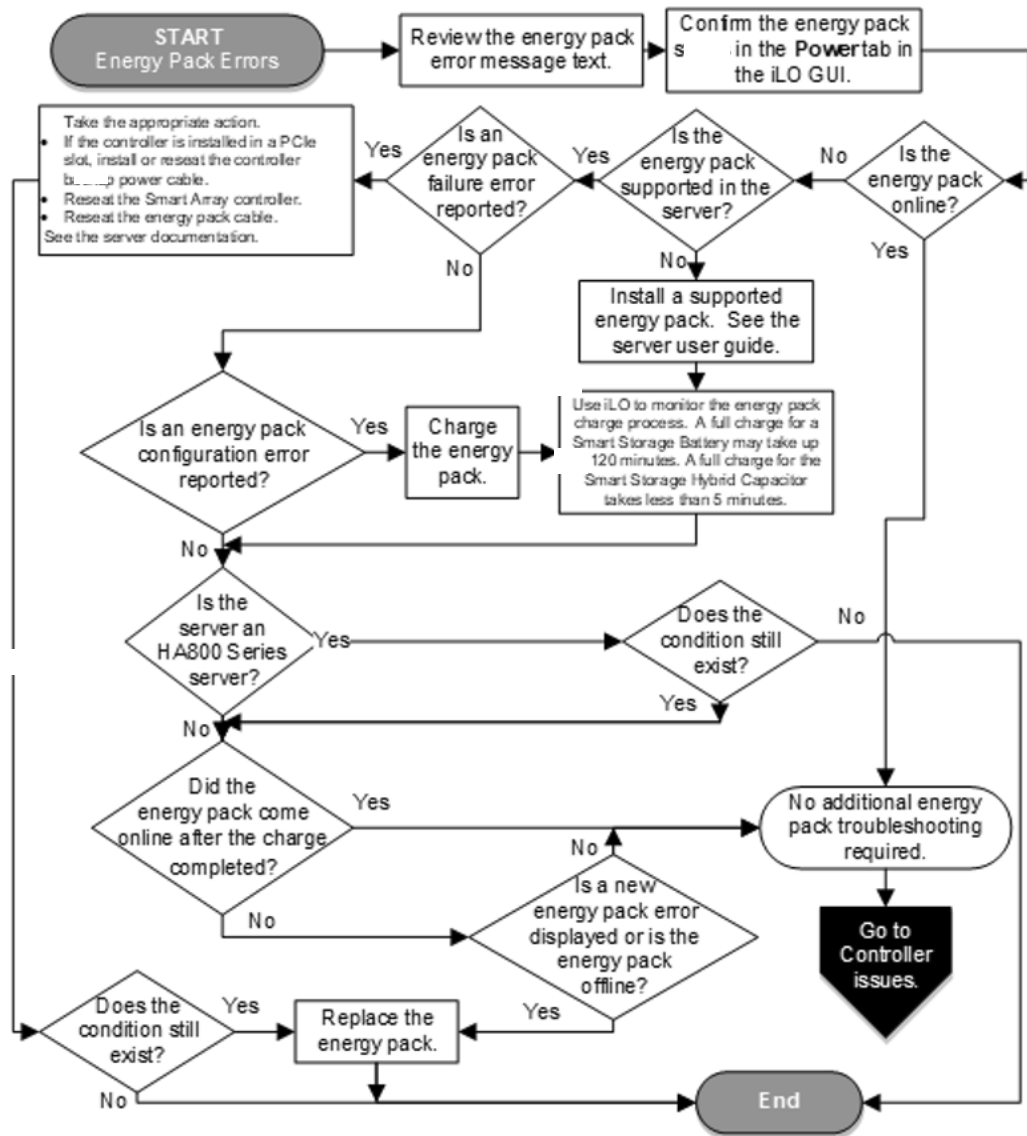


Figure 14: Energy pack errors flowchart

For removal and replacement procedures, see the user guide for your server.

For more information about iLO, see the iLO 5 User Guide on the [Hitachi Vantara website](#)

More information

[Energy pack issues](#)

[Gather important information before you begin](#)

[Smart Array controller documentation](#)

[Controller and energy pack cables](#)

[Controller issues flowchart](#)

Physical drive issues flowchart

Symptom

- A drive is not available.
- Drive errors are displayed in the logs during POST.

Cause

- The drive is faulty.
- The firmware is outdated.
- The drive does not match other drives in the same configuration.
- The controller is not cabled properly.

ⓘ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

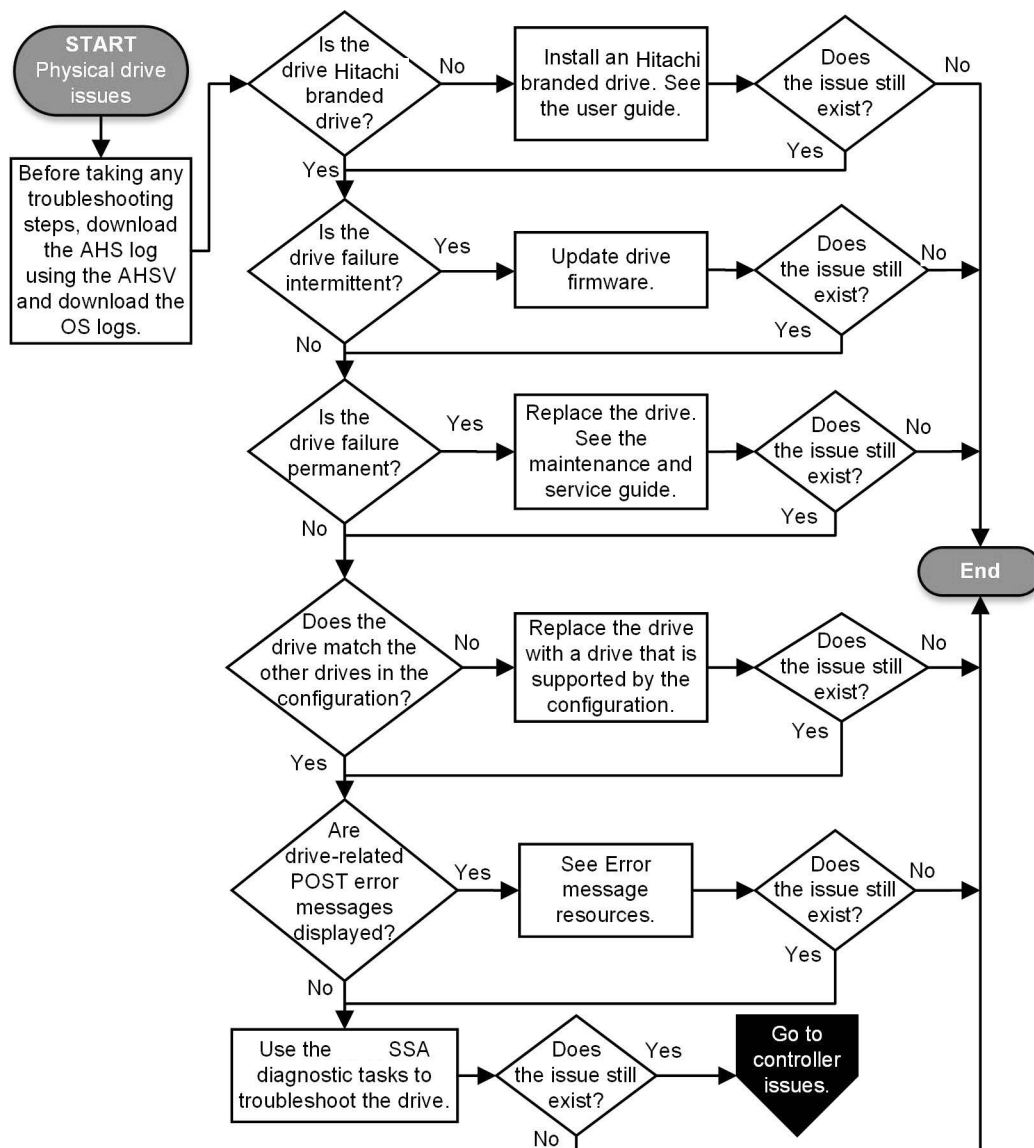


Figure 15: Physical drive issues flowchart

For removal and replacement procedures, see the user guide for your server

For installation procedures, see the user guide for your server.

For more information about error messages, see the error message guide on the [Hitachi Vantara website](#)

More information

[Smart Storage Administrator Diagnostics Utility CLIUpdating](#)

[firmware or system ROM](#)

[Gather important information before you begin](#)

[Controller issues flowchart](#)

Logical drive issues flowchart

Symptom

- Logical drive errors are displayed during POST or in one of the logs.
- The logical drives associated with an array controller are not visible during POST.

Cause

- The drives or cables are not seated properly.
- The associated physical drives are not available.
- Logical drives are configured.

❗ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

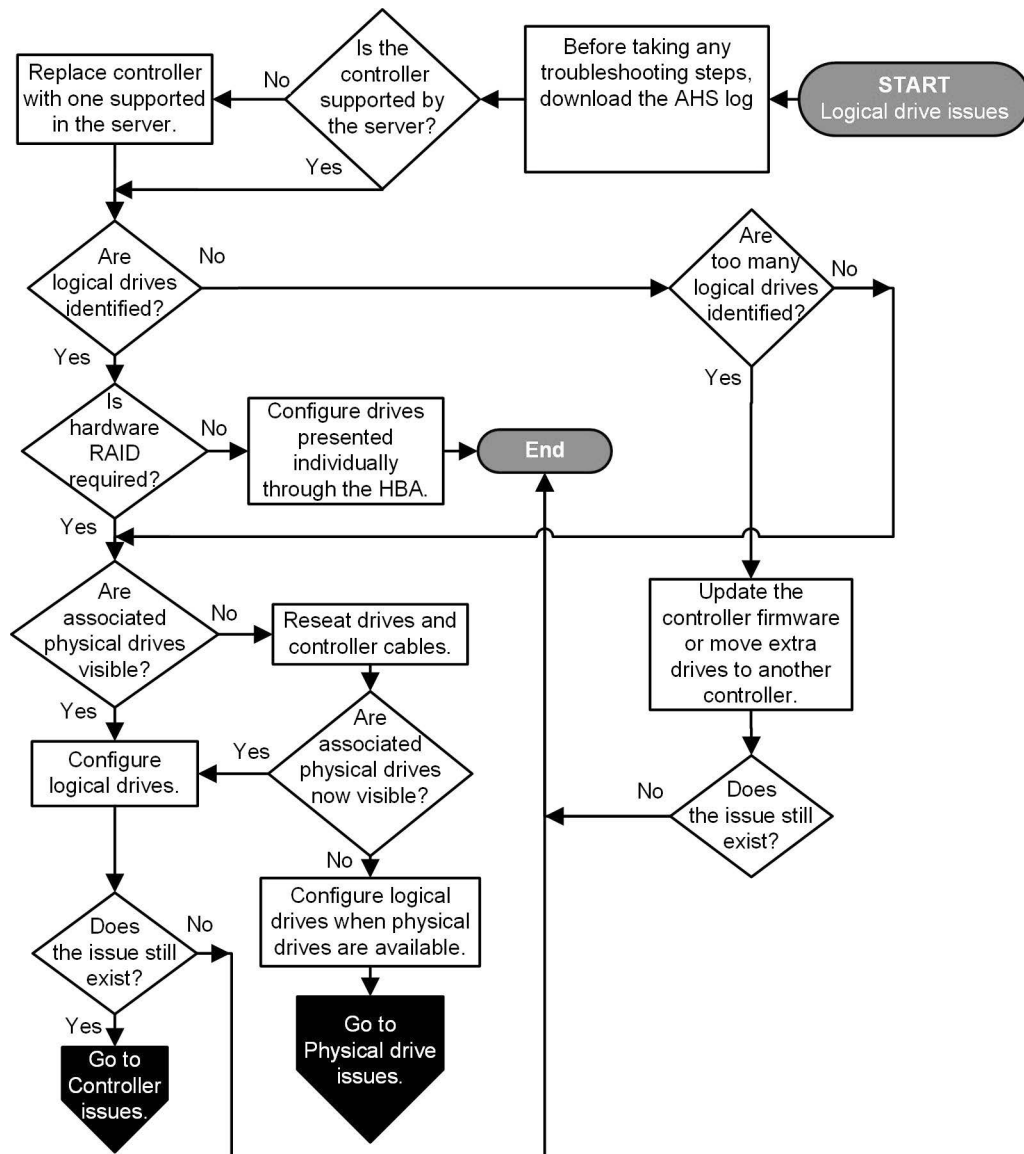


Figure 16: Logical drive issues

For removal and replacement procedures, see the user guide for your server.

For more information about UEFI System Utilities, see the UEFI System Utilities documentation on the

[Hitachi Vantara website](#)

More information

[Physical drive issues flowchart](#)

[Controller issues flowchart](#)

Fault indications flowchart

Server fault indications flowchart for non-blade servers

Symptom

- The server boots, but the system health LED or component health LED is red or amber.

Cause

- Improperly seated or faulty internal or external component
- Unsupported component installed
- Redundancy failure
- System over temperature condition

❗ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

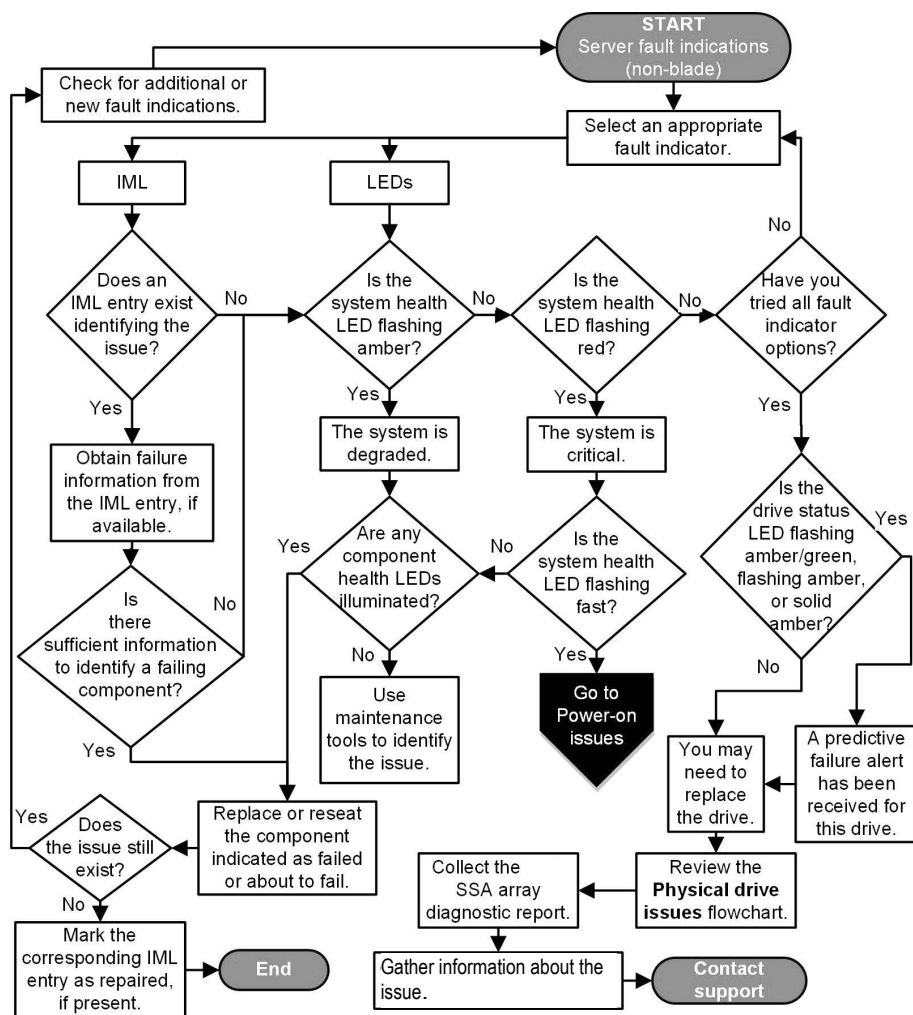


Figure 17: Server fault indications flowchart for non-blade servers

For the location of server LEDs and information on their statuses, see the user guide for your server.

For removal and replacement procedures, see the user guide for your server.

More information

[Power-on issues flowchart](#)

[Smart Storage Administrator Diagnostics Utility CLI Software
and configuration utilities](#)

[Gather important information before you begin](#)

[Physical drive issues flowchart](#)

More information

[Drive issues \(hard drives and solid state drives\)](#)

[Physical drive issues flowchart](#)

NIC issues flowchart

Symptom

- The NIC is not working.
- One or more ports on the NIC is not working.

Cause

- The firmware or drivers are outdated, mismatched, or faulty.
- The NIC or cable is not seated properly.
- The NIC, the cable, or other hardware is faulty.
- The hardware components are not supported in the same configuration.
- The NIC is not supported on the server.

❗ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

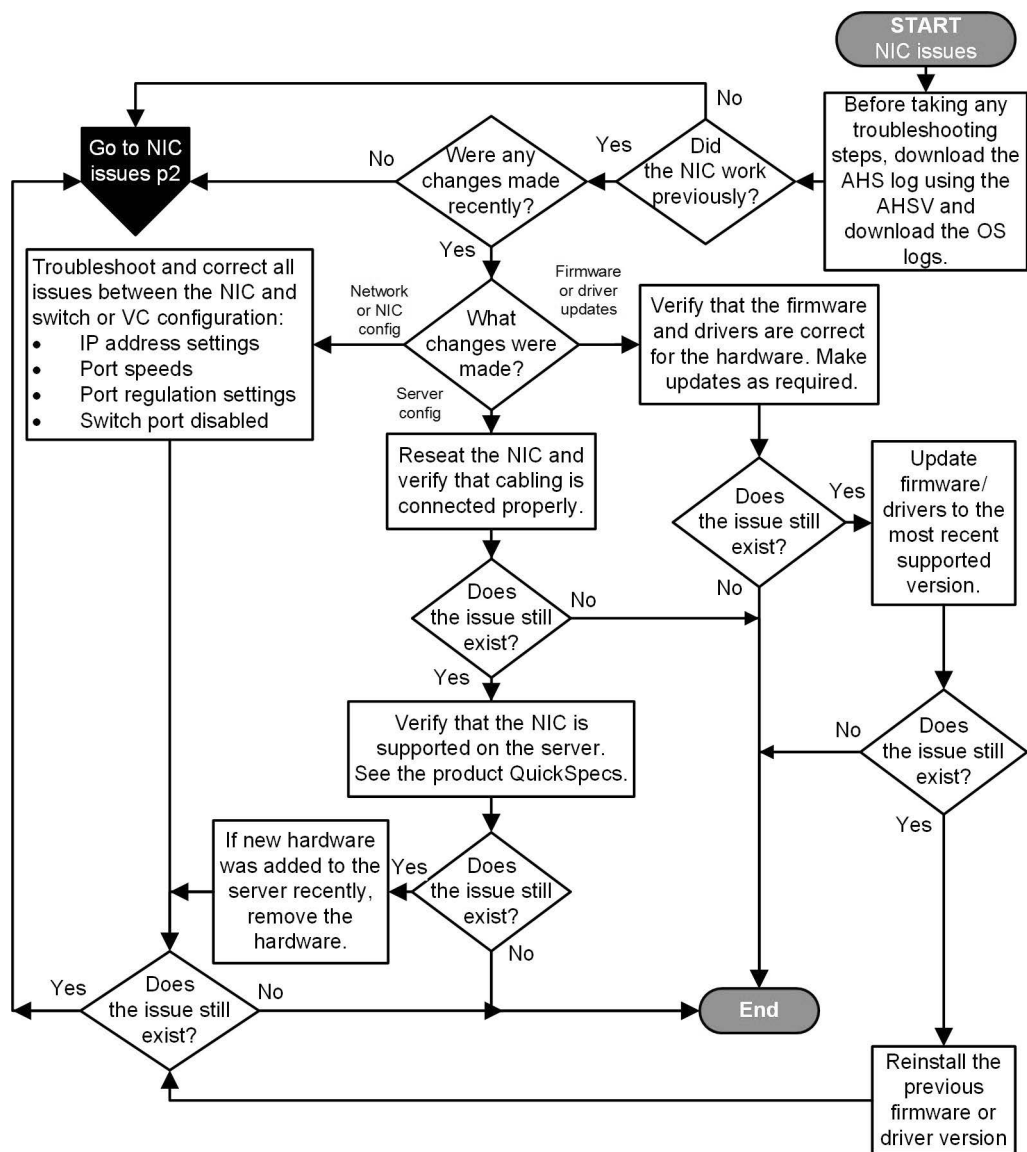


Figure 19: NIC issues flowchart (1 of 2)

General diagnosis flowchart

Symptom

If your symptoms are not clear, use this flowchart. However, before you begin, gather important information for use during troubleshooting. For more information, see [Gather important information before you begin](#).

The General diagnosis flowchart provides a generic approach to troubleshooting. If you are unsure of the issue, or if the other flowcharts do not fix the issue, use the following flowchart.

Cause

The cause is unknown or unclear.

❗ **IMPORTANT:** Before you make changes to your system, always download the Active Health System log.

Action

To resolve the issue, follow the steps in the flowchart.

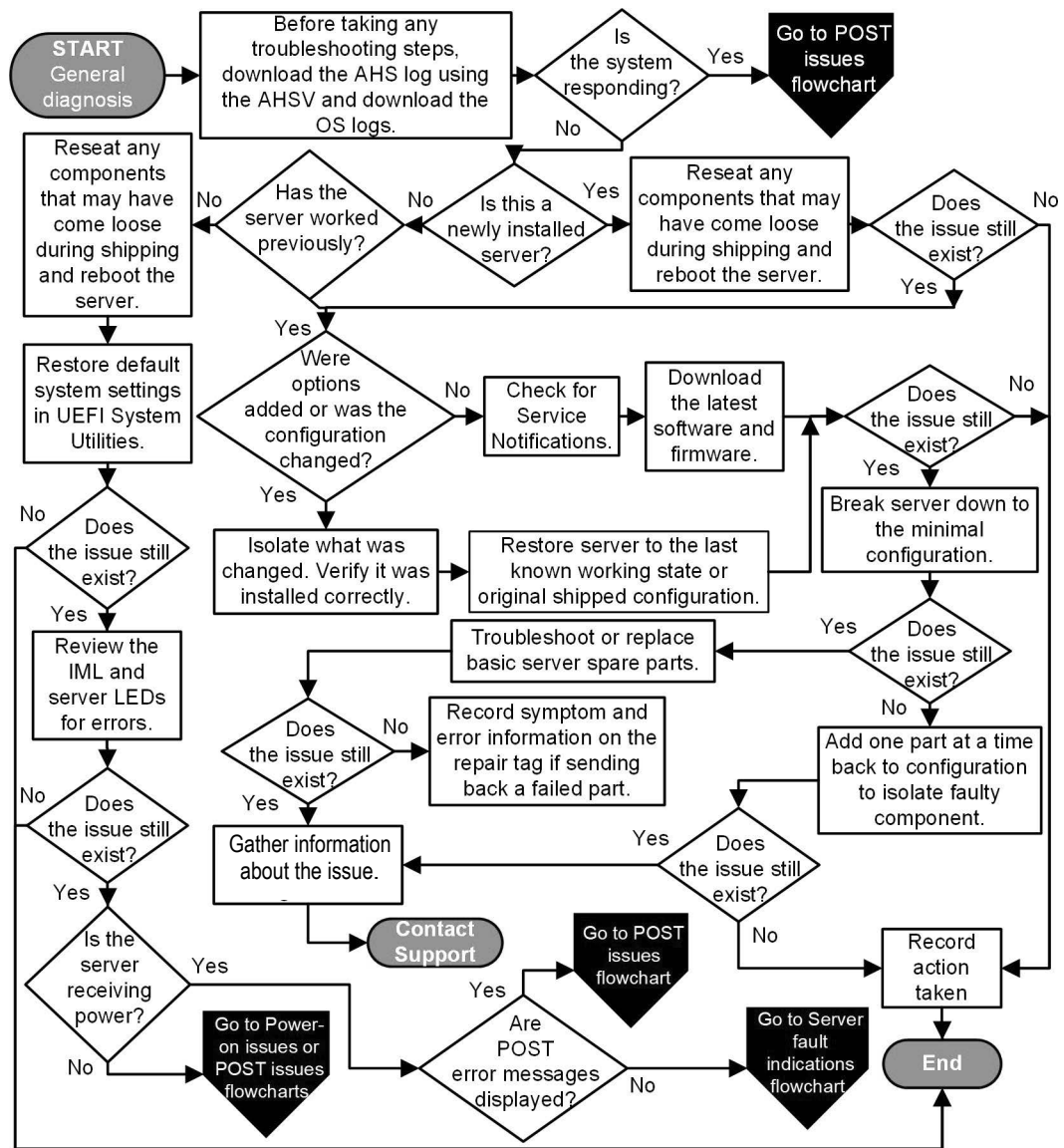


Figure 21: General diagnosis flowchart

For more information about error messages, see the error message guide on the [Hitachi Vantara website](#)

For removal and replacement procedures, see the user guide for your server

For more information about UEFI System Utilities, see the UEFI System Utilities documentation on the [Hitachi Vantara website](#).

More information

[Power-on issues flowchart](#)

[Resolving loose connections](#)

[Searching for service notifications](#)

[Breaking down the server to the minimum hardware configuration](#)

[Symptom information checklist](#)

[Fault indications flowchart](#)

[POST issues flowchart](#)

Hardware issues

Procedures for all Advanced Server products

The procedures in this section are comprehensive and include steps about or references to hardware features that might not be supported by the server you are troubleshooting.

⚠ CAUTION: Before removing or replacing any processors, be sure to follow the guidelines provided in [Processor troubleshooting guidelines](#). Failure to follow the recommended guidelines can cause damage to the system board, requiring replacement of the system board.

Power issues

Server does not power on

Symptom

The server does not power on.

Action

1. Review the Server Health Summary.
2. See the Power-on issues flowchart.

More information

[Power-on issues flowchart](#)

[Using the Server Health Summary](#)

Power source issues

Symptom

The server does not power on.

Cause

- The server is not powered on.
- Components or cables might not be properly connected or seated.
- The grounded power outlet is not working.
- The power cord is not functional.
- The power strip is not functional.
- The circuit breaker is in the Off position.
- The line voltage is insufficient for the load.
- Sufficient power is not allocated to support the server.

Action

1. Press the Power On/Standby button to be sure it is on.
If the server has a Power On/Standby button that returns to its original position after being pressed, be sure that you press the switch firmly.
2. Be sure that no loose connections exist.
3. Verify that the power LEDs on the power supplies are illuminated.
4. Plug another device into the grounded power outlet to be sure the outlet works.
Be sure that the power source meets applicable standards.
5. Replace the power cord with a known functional power cord to be sure it is not faulty.
6. Replace the power strip with a known functional power strip to be sure it is not faulty.
7. Be sure that the proper circuit breaker is in the On position.
8. Have a qualified electrician verify the line voltage to be sure it meets the required specifications.
9. If Enclosure Dynamic Power Capping or Enclosure Power Limit is enabled on supported servers, be sure to support the server.
For more information, see the following documents:

More information

[System power LED definitions](#)
[Resolving loose connections](#)

Power supply issues

Symptom

The power supply is not functioning or not working properly.

Cause

- The power supply might not be fully seated.
- AC power is unavailable.
- The power supply failed.
- The power supply is in standby mode.
- The power supply has exceeded the current limit.
- The power supply is not supported on the server.
- The power is not sufficient for the hardware installed.
- Redundant power supplies are configured but the power supplies are not compatible.

Action

1. Be sure that no loose connections exist.
2. If the power supplies have LEDs, be sure that they indicate that each power supply is working properly:
 - a. If the LEDs indicate an issue with a power supply (red, amber, or off), then inspect the power source.
 - b. If the power source is working properly, then replace the power supply.

For more information, see the server maintenance and service guide.
3. Verify that the system has enough power, particularly if you recently added hardware, such as drives.
 - a. Remove the newly added component and if the issue is no longer present, then additional power supplies are required.

For product-specific information, see the user guide for your server.

For more information, contact customer support.

If running a redundant configuration, be sure that all the power supplies have the same spare part number and are supported by the server.

4. For further troubleshooting, see the Power-on issues flowchart.

More information

[Power-on issues flowchart](#)

[Resolving loose connections](#)

[Server maintenance and service guide](#)

Insufficient power supply configuration

Symptom

The power supply configuration for the server is insufficient to meet the power requirements for the server.

Cause

The current power supply configuration is not sufficient to operate the server.

Action

1. Verify that the power supplies support the power requirements for the server configuration.

For more information, contact customer support.

Verify that all power supplies are supported for this server.
2. If the power supplies have LEDs, review the LED statuses to see if they indicate an issue:

- a. If the LEDs display red, replace the power supply.
 - b. If the LEDs display amber, then the power supply is in standby mode.
Press and hold the Power On/Standby button on the server.
 - c. If the LEDs are off, inspect the power source. Then, power on the server again.
 - d. If the power source is working properly, and the LEDs remain off, replace the power supply.
For more information, see the server maintenance and service guide.
3. Verify that the system has enough power, particularly if you recently added hardware, such as drives.
 - a. To verify that the system has enough power, remove the newly added component.
 - b. If the issue is no longer present, then additional power supplies are required.
For more information, see the server documentation.

More information

Server maintenance and service guide
[Server documentation](#)

UPS issues

UPS is not working properly

Symptom

The UPS is not working properly.

Cause

- The UPS switch is not in the ON position.
- The UPS batteries are not charged to the proper level.
- The UPS software is not up-to-date.
- The UPS power cord is not connected.
- The UPS power cord is not the correct type for the UPS and the country/region in which the server is located.

Action

1. Be sure that the UPS batteries are charged to the proper level for operation.
For more information, see the UPS documentation.
2. Be sure that the UPS power switch is in the ON position.
For the location of the switch, see the UPS documentation.
3. Be sure that the UPS software is updated to the latest version.

Use the Power Management software on the [Hitachi Vantara website](#)

Be sure that the power cord is the correct type for the UPS and the country/region in which the server is located. For specifications, see the UPS reference guide.

4. Be sure that the line cord is connected.
5. Be sure that each circuit breaker is in the ON position, or replace the fuse if needed.
If this occurs repeatedly, contact an authorized service provider.
6. Review the UPS LEDs to be sure that a battery or site wiring issue has not occurred.
For more information, see the UPS documentation.
7. If the UPS sleep mode is initiated, disable sleep mode for proper operation.
The UPS sleep mode can be turned off through the configuration mode on the front panel.
8. Change the battery to be sure that damage was not caused by excessive heat, particularly if a recent air conditioning outage has occurred.

NOTE: The optimal operating temperature for UPS batteries is 25°C (77°F). For approximately every 8°C to 10°C (16°F to 18°F) average increase in ambient temperature above the optimal temperature, battery life is reduced by 50 percent.

Low battery warning is displayed

Symptom

A low battery warning is displayed on the UPS.

Cause

- The batteries must be charged.
- The batteries are failing to hold a charge.
- The batteries are faulty.

Action

1. Plug the UPS into an AC grounded outlet for at least 24 hours to charge the batteries.
2. Test the batteries.
3. Replace the batteries if necessary.
4. Be sure that the alarm is set appropriately by changing the amount of time given before a low battery warning.
For more information, see the UPS documentation.

One or more LEDs on the UPS is red

Symptom

One or more of the UPS LEDs is red.

Action

For product-specific LED information and additional troubleshooting information, see the UPS documentation.

General hardware issues

New hardware issues

Symptom

The hardware is not functioning normally.

Cause

- Unsupported hardware
- Incomplete population of a memory bank
- Connection of the data cable, but not the power cable, of a new device

Action

1. Be sure the hardware being installed is a supported option on the server. If necessary, remove unsupported hardware.
2. Be sure that the issue is not caused by a change to the hardware release.
For more information, see the release notes included with the hardware. If no documentation is available, see the [Hitachi Vantara website](#)
Be sure that the new hardware is installed properly.
To be sure that all requirements are met, see the device, server, and OS documentation.
3. Be sure no memory, I/O, or interrupt conflicts exist.
4. Be sure that no loose connections exist.
5. Be sure that all cables are connected to the correct locations and are of the correct lengths.
For more information, see the server user guide.
6. Be sure that other components were not accidentally unseated during the installation of the new hardware component.
7. Be sure all necessary software updates, such as device drivers, ROM updates, and patches, are installed and current.
Be sure that the correct version for the hardware is installed.
For example, if you are using a smart array controller, you need the latest smart array Controller device driver. Uninstall any incorrect drivers before installing the correct drivers.
8. After installing or replacing boards or other options, verify that the system recognizes all changes to the hardware in UEFI System Utilities.
If the new hardware is not configured properly, you might receive a POST error message indicating a configuration error.

For more information, see [Hitachi Vantara website](#)

9. Be sure that all switch settings are set correctly.

For more information, see the server user guide.

10. Be sure that all boards are properly installed in the server.
11. Uninstall the new hardware.

More information

[Resolving loose connections](#)

[Server user guide](#)

Unknown issue

Symptom

The server is not functioning properly, but the specific cause is unknown.

Action

1. To see if any statuses indicate the source of the issue, check the server LEDs.
2. Power down and disconnect power to the server. Remove all power sources to the server.
3. Be sure that no loose connections exist.
4. Following the guidelines and cautionary information in the server documentation, reduce the server to the minimum hardware configuration. Remove all cards or devices that are not necessary to power on the server.

Before completing this step, review the guidelines for breaking down the server to the minimum hardware configuration. Keep the monitor connected to view the server power-on process.

5. Reconnect power, and then power on the system.



CAUTION: Only authorized technicians trained by Hitachi Vantara should attempt to remove the system board. If you believe the system board requires replacement, contact Hitachi Vantara technical support before proceeding. For more information, see [Accessing Hitachi Vantara Support](#).



CAUTION: Before removing or replacing any processors, be sure to follow the guidelines in "Processor troubleshooting guidelines" in the troubleshooting guide for your product. Failure to follow the recommended guidelines can cause damage to the system board, requiring replacement of the system board.

- If the system fails in this minimum configuration, one of the primary components has failed. If you have already verified that the processor, power supply, and memory are working before getting to this point, replace the system board. If not, be sure each of those components is working.
- If the system boots and video is working, add each component back to the server one at a time. To determine if that component is the cause of the issue, restart the server after adding each component. When adding each component back to the server, be sure to disconnect power to the server and follow the guidelines and cautionary information in the server documentation.

More information

[Resolving loose connections](#)

[Breaking down the server to the minimum hardware configuration](#)

[Server documentation](#)

[Processor troubleshooting guidelines](#)

Third-party device issues

Symptom

- A third-party device is not recognized by the server or the OS.
- A third-party device is not operating as expected.

Cause

- The device is not supported on the server or OS.
- The device is not installed properly.

Action

1. Verify that the server and operating system support the device.
For more information, see the operating system documentation.
2. Verify that the latest device drivers are installed.
3. Verify that the device is installed properly.

Testing the device

Procedure

1. Uninstall the device.
If the server works when the device is removed, then one of the following issues exists:
 - An issue exists with the device.
 - The server does not support the device.
 - The device conflicts with another device.
2. If there is only one device on a bus, verify that the bus works by installing a different device on the bus.
3. To determine if the device is working, install the device:
 - a. In a PCIe slot on a different bus.
 - b. In the same slot in another working server of the same or similar design.

Restart the server each time the device is reinstalled.

If the board works in any of these slots, either the original slot is bad or the board was not properly seated. Reinstall the board into the original slot to verify.

4. If you are testing a board (or a device that connects to a board):
 - a. Test the board with all other boards removed.
 - b. Test the server with only that board removed.
5. Clear the NVRAM.
6. Verify that the PCIe device or graphics controller does not need additional power to operate.
For more information, see the device documentation.

Drive issues (hard drives and solid state drives)

Drives are failed

Symptom

The drives are failed.

Action

1. Be sure no loose connections exist.
2. Check to see if an update is available for any of the following:
 - Smart array Controller firmware
 - Dynamic smart array driver
 - Host bus adapter firmware
 - Expander backplane SEP firmware
 - System ROM
3. Be sure the drive or backplane is cabled properly.
4. Be sure the drive data cable is working by replacing it with a known functional cable.
5. Be sure drive blanks are installed properly when the server is operating.
Drives may overheat and cause sluggish response or drive failure.
6. Run SSA and check the status of the failed drive.
7. Be sure the replacement drives within an array are the same size or larger.
8. Be sure the replacement drives within an array are the same drive type, such as SAS, SATA, or SSD.
9. Power cycle the server.
If the drive appears, verify the drive firmware and update, if needed.

More information

[Smart Storage Administrator](#)

[Resolving loose connections](#)

Drives are not recognized

Symptom

Drives are not recognized.

Action

1. Be sure that no power issues exist.
 2. Be sure that no loose connections exist.
 3. Check for available updates on any of the following components:
 - Smart array Controller firmware
 - Smart array S100i SR G2 driver
 - HBA firmware
 - Expander backplane SEP firmware
 - System ROM
 4. Be sure that the drive or backplane is cabled properly.
 5. Review the drive LED statuses to ensure that they indicate normal function.
For server-specific drive LED information, see server documentation.
 6. Be sure that the drive is supported.
 7. Power cycle the server.
If the drive appears, verify the drive firmware and update, if needed.
 8. Be sure that the drive bay is not defective by installing the hard drive in another bay.
 9. When the drive is a replacement drive on an array controller, be sure that the drive is the same type and of the same or larger capacity than the original drive.
 10. When using an array controller, be sure that the drive is configured in an array. Run SSA.
 11. Be sure that the correct controller drivers are installed and that the controller supports the hard drives being installed.
 12. If a storage enclosure is used, be sure that the storage enclosure is powered on.
 13. If a SAS switch is used, be sure that disks are zoned to the server using the Virtual SAS Manager.
-
- **IMPORTANT:** The smart array S100i SR G2 and the AHCI do not support SAS drives.
-
14. If the smart array S100i SR G2 is installed on the server, be sure that RAID mode is enabled and UEFI boot mode is enabled in UEFI System Utilities.

More Information

[Smart storage administrator](#)

[UEFI System Utilities](#)

[Resolving loose connections](#)

[Hot-plug drive LED definitions](#)

[Server documentation](#)

Data is inaccessible

Symptom

The data on the drives is inaccessible.

Cause

- The files are corrupt.
- Viruses exist on the server.
- A TPM is installed but not properly enabled on the server.

Action

1. Be sure the files are not corrupt. Run the repair utility for the operating system.
2. Be sure no viruses exist on the server. Run a current version of a virus scan utility.
3. When a TPM is installed and is being used with BitLocker, be sure the TPM is enabled in UEFI System Utilities. See the TPM replacement recovery procedure in the operating system documentation.
4. When a TPM is installed, be sure that the TPM is configured for a mode that is compatible with the OS running on the server. Verify that the OS supports the version of TPM installed and configured on the server.
5. When a TPM 2.0 is installed, verify that the server is configured for UEFI boot mode.
6. When migrating encrypted data to a new server, be sure to follow the recovery procedures in the operating system documentation.

More information

[UEFI System Utilities](#)

Server response time is slower than usual

Symptom

The server response time is slower than usual.

Cause

- The drive is full.
- Operating system encryption technology is causing a decrease in performance.
- A recovery operation is pending on the logical drive.

Action

1. Be sure the drive is not full. If needed, increase the amount of free space on the drive. Hitachi Vantara recommends that drives have a minimum of 15 percent free space.
2. Review information about the operating system encryption technology, which can cause a decrease in server performance. For more information, see the operating system documentation.
3. Use SSA to verify that a recovery operation is not pending on the logical drive.

More information

[Smart storage administrator](#)

SmartDrive icons or LEDs illuminate errors for the wrong drive or an error message is displayed in POST, SSA, or SSADUCLI

Symptom

- SmartDrive icons or LEDs illuminate indicating an error.
- An error message is displayed in POST, SSA, or SADUCLI.

Action

Verify that the cabling from the drive backplane to the system board is correct.
For server-specific cabling information, see the server user guide.

More information

[Server user guide](#)

SSD Smart Wear error

Symptom

A POST message is received.

Cause

The device is approaching the maximum usage limit for writes to the device.

Action

Replace the device.
For more information, see the server maintenance and service guide.

More information

[Server maintenance and service guide](#)

Diagnosing array problems

Diagnostic tools for smart array SR and MR G2 controllers

To troubleshoot array problems and generate feedback about arrays, use the diagnostic tools described in this section.

Diagnostic tools for smart array SR G2 controllers

- **Smart Storage Administrator (SSA)**

SSA can be accessed offline using Intelligent Provisioning or booting from the SPV ISO image. It can also be accessed online by downloading the SSA executables. For more information on accessing and using SSA, see the Smart array SR Controllers Configuration Guide at the [Hitachi Vantara website](#).

- **System Event Log**

Smart Array SR Event Notification Service for Windows reports array events to the Microsoft Windows system event log, and records the Smart Array serial log, which includes detailed diagnostic information of the most recent events encountered by the controller. The HA800 Agentless Management Service reports events to the Linux event log. You can obtain the utility from the [Hitachi Vantara website](#). When prompted for product information, enter the server model name.

- **iLO**

The iLO firmware continuously monitors smart array independent of the operating system and logs any failure events to the iLO web interface, iLO RESTful API, and SNMP.

- **Diagnostic tools for smart array MR G2 controllers**

- **MR Storage Administrator**

MR Storage Administrator displays event log messages and system messages. To view the event log, in the controller dashboard click **View Event Log** under the Actions menu. In the Actions menu for the event log, you can download the log file and clear the log file. To view the system messages, click the bell icon, and the messages appear on the top of the window.

- **System Event Log**

MR Storage Administrator reports array events to the application area inside of the Microsoft Windows system event log, which includes detailed diagnostic information of the most recent events encountered by the controller. On Linux, the system event log is located at `/var/log/messages`. On VMware, the system event log is located at `/var/log/vmkernel.log`.

Storage controller issues

General controller issues

Symptom

- The controller is not visible during the POST process.
- The controller shows errors during the POST process.

Cause

- The hardware is physically damaged.
- The controller is not supported on the server.
- The controller is not seated properly.
- The controller is faulty.
- The firmware is outdated.

Action

1. Verify that the controller is supported for the server.
2. Verify that the controller is not physically damaged.
3. If the controller is recognized by the system BIOS, then reseal the controller.
4. Run controller diagnostics and follow the steps displayed.
5. Update the firmware.
6. Download the Active Health System log.
7. If the issue persists, contact customer support.
8. Replace the controller.

For more information, see the server maintenance and service guide.

More information

Server maintenance and service guide

Controllers are no longer redundant

Symptom

- The controller shows errors during the POST process.
- The cache is disabled.

Cause

- The hardware on one or more controllers is physically damaged.
- One or more controllers are not supported on the server.
- The controllers are not compatible for redundant operation.

- One or more controllers are not installed properly.
- The firmware on one or more controllers is outdated or not compatible.
- The energy pack is not installed.
- The energy pack is not connected to the system board properly.
- The controller backup power cable is not connected from the controller to the PCIe riser board.

Action

1. Verify that the controllers are supported for the server.
2. Verify that both controllers are installed or seated properly.
3. Verify that the controllers are compatible controller models.
4. Verify that the controller firmware versions are compatible and current.
5. Verify that the controller cache sizes are compatible.
6. Verify that the energy pack is installed and connected properly.
7. Verify that all controller cabling is connected properly.
8. If the issue persists, download the Active Health System log.
9. Contact Hitachi Vantara technical support.

More information

[Active Health System Log](#)

Data located on drives accessed in RAID mode is not compatible with data accessed from non-RAID mode

Symptom

Data located on drives accessed in RAID mode is not compatible with data accessed from non-RAID mode and data located on drives accessed in non-RAID mode is not compatible with data accessed from RAID mode.

Action

Hitachi Vantara recommends that you access drive data only when the same RAID or non-RAID mode is enabled. Back up and restore the data on the drives.

The smart array controller does not show logical drives after moving drives to a newserver or JBOD

Symptom

The smart array controller does not show logical drives after moving drives to a new server or JBOD.

Cause

A drive migration issue occurred.

Action

Be sure to follow all drive roaming rules when migrating drives.

More information

Drive roaming

Drive roaming

Drive roaming lets you move disk drives and arrays while maintaining data availability. You can move one or more disk drives in a configured logical drive to a different bay position as long as the new bay position is accessible by the same controller. In addition, you can move a complete array from one controller to another, even if controllers are in different servers. The logical drive status must be good before you move physical drives to a new bay position.

Drive roaming is an offline feature. There is no method for removing an array while the server is online and then moving it to a new physical location.

Data failure or disk errors on a server with a 10 SFF drive backplane or a 12 LFF drive backplane

Symptom

Data failure or disk errors occur on a server with a 10 SFF or 12 LFF drive backplane.

Cause

The drive backplane is not cabled properly to the controller.

Action

Be sure that the drive backplane ports are connected to only one controller.

Only one cable is required to connect the backplane to the controller. The second port on the backplane is cabled to the controller to provide additional bandwidth.

More information

Smart array S100i SR G2 drives are not found when RAID mode is disabled

Symptom

The S100i SR G2 drives are not found when RAID mode is disabled.

Cause

When a smart array S100i SR G2 is enabled on a server and RAID mode is disabled in the UEFI System Utilities, then the drives are listed as AHCI drives and the RAID controller is not found in POST or device manager. When RAID mode is enabled, the drives appear as smart array S100i SR G2 drives.

Action

1. Reboot the server.
2. Access UEFI System Utilities by pressing **F9 (System Utilities)** during POST.

3. Select **System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > Embedded SATA Configuration > Smart array SW RAID Support** and press the Enter key.
4. In the SATA Controller Options screen, for the Embedded SATA configuration option, select **Smart array SW RAIDSupport** from the drop-down menu and click **OK**.
If you see the warning **Important: Smart array SW RAID is not supported when the Boot Mode is configured in Legacy BIOS Mode**, click **OK**.
5. Press **F12: Save and Exit**.
6. To save changes, click **Yes-Save Changes**.
7. Click **Reboot**.

Smart array S100i SR G2 drives are not recognized

Symptom

When installing an OS, the OS installation does not recognize the smart array S100i SR drives.

Action

Manually install the smart array S100i SR G2 drivers.
For more information, see the controller documentation.

Fan and thermal issues

General fan issues

Symptom

Fan not operating as expected.

Cause

- The fans are not seated properly.
- The fan configuration does not meet the functional requirements of the server.
- The server is not ventilated properly.
- One or more required fans are not installed.
- Required fan blanks are not installed.
- Error messages are displayed during POST.
- One or more fans are not functioning.

Action

1. Be sure that the fans are properly seated and working:

- a. Follow the procedures and warnings in the server documentation for accessing and replacing fans.
 - b. Unseat, and then reseat, each fan according to the proper procedures.
 - c. Replace the access panels, and then attempt to restart the server.
2. Be sure that the fan configuration meets the functional requirements of the server.
3. Be sure that no ventilation issues exist. If the server is operated for an extended period with the access panel removed, airflow might be impeded, causing thermal damage to components.
4. Be sure that no POST error messages are displayed while booting the server that indicate temperature violation or fan failure information.
5. Use iLO to see if any event list error messages relating to fans are listed.
6. In the iLO web interface, click **Power & Thermal** in the navigation tree:
 - a. Click the **Fans** tab, and verify the fan status and fan speed.
7. Click the **Temperatures** tab, and verify the temperature readings for each location on the Temperatures tab. If a hot spot is located, then check the airflow path for blockage by cables and other material.
8. A hot spot is not an absolute temperature but is relative to a component specification. Hot spot is defined as temperature on a sensor within 3°C of a Caution threshold listed on the Temperature tab.
9. Replace any required nonfunctioning fans and restart the server. For more information, see the server maintenance and service guide.
10. Be sure that all fan slots have fans or blanks installed.
11. Verify that the fan airflow path is not blocked by cables or other material.

More information

Server maintenance and service guide

[Troubleshooting resources](#)

Fans running at a higher than expected speed

Symptom

The fans are running at a higher speed than expected.

Cause

- The system temperature sensor is reading within approximately 10°C of the Caution threshold.
- An air baffle or blank is missing or not installed properly and causing a disruption of the airflow.
- The processor heatsink is not installed as indicated in the server documentation.
- A supported fan is not installed in the server.

Action

1. Update the server to the latest firmware versions, such as iLO firmware, system BIOS, option firmware, and so on.
2. Verify the Temperature tab. Fan speeds can be high if a sensor temperature is within approximately 10°C of the Caution threshold.
3. Verify that all air baffles and required blanks, such as drive blanks, processor heatsink blanks, power supply blanks, and so on, are installed.
4. Verify that the correct processor heatsink is installed.
5. Verify that the correct fan is installed, if the system supports both standard fans and performance fans.

More information

[Updating firmware or system ROM](#)
[Server documentation](#)

Excessive fan noise (high speeds)

Symptom

Fans are operating at high speeds with excessive noise.

Cause

Fans can generate noise if running at a high speed (as expected) or when at low speed if there is an issue with the fan.

Action

1. In the iLO web interface, click **Power & Thermal** in the navigation tree.
2. Click the **Fans** tab.
3. Verify the fan status and fan speed.
Fan speeds greater than 60% are expected to be loud.
4. If the fan is running at a higher speed than expected, see "Fans running at a higher than expected speed."

More information

[Server documentation](#)
[Fans running at a higher than expected speed](#)

Excessive fan noise (low speeds)

Symptom

Abnormal/rattling noise observed at low fan speeds.

Action

Replace the fan.
For more information, see the server maintenance and service guide.

More information

Hot-plug fan issues

Symptom

Hot-plug fans are not functioning properly.

Action

1. Check the LEDs to be sure the hot-plug fans are working.

For LED information, see the server documentation on the [Hitachi Vantara website](#)

NOTE: For servers with redundant fans, backup fans may spin up periodically to test functionality. This is part of normal redundant fan operation.

2. Verify that there are no POST error messages displayed.

If a POST error message is displayed, complete the steps required to resolve the error.

3. Verify that the hot-plug fan meets the requirements for the server.

For more information, see the server documentation on the [Hitachi Vantara website](#)

More information

Server documentation

Memory issues

General memory issues

Symptom

A DIMM error occurred or a DIMM failed.

Cause

- The memory does not meet server requirements.
- A DIMM has failed.
- Third-party memory is installed on the server.
- The DIMM is not properly seated.

Action

1. Be sure that the DIMMs meet the server requirements and is installed as required by the server.
Some servers might require that memory channels are populated fully or that all memory within a memory channel is of the same size, type, and speed.
2. Remove any third-party memory.
3. Check any server LEDs that correspond to memory slots.
4. Update the system ROM to the latest version.

5. Reseat the DIMM.
6. Isolate and minimize the memory configuration. Use care when handling DIMMs.
7. Replace the DIMM.

For more information, see the server maintenance and service guide.

More information

[Isolating and minimizing the memory configuration](#)

[Updating firmware or system ROM](#)

[DIMM handling guidelines](#)

Server user guide

Server maintenance and service guide

Isolating and minimizing the memory configuration

When troubleshooting memory issues, sometimes it is necessary to isolate DIMMs in a minimum configuration to determine which DIMM failed.

Prerequisites

Use care when handling DIMMs.

Procedure

1. If you are unsure which DIMM has failed, test each channel of DIMMs by removing all other DIMMs.
2. Isolate the failed DIMM by switching each DIMM in a channel with a known working DIMM.

More information

[DIMM handling guidelines](#)

Server is out of memory

Symptom

- The server is out of memory.
- A POST error message is displayed.

Cause

- The memory is not configured properly.
- An OS error is indicated.

Action

1. Be sure the memory is configured properly. For more information, see the product documentation to determine the memory configuration requirements.
2. Be sure no operating system errors are indicated.
3. Update the system ROM to the latest version.

More information

[Updating firmware or system ROM](#)

DIMM configuration errors

Symptom

A POST error message is displayed.

Cause

- The DIMM configuration does not support the Advanced Memory Protection setting configured for the server.
- The memory channel was not populated in the correct order.
- An unsupported DIMM is installed in the server.
- The corresponding processor is not installed.

Action

1. Verify that the DIMMs are installed according to the DIMM population guidelines.
2. Verify that the Advanced Memory Protection settings and DIMMs are installed according to the DIMM population guidelines.
3. Verify that the DIMMs are supported on the server.
4. Be sure that the associated processor is installed for all DIMMs on the server.
5. Update the system ROM to the latest version.

More information

[Updating firmware or system ROM](#)

[DIMM and NVDIMM population information](#)

[Server user guide](#)

Server fails to recognize existing memory

Symptom

The server does not recognize existing memory.

Cause

- The server does not support the processor installed in the server.
- The associated processor is not installed for all DIMMs in the server.
- The memory is not configured properly.
- The DIMM is degraded.
- The DIMM is not installed or seated properly.

Action

1. Verify that the server supports associated processor installed for the DIMM.
2. Verify that the associated processor is installed for all DIMMs in the server.
For more information, see the server user guide.
3. Verify that the memory is configured properly.
4. Reseat the memory.

 **IMPORTANT:** Use care when handling DIMMs. For more information, see "DIMM handling guidelines."

5. Replace all degraded DIMMs.

For more information, see the server maintenance and service guide.

6. Update the system ROM.

More information

[Updating firmware or system ROM](#)
[Server user guide](#)
[DIMM handling guidelines](#)
[Server maintenance and service guide](#)

Server fails to recognize new memory

Symptom

The server does not recognize new memory installed on the server.

Cause

- The memory is not supported on this server.
- The memory is not installed according to the server requirements.
- The memory limits are exceeded for the server.
- The processor is not supported on the server.
- The memory is not installed or seated properly.

Action

1. Be sure that the memory is the correct type for the server.
2. Be sure that the memory is installed according to the server requirements.
3. Be sure that you have not exceeded the memory limits of the server or operating system.
4. Be sure the server supports the number of processor cores.
Some server models support only 32 cores and this might reduce the amount of memory that is visible.
5. Be sure that no Event List error messages are displayed.
6. Be sure that the memory is seated properly.
7. Be sure that no conflicts are occurring with existing memory. Run the server setup utility.
8. Test the memory by installing the memory into a known working server.
Be sure that the memory meets the requirements of the new server on which you are testing the memory.
9. Update the system ROM to the latest version.
10. Replace the memory.
For more information, see the server maintenance and service guide.

More information

[Updating firmware or system ROM](#)
[Updating firmware or system ROM](#)

Uncorrectable memory error

Symptom

- A POST error message is displayed.
- Stop error or blue screen (Windows)
- Purple diagnostic screen (Linux)
- Linux kernel panic
- A system “hang”
- A system “freeze”
- ASR
- Server restarts or powers down unexpectedly
- Parity errors occur

Cause

- The DIMM is not installed or seated properly.
- The DIMM has failed.

Action

1. Reseat the DIMM.
2. Update the system ROM to the latest version.
3. If the issue still exists, then replace the DIMM.

For more information, see the server maintenance and service guide.

More information

[Updating firmware or system ROM](#)
Server maintenance and service guide
[DIMM handling guidelines](#)

Correctable memory error threshold exceeded

Symptom

- Performance is degraded.
- The memory LED is amber.
- ECC errors occur with no other symptoms.

Cause

- The DIMM is not installed or seated properly.
- The DIMM has failed.

Action

1. Update the system ROM to the latest version.
2. Replace the DIMM.

For more information, see the server maintenance and service guide.

More information

[Updating firmware or system ROM](#)

[Server maintenance and service guide](#)

[DIMM handling guidelines](#)

Persistent Memory issues

Persistent Memory module percentage remaining alerts

Symptom

A message is displayed.

Cause

- Persistent Memory module (PMM) is reporting a low percentage of its specified life remaining. Block swapping will not be possible in the near future to recover from errors and data may be lost.
- Persistent Memory module is reporting that its specified life remaining has dropped to a very low number and it must be replaced soon.

Action

1. Review the events related to the error, and follow any recommended actions.
2. Back up any data stored on the persistent regions of the Persistent Memory module.
3. Replace the Persistent Memory module.

For more information, see the user guide for your server.

Persistent Memory Module configuration errors

Symptom

An error message displays, stating that the memory option (DIMM or PMM) installed is not supported in the current configuration or that the memory option is not populated in the correct location for the configuration.

Cause

- The memory option installed is not supported in the current configuration.
- The memory option is not installed in a supported configuration.

Action

1. To ensure that you use a correct configuration, review the memory population rules for your server.
2. Remove the memory option indicated in the error message.
For more information, see the user guide for your server.
3. Install supported memory options in the server.
For more information, see the user guide for your server.
4. Review and make any required configuration changes in the System Utilities menus.
For more information, see the Persistent Memory User Guide on the [Hitachi Vantara website](#)

More information

Server maintenance and service guide
Server user guide

Persistent Memory Module goal configuration errors

Symptom

An error message displays, stating that there is a problem applying the goal configuration.

Cause

- The goal configuration could not be applied with the memory requested.
- DIMMs or the DIMM configuration was lost or mapped out when trying to apply the goal configuration.

Action

1. Review the events related to the error, and follow any recommended actions.
2. Verify that all Persistent Memory modules are present, in a healthy state, and at the same firmware revision.
3. Review the Persistent Memory error logs for any additional information.
4. Verify that a supported Persistent Memory tool was used to create the goal configuration.

For more information, see the Persistent Memory User Guide on the [Hitachi Vantara website](#).
If the issue persists, contact customer support.

Persistent Memory module memory health errors

Symptom

An error message displays, indicating a memory health error that indicates the following:

- The Persistent Memory module is approaching the end of its usable wear leveling.
- The Persistent Memory module has experienced a critical error and may no longer be operational.
- The Persistent Memory module has experienced an issue and is no longer resilient.

Cause

Persistent Memory module is reporting a nonhealthy health status due to one of the following:

- Low number or no available spare blocks
- Package sparing
- A critical internal failure

Action

1. Review the events related to the error, and follow any recommended actions.
2. Back up any data stored on the persistent regions of the Persistent Memory module.
3. If the issue persists, contact customer support.
4. If the issue persists, replace the Persistent Memory module.

For more information, see the user guide for your server.

NVDIMM issues

NVDIMM population errors

Symptom

- A POST error message is displayed.
- System halts.

Cause

- An unsupported number of NVDIMMs are installed on the server.
- An unsupported DIMM is installed on the server.
- The server contains an unsupported mixture of DIMM types.
- NVDIMMs and RDIMMs are not installed in the correct order.
- At least one standard DIMM is not installed on Processor 1 as required by the population guidelines.
- An Smart Storage Hybrid Capacitor is installed in the server.

Action

1. Review the messages that may indicate the reason the NVDIMMs are disabled. Perform steps stated in the error message.

For more information, see the error message guide for your server on the [Hitachi Vantara website](#)

Verify that all DIMMs are installed according to the population guidelines.

2. Remove all DIMM types that are not supported in the configuration.

For more information, see the server maintenance and service guide.

3. Verify that a Smart Storage Battery is installed on the server. The Smart Storage Hybrid Capacitor does not support NVDIMMs.

More information

Server maintenance and service guide

[DIMM handling guidelines](#)

NVDIMMs are disabled

Symptom

- All NVDIMMs are disabled.
- All NVDIMMs on a processor are disabled.

Cause

- Node interleaving is enabled.
- The current AMP mode is unsupported when NVDIMMs are installed.
- New NVDIMMs were installed on the server.
- The NVDIMM is installed in a slot that does not have backup power available.

Action

1. Review messages that may indicate the reason the NVDIMMs are disabled. Perform steps stated in the error message.

For more information, see the error message guide for your server on the [Hitachi Vantara website](#)

Ensure that all UEFI System Utility settings are configured to support NVDIMMs.

- If Node interleaving is enabled in UEFI System Utilities, change the setting to **Disabled**.
- If Advanced Memory Protection is set to any setting other than Advanced ECC Support, then change the setting to **Advanced ECC Support**.

For more information, see [Hitachi Vantara website](#)

If new NVDIMMs are installed on the server, sanitize the NVDIMMs to enable the NVDIMMs for use.

For more information, contact customer support.

For more information, contact customer support

Verify that your NVDIMM is installed in a slot that supports NVDIMMs. Move the NVDIMM to a slot that supports NVDIMMs.

For more information, see the server maintenance and service guide.

2. Verify that a supported Smart Storage Battery is properly installed and operating in the server.

More information

Server maintenance and service guide

[Troubleshooting resources](#)

The persistent memory drive does not appear in the OS

Symptom

When a persistent memory drive does not appear in the OS, this symptom usually indicates that the underlying NVDIMM is mapped out.

Cause

Uncorrectable memory errors exist in the NVDIMM and address range scrubbing is not enabled.

Action

1. In UEFI System Utilities, set the **Persistent Memory Address Range Scrub** option to **Enabled**.
 - a. From the **System Utilities** screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Persistent Memory Options > Persistent Memory Integrity Check.
 - b. Select Enabled.
 - c. Save your settings.

For more information, see the [Hitachi Vantara website](#).

The persistent memory drive is read only

Symptom

A persistent memory drive marked as "read only" usually indicates that the underlying NVDIMM detected is not armed for backup during the boot process.

Solution 1

Cause

- Previous backup operation failed.
- The current restore operation failed.
- A general arming error occurred.
- An erase error occurred.
- An NVDIMM controller error occurred.

Action

Solution 2

Cause

The persistent memory backup power requirements exceed the available backup battery power.

Action

Remove any hardware that was recently added to the server.

Solution 3

Cause

The backup energy source is not sufficiently charged and the charging process was skipped by the user.

Action

Reboot the system and wait for the backup energy source to sufficiently charge.

Solution 4

Cause

The backup energy source is not sufficiently charged and the charging process timed out.

Action

1. Check additional backup power source-related messages and perform any recommended actions.
2. If the issue still exists, replace the backup power source.

For more information, see the server maintenance and service guide.

More information

Server maintenance and service guide

The persistent memory drives lose persistency

Symptom

A persistent memory drive can potentially lose its ability to persist data after it has booted to the OS. When this event occurs, the server notifies the OS. The handling of this event is by the OS and version dependent.

Solution 1

Cause

The Persistent Memory Address Range Scrub error threshold is exceeded.

Action

Using UEFI System Utilities, reinitialize the backup storage devices.

For more information, see [Hitachi Vantara website](#)

Solution 2

Cause

The backup power source capacity no longer supports the backup operation.

Action

1. Review the messages indicating the error with a backup power source.
2. Replace the backup power source device.

For more information, see the server maintenance and service guide.

Solution 3

Cause

An NVDIMM controller error occurred at runtime.

Action

1. Review the messages indicating the NVDIMM controller error.
2. Perform the steps.

Scalable Persistent Memory issues

The persistent memory drive does not appear in the OS

Symptom

A persistent memory drive does not appear in the OS. This symptom usually indicates that the underlying NVDIMM is mapped out.

Solution 1

Cause

Uncorrectable memory errors exist in the logical NVDIMM and address range scrubbing is not enabled.

Action

1. In UEFI System Utilities, set the **Persistent Memory Address Range Scrub** option to **Enabled**.
 - a. From the **System Utilities** screen, select **System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Persistent Memory Options > Persistent Memory Integrity Check**.
 - b. Select **Enabled**.
 - c. Save your settings.

For more information, see [Hitachi Vantara website](#).

Solution 2

Cause

Invalid configuration data exists on one or more backup storage devices.

Action

Initialize the backup storage devices.

Solution 3

Cause

Not enough physical memory exists on the server.

Action

- Check the memory failures and perform the recommended action.
 - Install additional memory.
- For more information, see the server user guide.

Solution 4

Cause

Scalable Persistent Memory functionality is disabled because a physical NVDIMM is installed in the server.

Action

Remove the physical NVDIMM from the server.

For more information, see the server maintenance and service guide.

More information

Server maintenance and service guide
Server user guide
[DIMM handling guidelines](#)

The persistent memory drive is read only

Symptom

A persistent memory drive marked as "read only" usually indicates that the underlying NVDIMM detected is not armed for backup during the boot process.

Solution 1

Cause

Previous backup operation failed.

Action

Check the cause of the backup failure and perform the recommended action.

Solution 2

Cause

The current restore operation failed.

Action

Check the cause of the restore failure and perform the recommended action.

Solution 3

Cause

A general Scalable Persistent NVDIMM arming error occurred.

Action

Check the additional errors and perform the recommended action.

Solution 4

Cause

The persistent memory backup power requirements exceed the available backup battery power.

Action

Remove any hardware that was recently added to the server.

Solution 5

Cause

The backup energy source is not sufficiently charged and the charging process was skipped by the user.

Action

Reboot the system and wait for the backup energy source to sufficiently charge.

Solution 6

Cause

The backup energy source is not sufficiently charged and the charging process timed out.

Action

1. Check the additional backup power source-related messages and perform any recommended actions.
2. If the issue still exists, replace the backup power source.

For more information, see the server maintenance and service guide.

Solution 7

Cause

The backup power source capacity can no longer support the Scalable Persistent Memory backup operation.

Action

1. Review the backup power source errors.
2. Replace the backup power source device.

For more information, see the server maintenance and service guide.

More information

Server maintenance and service guide

The persistent memory drives lose persistency

Symptom

A persistent memory drive can potentially lose its ability to persist data after it has booted to the OS. When this event occurs, the server notifies the OS. The handling of this event is by the OS and version dependent.

Solution 1

Cause

The Persistent Memory Address Range Scrub error threshold is exceeded.

Action

Using UEFI System Utilities, reinitialize the backup storage devices.

For more information, see [Hitachi Vantara website](#)

Solution 2

Cause

The backup power source capacity no longer supports the Scalable Persistent Memory backup operation.

Action

1. Review the messages indicating the error with a backup power source.
2. Replace the backup power source device.
3. For more information, see the server maintenance and service guide.

More information

Server maintenance and service guide

Scalable Persistent Memory backup and restore failure

Symptom

Failures occur during the Scalable Persistent Memory backup or restore operations. This symptom usually occurs because of hardware errors and failures.

Solution 1

Cause

A backup storage device fails.

Action

1. To locate a message that indicates the failed backup storage device.
2. Replace the failed backup storage device.

For more information, see the server maintenance and service guide.

Solution 2

Cause

A backup storage device is missing.

Action

1. To locate a message that indicates the location of the missing backup storage device.
2. Replace the failed backup storage device.

For more information, see the server maintenance and service guide.

Solution 3

Cause

Persistent memory backup power requirements exceed the available backup battery power.

Action

Remove any hardware that was recently added to the server.

For more information, see the server maintenance and service guide.

Solution 4

Cause

The backup power source was not sufficiently charged and the charging process was skipped by the user.

Action

Reboot the server and wait for the backup power source to sufficiently charge.

Solution 5

Cause

The backup power source was not sufficiently charged and the charging process timed out.

Action

1. Review the additional backup power source-related messages.
2. Perform any actions.
3. If the issues still exist, replace the backup power source.

For more information, see the server maintenance and service guide.

More information

Server maintenance and service guide

Unable to configure Scalable Persistent Memory

Cause

Scalable Persistent Memory functionality is disabled because a physical NVDIMM-N is installed in the server.

Action

Remove the physical NVDIMM-N from the server.

For more information, see the server maintenance and service guide.

More information

Server maintenance and service guide

[DIMM handling guidelines](#)

Processor issues

Troubleshooting the processor

Symptom

A POST error message is received.

Cause

- One or more processors are not supported by the server.
- The processor configuration is not supported by the server.
- The server ROM is not current.
- A processor is not seated properly.
- A processor has failed.



CAUTION: To avoid damage to the processor or system board, only authorized personnel should attempt to replace or install the processor in this server.

Be sure to review the [Processor troubleshooting guidelines](#) before you attempt any steps that involve the processor.

Some steps in this procedure may require an authorized service provider. Be sure to refer to the server user guide for procedures provided in this section.

Action

1. Be sure that each processor is supported by the server. Be sure that each processor is installed as directed in the server documentation.

The processor socket requires specific installation steps. Only install supported processors.

2. Be sure the server ROM is current.
3. If not supported by the server, be sure that you are not mixing processor stepping, core speeds, or cache sizes.
4. If the server has only one processor installed, reseal the processor.

For more information, see the server maintenance and service guide.

If the issue is resolved after you restart the server, the processor was not installed properly.

5. If the server has only one processor installed, replace it with a known functional processor.

If the issue is resolved after you restart the server, the original processor failed.

6. If the server has multiple processors installed, test each processor:

- a. Remove all but one processor from the server.

Replace each with a processor terminator board or blank, if applicable to the server.

- b. Replace the remaining processor with a known functional processor.

If the issue is resolved after you restart the server, a fault exists with one or more of the original processors. To locate the faulty processor or processors, install each processor one by one, restarting each time. At each step, be sure the server supports the processor configurations.

More information

Server user guide

Server maintenance and service guide

[Processor troubleshooting guidelines](#)

Uncorrectable machine check exception

Symptom

A POST error message is received indicating an uncorrectable machine check exception.

Cause

There are many possible causes for this error. Review the additional details provided with the error message.

Action

1. Review the error message text for additional details to troubleshoot the specified components.
 - a. If the message text directs you to replace an AMD processor, try reseating the processor before replacing the processor.

Be sure to review the processor information in the maintenance and service guide before servicing the processor.

- b. If the issue still exists, continue to the next step.
2. Download the Active Health System log and the OS logs.
3. Update the system firmware.

Do not attempt to update the firmware more than one time. If the issue still exists after updating the firmware, continue to the next step.
4. If the issue persists, contact customer support.

More information

[Updating firmware or system ROM](#)

[Processor troubleshooting guidelines](#)

[Server maintenance and service guide](#)

[Reports and Logs overview](#)

Trusted Platform Module issues

TPM fails or is not detected

Symptom

The TPM failed or the TPM is no longer detected.

Cause

- The TPM failed.
- The TPM is not configured properly in UEFI System Utilities.
- The boot mode is not configured for the TPM installed on the server.

Action

1. When a TPM is installed and used with BitLocker, be sure that the TPM is enabled in UEFI System Utilities.

See the TPM replacement recovery procedure in the operating system documentation.
2. When a TPM is installed, be sure that the TPM is configured for a mode that is compatible with the OS running on the server.

Verify that the OS supports the version of TPM installed and configured on the server.
3. When a TPM 2.0 is installed, verify that the server is configured for UEFI boot mode.
4. Leave the TPM installed and request a new system board and TPM from a Hitachi Vantara authorized service provider.

System battery is low or lost power

Symptom

An error message is received indicating low power or loss of power.

Cause

Real-time clock system battery is running low on power or lost power.

Action

Replace the battery.

For more information, see the server maintenance and service guide.

More information

Server maintenance and service guide

System board and power backplane issues

Symptom

A POST message is received indicating an issue with either the system board or the power backplane.

Action

- Review all error messages for possible issues with other components and troubleshoot components identified.
- Verify that no loose connections exist on the system board or power backplane. It is not necessary to reseal processors.
- Verify that the custom Hitachi Vantara image files were reinstalled after the system board was replaced
- Remove any components recently added.

For more information, see the server maintenance and service guide.

- Power down and remove all power from the server. Remove the system battery for 10 minutes. Reinstall the battery and power on the server.

To locate the system battery and for server-specific procedures, see the product documentation on the

[Hitachi Vantara website](#)

To default using the BIOS utility (F9), reset the NVRAM. If the system will not boot, then use the System Maintenance Switch, SW6, to reset the NVRAM.

- If the issue persists, contact customer support.

More information

[Resolving loose connections](#)

microSD card issues

The system does not boot from the microSD card

Symptom

The system is not booting from the drive.

Cause

- The drive boot order is not set to boot from the microSD card.
- The microSD card is not detected by iLO.
- The microSD card is not seated properly.

Action

1. Be sure that the drive boot order in the UEFI System Utilities is set so that the server boots from the microSD card.
For more information, see [Hitachi Vantara website](#)
2. Use the iLO web interface to verify that the microSD card is detected by iLO.
3. Remove all power from the server. Reseat the microSD card, and then power on the server.

USB drive key issues

System does not boot from the USB drive key

Symptom

The system does not boot from the USB drive key.

Cause

- The USB drive key is not enabled in the UEFI System Utilities.
- The drive boot order is not set to boot from the USB drive key.
- The USB drive key is not seated properly.

Action

1. Be sure that USB is enabled in the UEFI System Utilities.
For more information, see [Hitachi Vantara website](#)
Be sure that the drive boot order in the UEFI System Utilities is set so that the server boots from the USB drive key.

2. Reseat the USB drive key.
3. Move the USB drive key to a different USB port, if available.

Graphics and video adapter issues

Troubleshooting general graphics and video adapter issues

Symptom

Graphics are not displaying as expected.

Cause

- The graphics or video adapter is not supported on the server.
- Insufficient power to support the graphics or video adapter.
- The graphics or video adapter is not installed or seated properly.

Action

- Use only cards listed as a supported option for the server.
- Be sure that the power supplies installed in the server provide adequate power to support the server configuration. Some high-power graphics adapters require specific cabling, fans, or auxiliary power.

For more information about adapter power requirements, see the documentation that ships with the graphics option or see the vendor website.

For more information about server power capabilities, see the server documentation on the [Hitachi Vantara website](#)

- Be sure that the adapter is seated properly.

Video issues

The screen is blank for more than 60 seconds after you power up the server

Symptom

The screen is blank for more than 60 seconds after the server powered up.

Cause

- The monitor is not receiving power.
- The monitor is not cabled properly.
- The monitor cables are not connected properly.
- The power is not sufficient for a PCIe device or graphics controller installed on the server.

- A video expansion board is installed, but is not powered or configured properly.
- A video expansion board installed on the server is not supported.
- The video drive is not current.

Action

1. Be sure that the monitor power cord is plugged into a working grounded (earthed) AC outlet.
2. Power up the monitor and be sure that the monitor light is on, indicating that the monitor is receiving power.
3. Be sure that the monitor is cabled to the intended server or KVM connection.
4. Be sure that no loose connections exist by verifying the following connections:
 - For rack-mounted servers, check the cables to the KVM switch and be sure that the switch is correctly set for the server. You might need to connect the monitor directly to the server to be sure that the KVM switch has not failed.
 - For tower model servers, check the cable connection from the monitor to the server, and then from the server to the power outlet.
 - For blades, verify that the SUV cable is connected to the VGA cable on the monitor and to the connector on the front of the blade.
5. Press any key, or enter the password, and wait for a few moments for the screen to activate to be sure that the energy saver feature is not in effect.
6. Verify that a PCIe device or graphics controller does not need additional power to operate. For more information, see the device documentation.
7. Be sure that a video expansion board has not been added to replace onboard video, making it seem like the video is not working. Disconnect the video cable from the onboard video, and then reconnect it to the video jack on the expansion board.

NOTE: All servers automatically bypass onboard video when a video expansion board is present.

8. Press any key, or enter the password, and wait for a few moments for the screen to activate to be sure that the power-on password feature is not in effect.

You can also tell if the power-on password is enabled if a key symbol is displayed on the screen when POST completes. If you do not have access to the password, you must disable the power-on password by using the Password Disable switch on the system board.

For more information, see the server documentation on the [Hitachi Vantara website](#)
9. If the video expansion board is installed in a PCI hot-plug slot, be sure that the slot has power by checking the power LED on the slot, if applicable.

For more information, see the server documentation on the [Hitachi Vantara website](#)
10. Be sure the server and the OS support the video expansion board.
11. Be sure that the video driver is current.

For driver requirements, see the third-party video adapter documentation.

More information

[Resolving loose connections](#)

[Server documentation](#)

Monitor does not function properly with energy saver features

Symptom

The monitor does not function properly with energy saver features.

Cause

The monitor does not support energy saver features.

Action

Verify that the monitor supports energy saver features. If the monitor does not support energy saver features, disable the features.

Video colors are wrong

Symptom

The video colors are displayed wrong on the monitor.

Cause

- The video cable is not connected securely to the correct port.
- The monitor and KVM switch are not compatible with the video output of the server.
- The video cable is damaged.

Action

- Be sure that the 15 pin VGA cable is securely connected to the correct VGA port on the server and to the monitor.
- Be sure the monitor and any KVM switch are compatible with the VGA output of the server.
- Be sure that the VGA cable is not damaged.
Replace the cable with a known working cable.

Slow-moving horizontal lines are displayed

Symptom

Slow-moving horizontal lines are displayed on the monitor.

Cause

Magnetic field interference is occurring.

Action

Move the monitor away from other monitors or power transformers.

Mouse and keyboard issues

Symptom

The mouse and/or keyboard are not operating normally.

Action

1. Verify that all cables and cords are securely and properly connected. Check the following:
 - If you are using a KVM switching device, verify that the server is properly connected to the switch.
 - If you have rack-mounted servers, check the cables to the switch box to verify that the switch is correctly set for the server.
 - If you have tower model servers, check the cable connection from the input device to the server.
2. If you are using a KVM switching device, verify that all cables and connectors are the proper length and are supported by the switch.

For more information, see the switch documentation.
3. Be sure the current drivers for the operating system are installed.
4. Replace the driver with a known functioning driver to verify that the device driver is not corrupted.
5. Restart the system. Check whether the input device functions correctly after the server restarts.
6. Replace the device with a known working equivalent device (a similar mouse or keyboard):
 - If the issue still occurs with the new mouse or keyboard, the connector port on the system I/O board is defective. Replace the board.
 - If the issue no longer occurs, the original input device is defective. Replace the device.
7. Be sure the keyboard or mouse is connected to the correct port. Determine whether the keyboard lights flash at POST or the NumLock LED illuminates. If not, change port connections.
8. Clean the keyboard or mouse.

More information

[Resolving loose connections](#)

Expansion board issues

System requests recovery method during expansion board replacement

Symptom

The system requests a recovery method during expansion board replacement on a BitLocker-encrypted server.

Action

When replacing an expansion board on a BitLocker-encrypted server, always disable BitLocker before replacing the expansion board. If BitLocker is not disabled, the system requests the recovery method selected when BitLocker was configured. Failure to provide the correct recovery password or passwords results in loss of access to all encrypted data.

Be sure to enable BitLocker after the installation is complete.

For information on BitLocker, see BitLocker for Servers on the [Microsoft website](#).

Network controller or FlexibleLOM issues

Network controller or FlexibleLOM is installed but not working

Symptom

The network controller or the FlexibleLOM is not working.

Action

1. Check the network controller or FlexibleLOM LEDs to see if any statuses indicate the source of the issue. For LED information, see the network controller documentation or server documentation.
2. Review the error messages that could indicate the issue.
3. Be sure no loose connections exist.
4. Be sure the correct cable type is used for the network speed or that the correct SFP or DAC cable is used. For dual-port 10 GB networking devices, both SFP ports should have the same media (for example, DAC cable or equivalent SFP+ module). Mixing different types of SFP (SR/LR) on a single device is not supported.
5. Be sure the network cable is working by replacing it with a known functional cable.
6. Be sure a software issue has not caused the failure. For more information, see the operating system documentation.
7. Be sure the server and operating system support the controller. For more information, see the operating system documentation or server documentation.
8. Be sure the controller is enabled in the UEFI System Utilities.
9. Be sure the server ROM is up to date.
10. Be sure the controller drivers are up to date.
11. Be sure a valid IP address is assigned to the controller and that the configuration settings are correct.

More information

[Resolving loose connections](#)

Server documentation

Network controller or FlexibleLOM has stopped working

Symptom

The network controller or FlexibleLOM stopped working.

Action

1. Check the network controller or FlexibleLOM LEDs to see if any statuses indicate the source of the issue. For LED information, see the network controller documentation or server documentation.
2. Be sure the correct network driver is installed for the controller and that the driver file is not corrupted. Reinstall the driver.
3. Be sure no loose connections exist.
4. Be sure the network cable is working by replacing it with a known functional cable.
5. Be sure the network controller or FlexibleLOM is not damaged.

More information

[Resolving loose connections](#)

Server documentation

Network controller or FlexibleLOM stopped working when an expansion board was added

Symptom

The network controller or FlexibleLOM stopped working when an expansion board was added to the server.

Cause

- The network controller or FlexibleLOM is not seated or connected properly.
- The network controller or FlexibleLOM is not supported by the OS or the server.
- Installation of the network controller or FlexibleLOM changes the server configuration.
- The network controller or FlexibleLOM drivers are out of date.
- The driver parameters do not match the configuration of the network controller.

Action

1. Be sure no loose connections exist.
2. Be sure the server and operating system support the controller. For more information, see the operating system documentation or server documentation.
3. Be sure the new expansion board has not changed the server configuration, requiring reinstallation of the network driver:
 - a. Uninstall the network controller driver for the malfunctioning controller in the operating system.
 - b. Restart the server and run the appropriate option in the UEFI System Utilities. Be sure the server recognizes the controller and that resources are available for the controller.
 - c. Restart the server, and then reinstall the network driver.
4. Be sure the correct drivers are installed. For more information, see the operating system documentation.
5. Be sure that the driver parameters match the configuration of the network controller. For more information, see the operating system documentation.

More information

[Resolving loose connections](#)
[Server documentation](#)

Network performance or virtual machine performance issues with G2 servers with AMD processors

Symptom

Network performance or virtual machine performance is not optimal with G2 servers with AMD processors.

Cause

Various system component configurations might impact network performance:

- Network tuning
- Adapter parameters
- Operating system settings

Action

1. Review networking tuning information.

For more information, see the following:

- Service notices, contact customer support.
- Network tuning guides on the [AMD website](#).

Energy pack issues

If you are required to replace an energy pack as part of the troubleshooting process, be sure to dispose of the energy pack properly.



WARNING: To reduce the risk of fire or burns after removing the energy pack:

- Do not disassemble, crush, or puncture the energy pack.
 - Do not short external contacts.
 - Do not dispose of the energy pack in fire or water.
-

After power is disconnected, battery voltage might still be present for 1s to 160s.

AVERTISSEMENT: Pour réduire les risques d'incendie ou de brûlures après le retrait du module batterie :

- N'essayez pas de démonter, d'écraser ou de percer le module batterie.
- Ne court-circuitiez pas ses contacts externes.
- Ne jetez pas le module batterie dans le feu ou dans l'eau.

Après avoir déconnecté l'alimentation, une tension peut subsister dans la batterie durant 1 à 160 secondes.

Energy pack support in G2 servers

Hitachi Vantara offers two centralized backup power source options to back up write cache content on P-series smart array controllers in case of an unplanned server power outage. In documentation and system messaging, energy pack is used to refer to both the Smart Storage Battery and the Smart Storage Hybrid Capacitor.

The energy pack might lose charge when shelved for long periods of time

Symptom

Any server configured with an energy pack for smart array Controllers might display a POST error message stating that the energy pack failed.

Cause

The energy pack discharged to a threshold where it is permanently disabled and must be replaced.

Action

1. Verify the energy pack status in iLO.
2. For more information, see the iLO User Guide on the [Hitachi Vantara website](#)
3. Install an energy pack with a recharge date that is in the future.

More information

[Active Health System Log](#)

Energy pack configuration error

Symptom

Any Advanced Server product configured with an energy pack that receives a POST error message indicating a configuration error or that the load capacity is exceeded for the energy pack.

Cause

The number of battery-backed devices exceeds the installed energy pack capacity.

Action

1. Do one of the following:
 - Ensure that the energy pack is fully charged. An Smart Storage Battery might take up to 120 minutes in a powered server or chassis to charge enough to support the number of battery-backed devices installed. An Smart Storage Hybrid Capacitor takes only 5 minutes to charge.
 - If the charge level is insufficient to support the battery-backed devices installed in the server or chassis, the energy pack output might not be enabled while the energy pack is charging. It might take up to 120 minutes in a powered server or chassis for the battery to charge fully. An Smart Storage Hybrid Capacitor takes only 5 minutes to charge.
 - Verify the energy pack status in iLO.
For more information, see the iLO User Guide on the [Hitachi Vantara website](#)
 - Remove some of the battery-backed devices using the energy pack. Smart array Controllers and NVDIMMs use the Smart Storage Battery. NVDIMMs are not supported with the Smart Storage Hybrid Capacitor.

For more information, see the server maintenance and service guide.

- Verify that the BIOS version supports the energy pack and controllers installed on the server.

More information

Server user guide

Server maintenance and service guide

Energy pack failure

Symptom

Any server configured with an energy pack for smart array Controllers receives a POST error message indicating an energy pack failure.

Cause

- Communication with the energy pack failed.
- The energy pack output is not enabled.

Action

- Verify that the energy pack is installed and cabled properly.

For more information, see the *Smart array Controllers User Guide* at <https://knowledge.hitachivantara.com/Documents/Servers>.

- Verify the energy pack status in iLO.
For more information, see the iLO User Guide on the [Hitachi Vantara website](#)
- Update the system ROM.
- If the issue persists, contact customer support.

More information

[Updating firmware or system ROM](#)

Cable issues

Drive errors, retries, timeouts, and unwarranted drive failures occur when using an older Mini SAS cable

Symptom

Errors, retries, timeouts, and unwarranted drive failures occur when using an older Mini SAS cable.

Cause

The Mini SAS cable might be reaching its life expectancy.

Action

The Mini SAS connector life expectancy is 250 connect/disconnect cycles (for external, internal, and cable Mini SAS connectors).

If using an older cable that could be near the life expectancy, replace the Mini SAS cable.

USB device not recognized, an error message is displayed, or the device does not power on when connected to an SUV cable

Symptom

- The USB device is not recognized when connected to an SUV cable.
- An error message is displayed.
- The device does not power on when connected to an SUV cable.

Cause

The USB connectors on the SUV cable do not support devices that require a power source greater than 500mA.

Action

1. Remove the USB device and do one of the following:
 - Attach a USB device that requires a power source less than 500mA.
 - Attach an externally powered USB hub to the SUV cable and connect the USB device to the hub.

Software issues

Operating system issues and resolutions

Operating system issues

Operating system locks up

Symptom

The operating system locks up.

Action

- Scan for viruses with an updated virus scan utility.
- Review the iLO Event Log.
- Gather the NMI Crash Dump information for review, if needed.
- If the issue persists, contact customer support.

Errors are displayed in the error log

Symptom

Error messages are displayed in the error log.

Action

Follow the information provided in the error log.

For more information, see the operating system documentation.

Issues occur after the installation of a service pack

Symptom

Issues occur after the installation of a service pack

Action

Update the operating system.

More information

[Updating the operating system](#)

Updating the operating system

Prerequisites

Before updating the operating system, read the release notes for each update.

Use care when applying operating system updates (Service Packs, hotfixes, and patches). If you do not require specific fixes from the update, Hitachi Vantara recommends that you do not apply the updates. Some updates overwrite files specific to

Procedure

1. Perform a full system backup.
2. Apply the operating system update, using the instructions provided.
3. Install the current drivers.

If you apply the update and have issues, locate files to correct the issues on the Hitachi Vantara Support Center <https://support.hitachivantara.com/en/user/answers/downloads.html#hardware-download>

Reconfiguring or reloading software

Prerequisites for reconfiguring or reloading software

If all other options have not resolved the issue, consider reconfiguring the system. Before reconfiguring the system, do the following:

Procedure

1. Weigh the projected downtime of a software reload against the time spent troubleshooting intermittent issues. It might be advantageous to start over by removing and reinstalling the software with issues, or, in some cases, by using the Erase Utility and reinstalling all system software.



CAUTION: Perform a backup before running the System Erase Utility. The utility sets the system to its original factory state, deletes the current hardware configuration information, including array setup and disk partitioning, and erases all connected hard drives completely. Refer to the instructions for using this utility.

2. Be sure the server has adequate resources (processor speed, hard drive space, and memory) for the software.
3. Be sure the server ROM is current and the configuration is correct.
4. Be sure that you have printed records of all troubleshooting information you have collected to this point.
5. Be sure that you have two good backups before you start. Test the backups using a backup utility.
6. Check the operating system and application software resources to be sure that you have the latest information.
7. If the last-known functioning configuration does not work, try to recover the system with operating system recovery software.

For more information, see the operating system documentation.

Restoring a backup version

If you recently upgraded the operating system or software and cannot resolve the issue, try restoring a previously saved version of the system. Before restoring the backup, make a backup of the current system. If restoring the previous system does not correct the issue, you can restore the current set to be sure you do not lose additional functionality.

For more information, see the documentation provided with the backup software.

Linux resources

To assist in possible LINUX installation issues on Hitachi Advanced Server products, capture either the so report or support config before contacting Hitachi Vantara technical support.

More information

Application software issues

Software locks up

Symptom

The software locks up.

Cause

- The software might be incompatible with other software on the server.
- Known issues might exist with the software.
- The server configuration might have changed.
- The server might be infected by a virus.

Action

1. Verify the application log and operating system log for entries indicating why the software locked up.
2. Verify for compatibility and incompatibility with other software on the server.
3. Verify the support website of the software vendor for known issues.
4. Review log files for changes made to the server that might have caused the issue.
5. Scan the server for viruses with an updated virus scan utility.

Errors occur after a software setting is changed

Symptom

The system locks up after settings were changed.

Cause

The new system settings are not supported.

Action

Check the system logs to determine what changes were made, and then change the settings back to the original configuration.

Errors occur after the system software is changed

Symptom

Errors occur after the system software is changed.

Action

Change the settings back to the original configuration. If more than one setting was changed, change the settings one at a time to isolate the cause of the issue.

Errors occur after an application is installed

Symptom

Errors occur after an application is installed on a server.

Action

- Verify the application log and operating system log for entries indicating why the software failed.
- Verify the system settings to determine if they are the cause of the error.
You might need to obtain the settings from the server setup utility and manually set the software switches.
For more information, see the application documentation, the vendor website, or both.
- Check for overwritten files.

To determine which files are added by the application, see the application documentation.

- Reinstall the application.
- Be sure you have the most current drivers.

ROM issues

Remote ROM flash issues

Command-line syntax error

Symptom

If the correct command-line syntax is not used, an error message describing the incorrect syntax is displayed and the program exits.

Cause

Incorrect command-line is used.

Action

1. Correct the command-line syntax.
2. Restart the process.

Access denied on target computer

Symptom

When attempting to access a networked target computer for which administrative privileges are not authorized, an error message is displayed describing the issue, and then the program exits.

Cause

Administrative privileges are not available for the user requesting access.

Action

1. Obtain administrative privileges for the target computer or server.
 2. Restart the process.
- Be sure the remote registry service is running on a Windows-based system.

Invalid or incorrect command-line parameters

Symptom

If incorrect parameters are passed into command-line options, an error message describing the invalid or incorrect parameter is displayed and the program exits.

Cause

Invalid or incorrect command-line parameters are used.

Action

1. Correct the invalid parameter.
2. Restart the process.

Network connection fails on remote communication

Symptom

An error message describing the broken connection displays and the program exits.

Cause

Because network connectivity cannot be guaranteed, it is possible for the administrative client to become disconnected from the target server during the ROM flash preparation. If any remote connectivity procedure fails during the ROM flash online preparation, the ROM flash does not occur for the target system.

Action

1. Attempt to ascertain and correct the cause of connection failure.
2. Restart the process.

Failure occurs during ROM flash

Symptom

The server will not start.

Cause

The flash cannot be interrupted during a ROM flash, or the ROM image is corrupted and the server does not start. The most likely reason for failure is a loss of power to the system during the flash process.

Action

Initiate ROMPaq disaster recovery procedures.

Target system is not supported

Symptom

If the target system is not listed in the supported servers list, an error message appears and the program exits.

Cause

Only supported systems can be upgraded using the Remote ROM Flash utility.

Action

To determine if the server is supported, contact customer support.

System requests recovery method during a firmware update

Symptom

System requests recovery method during a firmware update.

Action

1. Always disable BitLocker before updating the firmware.

If BitLocker is not disabled, the system requests the recovery method selected when BitLocker was configured. Failure to provide the correct recovery password or passwords results in loss of access to all encrypted data.

2. Update the firmware.

If BitLocker is configured to measure option ROMs, follow the firmware upgrade steps in "Keeping the system current."

BitLocker can be configured to measure the following option ROMs:

- NIC
- Smart array storage
- Standup HBAs

3. Enable BitLocker after the firmware updates are complete.

For information on BitLocker, see BitLocker for servers on the Microsoft website at <http://technet.microsoft.com/en-us/library/cc732774.aspx>.

More information

[Keeping the system current](#)

Updating firmware

Procedure

1. Verify the firmware version on the device.
2. Determine the latest firmware version available.

For more information, see the operating system documentation.

3. If a Trusted Platform Module (TPM) is installed and enabled on the server, disable BitLocker before updating the firmware.

For more information, see the operating system documentation.

4. Download and update the firmware to the current version supported for the hardware configuration.
5. Verify the firmware update by checking the firmware version.
6. If a TPM is installed and enabled on the server, enable BitLocker after the firmware update is complete.

For more information, see the operating system documentation.

Boot issues

Server does not boot

Symptom

The server does not boot.

Cause

- The system ROMPaq flash fails.
- The system ROM is corrupt.
- The server fails to boot after a SYSROM update using ROMPaq.
- A logical drive is not configured on the smart array RAID controller.
- The controller boot order is not set properly.
- Smart arrays containing multiple logical drives might require the boot logical drive to be selected within SSA (F5).
- Invalid or corrupted firmware is detected.

Action

- Review the steps in the OS boot issues flowchart.
- Verify the controller boot order.

For more information, see [Hitachi Vantara website](#)

Access the redundant ROM using one of the following procedures:

- Accessing the redundant ROM (nonblade servers)

More Information

[OS boot issues flowchart](#)

Accessing the redundant ROM (non-blade servers)

If the system ROM is corrupted, the system automatically switches to the redundant ROM in most cases. If the system does not automatically switch to the redundant ROM, perform the following steps.

Procedure

1. Power down the server.
2. Remove the server from the rack, if necessary.
3. Remove the access panel.
4. Change positions 1, 5, and 6 of the system maintenance switch to on.
5. Install the access panel.
6. Install the server into the rack.
7. Power up the server.
8. After the system beeps, repeat steps 1 through 3.
9. Change positions 1, 5, and 6 of system maintenance switch to off.
10. Repeat steps 5 and 6.

If both the current and backup versions of the ROM are corrupt, return the system board for a service replacement.

To switch to the backup ROM when the System ROM is not corrupt, use the UEFI System Utilities.

More information

[UEFI System Utilities](#)

PXE boot guidelines for UEFI servers

- When the server is configured for UEFI Boot Mode, PXE servers must be configured with a UEFI boot image. For x64 EFI machines, the DHCP server also needs to be configured to support x64 EFI DHCP boot requests.

For more information, see [Hitachi Vantara website](#).

- When booting VMware ESX in UEFI Boot Mode, UEFI Optimized Boot must be enabled.
- When the server boots in UEFI Boot Mode, it does not boot media with a legacy OS installation. This includes DOS targets and Windows or Linux systems installed in Legacy BIOS Boot Mode. The reverse is also true for servers that boot in Legacy BIOS Boot Mode.

Software and configuration utilities

Server mode

The software and configuration utilities presented in this section operate in online mode, offline mode, or in both modes.

<u>Software or configuration utility</u>	<u>Server mode</u>
<u>Active Health System</u>	Online and Offline
<u>iLO 5</u>	Online and Offline
<u>Smart Storage Administrator</u>	Online and Offline
<u>iLO RESTful API</u>	Online and Offline
<u>Intelligent Provisioning</u>	Online and Offline
<u>Service Pack for Hitachi Vantara</u>	Online and Offline
<u>Smart update manager</u>	Online and Offline
<u>UEFI System Utilities</u>	Offline

Active Health System

The Active Health System monitors and records changes in the server hardware and system configuration.

The Active Health System provides:

- Continuous health monitoring of over 1600 system parameters
- Logging of all configuration changes
- Consolidated health and service alerts with precise time stamps
- Agentless monitoring that does not affect application performance

For more information about the Active Health System, see the iLO user guide at the following website:
<https://knowledge.hitachivantara.com/Documents/Servers>.

Active Health System data collection

The Active Health System does not collect information about your operations, finances, customers, employees, or partners.

Examples of information that is collected:

- Server model and serial number
- Processor model and speed
- Storage capacity and speed
- Memory capacity and speed
- Firmware/BIOS and driver versions and settings

The Active Health System does not parse or change OS data from third-party error event log activities (for example, content created or passed through the OS).

Active Health System Log

The data collected by the Active Health System is stored in the Active Health System Log. The data is logged securely, isolated from the operating system, and separate from customer data. Host resources are not consumed in the collection and logging of Active Health System data.

When the Active Health System Log is full, new data overwrites the oldest data in the log.

It takes less than 5 minutes to download the Active Health System Log and send it to a support professional to help you resolve an issue.

When you download and send Active Health System data to Hitachi Vantara, you agree to have the data used for analysis, technical resolution, and quality improvements. The data that is collected is managed according to the privacy statement, available at <https://knowledge.hitachivantara.com/Documents/Servers>

iLO 5 is a remote server management processor embedded on the system boards of Hitachi Advanced Server products. iLO enables the monitoring and controlling of servers from remote locations. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely. iLO (Standard) comes preconfigured on Hitachi Advanced Server products without an additional cost or license.

Features that enhance server administrator productivity and additional new security features are licensed. For more information, contact customer support.

For more information about iLO, see the iLO user guide at the following website:
<https://knowledge.hitachivantara.com/Documents/Servers>.

iLO Federation

iLO Federation enables you to manage multiple servers from one system using the iLO web interface.

When configured for iLO Federation, iLO uses multicast discovery and peer-to-peer communication to enable communication between the systems in iLO Federation groups.

When you navigate to one of the iLO Federation pages, a data request is sent from the iLO system running the web interface to its peers, and from those peers to other peers until all data for the selected iLO Federation group is retrieved.

iLO supports the following features:

- Group health status—View server health and model information.
- Group virtual media—Connect URL-based media for access by a group of servers.
- Group power control—Manage the power status of a group of servers.
- Group power capping—Set dynamic power caps for a group of servers.
- Group firmware update—Update the firmware of a group of servers.
- Group license installation—Enter a license key to activate iLO licensed features on a group of servers.
- Group configuration—Add iLO Federation group memberships for multiple iLO systems.

Any user can view information on iLO Federation pages, but a license is required for using the following features: Group virtual media, Group power control, Group power capping, Group configuration, and Group firmware update.

For more information about iLO Federation, see the iLO user guide at the following website:
<https://knowledge.hitachivantara.com/Documents/Servers>.

iLO Service Port

The Service Port is a USB port with the label **iLO** on supported servers .

When you have physical access to a server, you can use the Service Port to do the following:

- Download the Active Health System Log to a supported USB flash drive.
When you use this feature, the connected USB flash drive is not accessible by the host operating system.
- Connect a client (such as a laptop) with a supported USB to Ethernet adapter to access the iLO web interface, remote console, CLI, iLO RESTful API, or scripts.

Hitachi Vantara recommends the USB to Ethernet Adapter (part number Q7Y55A).

Port. Hitachi Vantara recommends the Micro USB to USB Adapter (part number 789904-B21).

When you use the iLO Service Port:

- Actions are logged in the iLO event log.
 - The server UID flashes to indicate the Service Port status.
- You can also retrieve the Service Port status by using a REST client and the iLO RESTful API.

- You cannot use the Service Port to boot any device within the server, or the server itself.
- You cannot access the server by connecting to the Service Port.
- You cannot access the connected device from the server.

For more information about the iLO Service Port, see the iLO user guide at the following website:
<https://knowledge.hitachivantara.com/Documents/Servers>.

iLO RESTful API

iLO includes the iLO RESTful API, which is Redfish API conformant. The iLO RESTful API is a management interface that server management tools can use to perform configuration, inventory, and monitoring tasks by sending basic HTTPS operations (GET, PUT, POST, DELETE, and PATCH) to the iLO web server.

To learn more about the iLO RESTful API, see the [Hitachi Vantara website](#)

For specific information about automating tasks using the iLO RESTful API, contact customer support

RESTful Interface Tool

The RESTful Interface Tool (iLOREST) is a scripting tool that allows you to automate Advanced Server product management tasks. It provides a set of simplified commands that take advantage of the iLO RESTful API. You can install the tool on your computer for remote use or install it locally on a server with a Windows or Linux Operating System. The RESTful Interface Tool offers an interactive mode, a scriptable mode, and a file-based mode similar to CONREP to help decrease automation times.

Intelligent Provisioning

Intelligent Provisioning is a single-server deployment tool embedded in Advanced Server products. Intelligent Provisioning simplifies server setup, providing a reliable and consistent way to deploy servers.

NOTE: After you have selected a mode, you must reprovision the server to change the mode that launches when you boot to F10.

Intelligent Provisioning prepares the system for installing original, licensed vendor media and OS software. Intelligent Provisioning also prepares the system to integrate optimized server support software from the Service Pack for Advanced Server (SPV). SPV is a comprehensive systems software and firmware solution for Advanced Server products. These components are preloaded with a basic set of firmware and OS components that are installed along with Intelligent Provisioning.

After the server is running, you can update the firmware to install additional components. You can also update any components that have been outdated since the server was manufactured.

To access Intelligent Provisioning:

- Press **F10** from the POST screen and enter Intelligent Provisioning.
- From the iLO web interface using **Always On**. **Always On** allows you to access Intelligent Provisioning without rebooting your server.

Intelligent Provisioning operation

NOTE: Intelligent Provisioning 3.40 and later requires iLO firmware version 2.10.

Intelligent Provisioning includes the following components:

- Critical boot drivers
- Active Health System (AHS)
- Erase Utility
- Deployment Settings

❗ IMPORTANT:

- Although your server is preloaded with firmware and drivers, Hitachi Vantara recommends updating the firmware upon initial setup. Also, downloading and updating the latest version of Intelligent Provisioning ensures the latest supported features are available.
- For Advanced Server products, firmware is updated using the Intelligent Provisioning Firmware Update utility.
- Do not update firmware if the version you are currently running is required for compatibility.

NOTE: Intelligent Provisioning does not function within multihomed configurations. A multihomed host is one that is connected to two or more networks or has two or more IP addresses.

Intelligent Provisioning provides installation help for the following operating systems:

- Microsoft Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware ESXi/vSphere Custom Image
- ClearOS

Not all versions of an OS are supported. For information about specific versions of a supported operating system, see the OS Support Matrix on the [Hitachi Vantara website](https://knowledge.hitachivantara.com/Products/Server/Support/OS)

Management security

Hitachi Advanced Server products are built with some of the industry's most advanced security capabilities, out of the box, with a foundation of secure embedded management applications and firmware. The management security provided by embedded management products enables secure support of modern workloads, protecting your components from unauthorized access and unapproved use. The range of embedded management and optional software and firmware available with the iLO Advanced license provides security features that help ensure protection, detection, and recovery from advanced cyber attacks. For more information, see the HA800 G2 Series Server Security Reference Guide on the Hitachi Vantara at <https://knowledge.hitachivantara.com/Documents/Servers>.

UEFI System Utilities

The UEFI System Utilities is embedded in the system ROM. Its features enable you to perform a wide range of configuration activities, including:

- Configuring system devices and installed options.
- Enabling and disabling system features.
- Displaying system information.
- Selecting the primary boot controller or partition.

- Configuring memory options.
- Launching other preboot environments.

UEFI can provide:

- Support for boot partitions larger than 2.2 TB. Such configurations could previously only be used for boot drives when using RAID solutions.
- Secure Boot that enables the system firmware, option card firmware, operating systems, and software collaborate to enhance platform security.
- UEFI Graphical User Interface (GUI)
- An Embedded UEFI Shell that provides a preboot environment for running scripts and tools.
- Boot support for option cards that only support a UEFI option ROM.

Selecting the boot mode

This server provides two **Boot Mode** configurations: UEFI Mode and Legacy BIOS Mode. Certain boot options require that you select a specific boot mode. By default, the boot mode is set to **UEFI Mode**. The system must boot in **UEFI Mode** to use certain options, including:

- Secure Boot, UEFI Optimized Boot, Generic USB Boot, IPv6 PXE Boot, iSCSI Boot, and Boot from URL
- Fibre Channel/FCoE Scan Policy

NOTE: The boot mode you use must match the operating system installation. If not, changing the boot mode can impact the ability of the server to boot to the installed operating system.

Prerequisite

When booting to **UEFI Mode**, leave **UEFI Optimized Boot** enabled.

Procedure

1. From the **System Utilities** screen, select **System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options > Boot Mode**.
2. Select a setting.
 - **UEFI Mode** (default)—Configures the system to boot to a UEFI compatible operating system.
 - **Legacy BIOS Mode**—Configures the system to boot to a traditional operating system in Legacy BIOS compatibility mode.
3. Save your setting.
4. Reboot the server.

Secure Boot

Secure Boot is a server security feature that is implemented in the BIOS and does not require special hardware. Secure Boot ensures that each component launched during the boot process is digitally signed and that the signature is validated against a set of trusted certificates embedded in the UEFI BIOS. Secure Boot validates the software identity of the following components in the boot process:

- UEFI drivers loaded from PCIe cards
- UEFI drivers loaded from mass storage devices
- Preboot UEFI Shell applications
- OS UEFI boot loaders

When Secure Boot is enabled:

- Firmware components and operating systems with boot loaders must have an appropriate digital signature to execute during the boot process.
- Operating systems must support Secure Boot and have an EFI boot loader signed with one of the authorized keys to boot. For the latest information about supported operating systems, see <https://support.hitachivantara.com/en/user/answers/interoperability.html>.

You can customize the certificates embedded in the UEFI BIOS by adding or removing your own certificates, either from a management console directly attached to the server, or by remotely connecting to the server using the iLO Remote Console.

You can configure Secure Boot:

- Using the **System Utilities** options described in the following sections.
- Using the iLO RESTful API to clear and restore certificates. For more information, contact customer support.
- Using the `secboot` command in the Embedded UEFI Shell to display Secure Boot databases, keys, and security reports.

Launching the Embedded UEFI Shell

Use the **Embedded UEFI Shell** option to launch the Embedded UEFI Shell. The Embedded UEFI Shell is a preboot command-line environment for scripting and running UEFI applications, including UEFI boot loaders. The Shell also provides CLI-based commands you can use to obtain system information, and to configure and update the system BIOS.

Prerequisites

Embedded UEFI Shell is set to Enabled.

Procedure

1. From the **System Utilities** screen, select **Embedded Applications > Embedded UEFI Shell**.
The **Embedded UEFI Shell** screen appears.
2. Press any key to acknowledge that you are physically present.
This step ensures that certain features, such as disabling **Secure Boot** or managing the **Secure Boot** certificates using third-party UEFI tools, are not restricted.
3. If an administrator password is set, enter it at the prompt and press **Enter**.
The `Shell>` prompt appears.
4. Enter the commands required to complete your task.
5. Enter the `exit` command to exit the Shell.

Smart Storage Administrator

SSA is the main tool for configuring arrays on smart array SR controllers. It exists in three interface formats: the SSA GUI, the SSA CLI, and SSA Scripting. All formats provide support for configuration tasks. Some of the advanced tasks are available in only one format.

The diagnostic features in SSA are also available in the standalone software Smart Storage Administrator Diagnostics Utility CLI.

During the initial provisioning of the server, an array is required to be configured before the operating system can be installed. You can configure the array using SSA.

SSA is accessible both offline (either through Intelligent Provisioning) and online:

- Accessing SSA in the offline environment

! **IMPORTANT:** If you are updating an existing server in an offline environment, obtain the latest version of SSA through Service Pack for Advanced Server before performing configuration procedures.

Using one of multiple methods, you can run SSA before launching the host operating system. In offline mode, users can configure or maintain detected and supported devices, such as optional smart array controllers and integrated smart array controllers. Some SSA features are only available in the offline environment, such as setting the boot controller and boot volume.

- Accessing SSA in the online environment

This method requires an administrator to download the SSA executables and install them. You can run SSA online after launching the host operating system.

USB support

G2 servers support all USB operating speeds depending on the device that is connected to the server.

External USB functionality

Hitachi Vantara provides external USB support to enable local connection of USB devices for server administration, configuration, and diagnostic procedures.

For additional security, external USB functionality can be disabled through USB options in UEFI System Utilities.

Redundant ROM support

The server enables you to upgrade or configure the ROM safely with redundant ROM support. The server has a single ROM that acts as two separate ROM images. In the standard implementation, one side of the ROM contains the current ROM program version, while the other side of the ROM contains a backup version.

NOTE: The server ships with the same version programmed on each side of the ROM.

Safety and security benefits

When you flash the system ROM, the flashing mechanism writes over the backup ROM and saves the current ROM as a backup, enabling you to switch easily to the alternate ROM version if the new ROM becomes corrupted for any reason. This feature protects the existing ROM version, even if you experience a power failure while flashing the ROM.

Keeping the system current

Updating firmware or system ROM

To update firmware or system ROM, use one of the following methods:

- The **Firmware Update** option in the System Utilities.
- The `fwupdate` command in the **Embedded UEFI Shell**.
- Service Pack for Advanced Server (SPV)
- Online flash components

Service Pack for Advanced Server

SPV is a systems software and firmware solution delivered as a single ISO file download. This solution uses SUM as the deployment tool and is tested and supports Hitachi Advanced Server and infrastructure.

SPV, along with SUM and iSUT, provides Smart Update system maintenance tools that systematically update Hitachi Advanced Server and infrastructure.

SPV can be used in an online mode on a server running Windows, Linux, or VMware vSphere ESXi, or in an offline mode where the server is booted to an operating system included in the ISO file.

The SPV is also available for download from the SPV download page at <https://support.hitachivantara.com/en/user/answers/downloads.html#hardware-download>.

Smart update manager

SUM is an innovative tool for maintaining and updating the firmware, drivers, and system software of Hitachi Advanced Server products, infrastructure, and associated options.

SUM identifies associated nodes you can update at the same time to avoid interdependency issues.

Key features of SUM include:

- Discovery engine that finds installed versions of hardware, firmware, and software on nodes.
- SUM deploys updates in the correct order and ensures that all dependencies are met before deploying an update.
- Interdependency checking.
- Automatic and step-by-step Localhost Guided Update process.
- Web browser-based user interface.
- Ability to create custom baselines and ISOs.
- Support for iLO Repository (G2 or later iLO 5 nodes only).
- Simultaneous firmware and software deployment for multiple remote nodes.
- Local offline firmware deployments with SPV deliverables.
- Extensive logging in all modes.

NOTE: SUM does not support third-party controllers, including flashing hard drives behind the controllers.

Integrated Smart Update Tools

- **iLO 5 with integrated Smart Update (G2 or later servers only):** Performs iLO Repository-based updates by downloading the components from iLO Repository when iLO Installation Queue has the components which can be updated by iSUT.

- **SUM:** A tool for firmware and driver maintenance for Hitachi Advanced Server products and associated options.

NOTE: SUM should not manage the same nodes.

Updating firmware from the System Utilities

Use the **Firmware Updates** option to update firmware components in the system, including the system BIOS, NICs, and storage cards.

Procedure

1. Access the System ROM Flash Binary component for your server from the Hitachi Vantara Support Center.
2. Copy the binary file to a USB media or iLO virtual media.
3. Attach the media to the server.
4. Launch the **System Utilities**, and select **Embedded Applications > Firmware Update**.
5. Select a device.

The **Firmware Updates** screen lists details about your selected device, including the current firmware version in use.

6. Select **Select Firmware File**.
7. Select the flash file in the **File Explorer** list.

The firmware file is loaded and the **Firmware Updates** screen lists details of the file in the **Selected firmware file** field.

8. Select **Image Description**, and then select a firmware image.
A device can have multiple firmware images.
9. Select **Start firmware update**.

Updating the firmware from the UEFI Embedded Shell

Procedure

1. Access the System ROM Flash Binary component for your server from the Hitachi Vantara Support Center (<https://support.hitachivantara.com/en/user/answers/downloads.html#hardware-download>).
2. Copy the binary file to a USB media or iLO virtual media.
3. Attach the media to the server.
4. Boot to the UEFI Embedded Shell.
5. To obtain the assigned file system volume for the USB key, enter `map -r`.
6. Change to the file system that contains the System ROM Flash Binary component for your server. Enter one of the `fsx` file systems available, such as `fs0:` or `fs1:`, and press **Enter**.
7. Use the `cd` command to change from the current directory to the directory that contains the binary file.
8. Flash the system ROM by entering `fwupdate -d BIOS -f filename`.
9. Reboot the server. A reboot is required after the firmware update in order for the updates to take effect and for hardware stability to be maintained.

Online Flash components

This component provides updated system firmware that can be installed directly on supported operating systems. Additionally, when used in conjunction with SUM, this Smart Component allows the user to update firmware on remote servers from a central location. This remote deployment capability eliminates the need for the user to be physically present at the server to perform a firmware update.

Drivers

❗ **IMPORTANT:** Always perform a backup before installing or updating device drivers.

Update drivers using any of the following **Smart Update Solutions**:

- Download the latest Service Pack for **Advanced Server** (includes smart update manager)
- Download **smart update manager** for Linux
- Download specific drivers

To locate the drivers for a server, go to

<https://support.hitachivantara.com/en/user/answers/downloads.html#hardware-download> , and then search for the product name/number.

Software and firmware

Update software and firmware before using the server for the first time, unless any installed software or components require an older version.

For system software and firmware updates, use one of the following sources:

- Download the SPV from the **Hitachi Vantara website**
- Download individual drivers, firmware, or other system software components from the server product page in the **Hitachi Vantara website**

Operating system version support

For information about specific versions of a supported operating system, see <https://support.hitachivantara.com/en/user/answers/interoperability.html>.

Reports and logs

More information

[Active Health System Log](#)

[Smart Storage Administrator Diagnostics Utility CLI](#)

[HPS report](#)

[Linux reports](#)

Reports and Logs overview

You might be asked to gather some of the following reports or logs when you contact Hitachi Vantara :

- Smart Storage Administrator Diagnostic Utility CLI reports
- HPS report
- Linux reports—`sosreport` and `supportconfig`

Active Health System Log

The data collected by the Active Health System is stored in the Active Health System Log. The data is logged securely, isolated from the operating system, and separate from customer data. Host resources are not consumed in the collection and logging of Active Health System data.

When the Active Health System Log is full, new data overwrites the oldest data in the log.

It takes less than 5 minutes to download the Active Health System Log and send it to a support professional to help you resolve an issue.

When you download and send Active Health System data to Hitachi Vantara, you agree to have the data used for analysis, technical resolution, and quality improvements. The data that is collected is managed according to the privacy statement, available at <https://www.hitachivantara.com/en-us/company/legal.privacy.html>

Active Health System Log download methods

You can use the following methods to download the Active Health System Log:

- **iLO web interface**—Download the log for a range of days or download the entire log from the **Active Health System Log** page.
- **cURL utility**—Download the log by using the cURL command-line tool.
- **iLO RESTful API and RESTful Interface Tool**—For more information, see <https://knowledge.hitachivantara.com/Documents/Servers>.

Downloading the Active Health System Log for a date range

Procedure

1. Click **Information** in the navigation tree, and then click the **Active Health System Log** tab.

The Active Health System Log is inaccessible when a download of the log is in progress.

2. Enter the range of days to include in the log. The default value is seven days.
 - a. Click the **From** box.
A calendar is displayed.
 - b. Select the range start date on the calendar.
 - c. Click the **To** box.
A calendar is displayed.
 - d. Select the range end date on the calendar.

To reset the range to the default values, click ↶.

3. (Optional) Enter the following information to include in the downloaded file:

- Support case number (up to 14 characters)
- Contact name
- Phone number (up to 39 characters)
- Email address
- Company name

The contact information you provide will be treated in accordance with the Hitachi Vantara privacy statement. This information is not written to the log data stored on the server.

4. Click **Download**.
5. Save the file.
Files that are larger than 25 MB must be compressed and uploaded to an FTP site. If needed, contact customer support.

Downloading the entire Active Health System Log

It might take a long time to download the entire Active Health System Log. If you must upload the Active Health System Log for a technical issue, Hitachi Vantara recommends downloading the log for the specific range of dates in which the problem occurred.

Procedure

1. Click **Information** in the navigation tree, and then click the **Active Health System Log** tab.
The Active Health System Log is inaccessible when a download of the log is in progress.
2. Click **Show Advanced Settings**.
3. (Optional) Enter the following information to include in the downloaded file:
 - Support case number (up to 14 characters)
 - Contact name
 - Phone number (up to 39 characters)
 - Email address
 - Company name

The contact information that you provide will be treated in accordance with the Hitachi Vantara privacy statement. This information is not written to the log data stored on the server.

4. Click **Download Entire Log**.
5. Save the file.

Files that are larger than 25 MB must be compressed and uploaded to an FTP site. If needed, contact customer support.

Downloading the Active Health System Log by using cURL

Procedure

1. Install cURL.
2. You can download cURL from the following website: <http://curl.haxx.se/>.
3. Open a command window.
4. Enter a command similar to the following examples.

! **IMPORTANT:** When you enter these commands, ensure that you do not use spaces or other unsupported characters.

If required by your command-line environment, special characters such as the ampersand must be preceded by the escape character. See the command-line environment documentation for more information.

To download the Active Health System Log for a range of dates:

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?from=<yyyy-mm-dd>&to=<yyyy-mm-dd>" -k -v -u <username>:<password> -o <filename>.ahs
```

- To download the Active Health System Log for the last seven days, and add a Hitachi Vantara supportcase number to the log header:

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?days=<number_of_days>&case_no=<number>" -k -v -u <username>:<password> -o <filename>.ahs
```

- To download the Active Health System Log for the last seven days, and include a case number and contact information:

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?days=<number_of_days>&case_no=<number>&contact_name=<name>&phone=<phone_number>&email=<email_address>&co_name=<company>" -k -v -u <username>:<password> -o <filename>.ahs
```

- To download the entire Active Health System Log:

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?downloadAll=1" -k -v -u <username>:<password> -o <filename>.ahs
```

5. The file is saved to the specified path.
6. Close the command window.

Files that are larger than 25 MB must be compressed and uploaded to an FTP site. If needed, contact customer support.

cURL command usage with iLO

When you use cURL to extract the Active Health System log, the command components include the following:

Options

<iLO IP address>

Specifies the iLO IP address.

from=<yyyy-mm-dd>&to=<yyyy-mm-dd>

Represents the start and end date of the range of dates to include in the log. Enter dates in the format year-month-day, for example, 2017-07-29 for July 29, 2017.

days=<number of days>

Specifies that you want to download the log file for the last <number of days>from today's date.

downloadAll=1

Specifies that you want to download the entire log.

-k

Specifies that HTTPS warnings will be ignored, which could make the connection insecure.

-v

Specifies verbose output.

-u <username>:<password>

Specifies your iLO user account credentials.

-o <filename>.ahs

Specifies the output file name and path.

case_no=<support case number>

Specifies a Hitachi Vantara support case number to add to the log header.

Options for adding contact information to the downloaded log

phone=<phone number>

Specifies a phone number to add to the log header.

email=<email address>

Specifies an email address to add to the log header.

contact_name=<contact name>

Specifies a contact name to add to the log header.

co_name=<company name>

Insert your company name in the log header.

Clearing the Active Health System Log

If the log file is corrupted, or if you want to clear and restart logging, clear the Active Health System Log.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click **Information** in the navigation tree, and then click the **Active Health System Log** tab.
The Active Health System Log is inaccessible when a download of the log is in progress.
2. Click **Show Advanced Settings**.
3. Scroll to the **Clear Log** section, and then click **Clear**.
4. When prompted to confirm the request, click **Yes, clear**.
iLO notifies you that the log is being cleared.
5. Reset iLO.

Resetting iLO is required because some Active Health System data is recorded to the log only during iLO startup. Performing this step ensures that a complete set of data is available in the log.

6. Reboot the server.

Rebooting the server is required because some information, such as the operating system name and version, is logged at server startup. Performing this step ensures that a complete set of data is available in the log.

Downloading the AHS log through IP

For more information, see the Intelligent Provisioning user guide at <https://knowledge.hitachivantara.com/Documents/Servers>.

Procedure

1. Open Intelligent Provisioning [F10] at boot-up.
2. Click **Perform Maintenance**.
3. Click Active Health System download.
4. Leave the range as the default or as instructed by the Hitachi Vantara technician.
5. Click **Download**.

Downloading the Active Health System log (iLOREST)

Prerequisites

- The RESTful Interface Tool is installed.
- Configure iLO Settings privilege

Procedure

1. Start the RESTful Interface Tool.
2. Log in to an iLO system:

```
iLOrest > login iLO host name or IP address -u iLO user name -p iLO password
```
3. Download the Active Health System log for the server you logged into in step **2**.
 - To download the log for the last seven days, enter a command similar to the following:

```
iLOrest > serverlogs --selectlog=AHS --directorypath=directory path
```
 - To download the log for a specified time period, enter a command similar to the following:

```
iLOrest > serverlogs --selectlog=AHS --directorypath=directory path  
--customiseAHS="from=YYYY-MM-DD&&to=YYYY-MM-DD"
```
 - To download the entire Active Health System log, enter a command similar to the following:

```
iLOrest > serverlogs --selectlog=AHS --downloadallahs --directorypath=directory path
```

The log is downloaded with the following file name: `_server serial number_YYYYMMDD.ahs`.

Files that are larger than 25 MB must be compressed and uploaded to an FTP site. If needed, contact customer support.

iLOREST serverlog command usage

`--selectlog=AHS`

Specifies that you want to work with the Active Health System log type.

`--directorypath=directory path`

Specifies the output file path.

`--customiseAHS="from=YYYY-MM-DD&&to=YYYY-MM-DD"`

Represents the start and end date of the range of dates to include in the log. Enter dates in the format year-month-day, for example, 2017-07-29 for July 29, 2017.

`--downloadallahs`

Specifies that you want to download the entire log.

For more information, see the [RESTful Interface Tool documentation](#).

Intelligent Provisioning diagnostic tools

Diagnostic tools are embedded on a NAND flash module that can be accessed by pressing F10 at POST during server boot. For more information, see "[Intelligent Provisioning software documentation](#)."

Performing a Diagnostics task using SSA

Procedure

1. Open SSA.
2. Open the **Diagnostics** panel by doing one of the following:
 - Select a device and click **Diagnose** in the quick navigation menu.
 - Select an available device from the **Home** screen, and then click **Diagnose** under the available options.
3. Select a report type.

For this example, use the Array Diagnostic Report selection.
4. Select **Array Diagnostic Report**.

The **Actions** panel for Array Diagnostic Report appears.
5. Click one of the task buttons:
 - If you click **View Diagnostic Report**, the report appears. When you are finished viewing the current report, click **Close** or **Save**.
 - If you click **Save Diagnostic Report**, wait for the report to generate, and then click **Close Report** or **Save Report**.

Smart Storage Administrator Diagnostics Utility CLI

Installing the utility

Procedure

1. Browse to the [Smart storage administrator website](#).
2. Click **Download software**.
3. Select an OS.
4. Identify the preferred software and version, and then click **Download**.
5. Save, and then run, the executable file.

By default, the software installs at `C:\Program Files\Smart Storage Administrator\`.

Launching the utility in CLI mode

Procedure

1. Click **Start>All Programs>Windows System>Smart Storage Administrator Diagnostics Utility>Read Me**
2. Open a command prompt as administrator.
3. Change directory (`cd`) to the location where `ssaduccli.exe` is installed.

This directory is commonly `C:\Program Files\Smart Storage Administrator\ssaduccli\bin`.

4. Do one of the following:
 - Generate a diagnostic report with the following command:`ssaduccli -f adu-report.zip`
 - Generate a SmartSSD Wear Gauge report with the following command:`ssaduccli -ssd -f ssd-report.zip`

For more options, use the following command:

```
ssaduccli -help
```

Diagnostic report procedures

Viewing the diagnostic report

Procedure

1. [Launch the utility](#).
2. Browse to the .zip file you created using the utility.
3. Open the HTML file to view the report.

Identifying and viewing diagnostic report files

The diagnostic report output archive contains the following files:

- `ADUReport.txt`—Diagnostic report in text format

- `ADUReport.xml`—Diagnostic report in XML format
- `ADUReportViewer.htm`—HTML viewer for XML diagnostic report
- `SlotX.txt` (`SlotX.old`)—Controller serial output log

The serial output log file(s) are only available if the Smart Array SAS/SATA Event Notification Service is installed and running.

Procedure

1. Extract `ADUReportViewer.htm` to a directory.
2. Open `ADUReportViewer.htm` in the browser.

SmartSSD Wear Gauge report procedures

Viewing the SmartSSD Wear Gauge report

Procedure

1. Launch the utility.
2. Browse to the .zip file you created using the utility.
3. Open the HTML file to view the report.

Identifying and viewing SmartSSD Wear Gauge report files

The SmartSSD Wear Gauge report output archive contains the following files:

- `SmartSSDWearGaugeReport.txt`—SmartSSD wear gauge report in text format
- `SmartSSDWearGaugeReport.json`—SmartSSD wear gauge report in JSON format
- `SmartSSDWearGaugeReport.htm`—HTML viewer for the JSON wear gauge report

Procedure

1. Extract the following files to a single directory:
 - `SmartSSDWearGaugeReport.json`
 - `SmartSSDWearGaugeReport.htm`
2. Open `SmartSSDWearGaugeReport.htm` in the browser.

Linux reports

To assist in possible Linux installation issues on Advanced Server products, capture either the `sosreport` or `supportconfig` before contacting Hitachi Vantara Support.

Symptom information checklist

Before troubleshooting a server issue, collect the following symptom information:

Procedure

- ☐ Does the server power on?
- ☐ Does the server complete POST?
- ☐ If the server does not complete POST, what is the status and behavior of each of the server LEDs?
- ☐ If server completes POST and video is available, are there any POST error messages? Record the text of the POST error message as displayed.
- ☐ Does the server successfully boot an operating system or hypervisor? If not, does the server display any of the following symptoms and at what point did the following symptom occur?
 - An uncorrectable machine check exception
 - Stop error or blue screen (Windows)
 - Purple diagnostic screen (Linux)
 - Linux kernel panic
 - A system “hang”
 - A system “freeze”
- ☐ Does the issue occur after an OS is installed?
- ☐ Does the issue occur when a new application is loading?
- ☐ What symptoms did the server display when the server malfunctioned?

For example, did the server reboot? Were there LED codes, health logs, or messages displayed on the screen?
- ☐ Are any indications present that show that the malfunction was reported as a memory error, PCI error, or so forth?

The processor now contains the memory controller and PCI Express controller, so faults in other areas might be attributed to a processor malfunction.
- ☐ When did the issue occur?

Record exactly when the issue happens (include the date and time). If it happens more than once, keep a list of all symptoms for each occurrence.
- ☐ What events preceded the failure? After which steps does the issue occur?
- ☐ What has been changed since the time the server was working?
- ☐ Has hardware or software been recently added or removed?

If yes, were the appropriate settings in the server setup utility changed?
- ☐ How long has the server exhibited issue symptoms?

☐ If the issue occurs randomly, what is the duration or frequency of the issue? ☐

What failed based on the iLO Event Log?