HITACHI

Hitachi Vantara

Hitachi VSP One File and NAS Platform

Remote Management using IPMI on VSP One File 32, HNAS 5200 and HNAS 5300

This document provides information on using the Intelligent Platform Management Interface (IPMI) in an HNAS environment.

MK-92HNAS092-07

January 2026

© 2026 Hitachi Vantara, 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., Hitachi Vantara, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.
Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.
Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.
Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.
By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and

2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.
Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.
AIX, DB2, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, IntelliMagic, IntelliMagic Vision, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z17, 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, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.
All other trademarks, service marks, and company names in this document or website are properties of their respective owners.
The open source content used in Hitachi Vantara products may be found within the Product documentation or you may request a copy of such information (including source code and/or modifications to the extent the license for any open source requires Hitachi make it available) by sending an email to OSS_licensing@hitachivantara.com.

Table of Contents

Table of Contents **3**
Preface **4**
About this document 4
Document conventions 4
Intended audience 4
Accessing product downloads 4
Getting Help 4
Chapter 1: IPMI overview 6
What is IPMI? 6
IPMI features supported by the HNAS server 6
Security considerations 7
Further reading 7
Chapter 2: Installing and configuring IPMI 8
Enabling IPMI on the HNAS server 8
Changing the IP address using a Web browser 10
Checking the IPMI version 10
Obtaining the IPMI firmware 10
Updating an IPMI installation 11
Chapter 3: Using IPMI 12
Using Remote Console Access 12
Checking the server power status 12
Using Power Cycle Server 12
Using Power Off Server - Immediate 13
Using Power On Server 13
Using a Web browser for IPMI power options 13
Setting the IPMI network port to “dedicated” 14
Chapter 4: Backup and restore overview 15
IPMI configuration backup 15
IPMI configuration restore 15

Preface

About this document

This document provides information on using the Intelligent Platform Management Interface (IPMI) in an HNAS environment.

Document conventions

This document uses the following typographic convention:

Convention	Description
Bold	• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: **Click OK**. • Indicates emphasized words in list items.
Italic	Indicates a document title or emphasized words in text.
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`

Intended audience

This document is intended for users working on Intelligent Platform Management Interface (IPMI) in an HNAS environment.

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: https://support.hitachivantara.com/.

Log in and select Product Downloads to access the most current downloads, including 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 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.

Chapter 1: IPMI overview

This document provides information on using the Intelligent Platform Management Interface (IPMI) in an HNAS environment.

What is IPMI?

The Intelligent Platform Management Interface (IPMI) is a specification for providing management and monitoring capability directly to computer hardware without requiring access to the firmware or software. This functionality is useful for unmanned data centers where physical access to the hardware is not available. For example, if an Administrator needs to turn the power to a server on or off but is not based at the same geographical location as the server, IPMI provides a method of power cycling the server remotely.

IPMI features supported by the HNAS server

The HNAS server supports the following IPMI features:

- Remote console access
- Power Off Server - Immediate
- Power On Server
- Power Cycle Server

Remote console access

This feature enables a remote Administrator to access a server over a network connection by providing a remote console.

Power Off Server - Immediate

This option turns off power to the server. It does not restart the server.

Caution: IPMI also provides a Power Off Server - Orderly Shutdown option. This option is not supported as it causes the NAS server to reboot instead of shut down.

Power On Server

This option restarts the server by turning on the power.

Power Cycle Server

For remote power cycling, IPMI provides two options:

- Reset Server
- Power Cycle Server

The NAS server supports **Power Cycle Server** only. This feature enables a remote Administrator to reboot the NAS server as if someone were pressing the power button locally.

On reboot the server will report the boot reason in the dblog:

```
Boot reason: Power up
```

The NVRAM log is always preserved and replayed after a reboot.

Caution: Using the unsupported Reset Server option results in no diagnostics being generated and no event appears in the dblog before shutdown. The boot reason on the following boot appears as:

```
Hm Early Fail Cause (4): TAN_PCIE_Reset CFB boot reason:
Motherboard
```

Security considerations

Before using IPMI with an HNAS server, note the following security considerations:

- Ensure that any HNAS server Linux passwords are changed from the default password, especially the root user password.
- Ensure that the ADMIN password on the IPMI installation is changed from the default password.
- Configure IPMI to use a dedicated network port which is connected to a dedicated secure network that cannot be accessed from anywhere except the remote monitoring site.

These steps help to protect your HNAS server from unauthorized access.

Further reading

Further information regarding the IPMI interface may be found in the SUPERMICRO® document titled “IPMI User’s Guide” which is located here:

https://www.supermicro.com/manuals/other/IPMI_Users_Guide.pdf

Chapter 2: Installing and configuring IPMI

Before using the IPMI features, the Administrator must enable and configure the IPMI settings on each individual HNAS server in order to be able to control them with IPMI - not just the node containing the Admin EVSs.

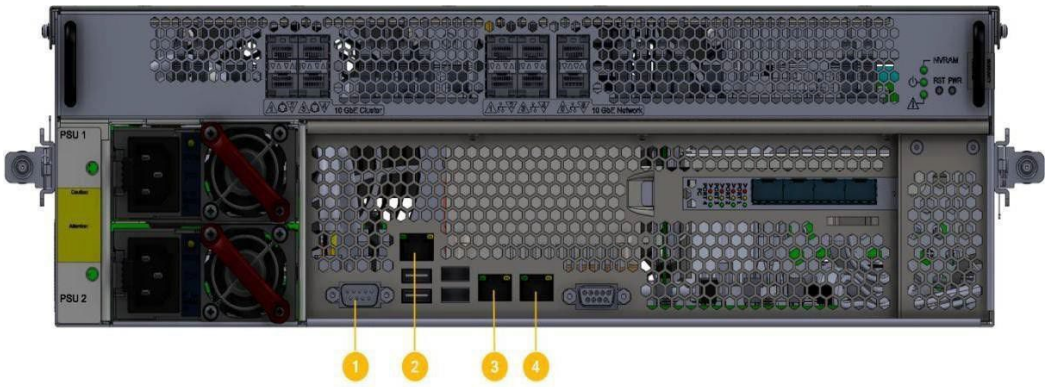
Enabling IPMI on the HNAS server

The HNAS server has the following pre-installed IPMI tools:

- ipmitool
- ipmievd
- All necessary Linux kernel modules To enable IPMI on an HNAS server in a cluster:

Procedure

1. Connect the separate IPMI network port (indicated below as annotation number 2) to your secure management network.



2. Connect to the SMU CLI and navigate to the Linux prompt on the HNAS server as follows:

    i. Login as the Manager user.

    ii. If you already know the IP addresses of the individual HNAS server nodes in the cluster, proceed to step 2(c).

Otherwise:

    i. Select the Admin EVS from the list of available servers by typing the corresponding number and pressing Enter.

ii. On the Admin EVS server, type ipaddr -s and press Enter. This displays the IP address of each server node in the cluster. Note the IP address of the HNAS server node being updated.

a) Type **Ctrl+c** to return to the SMU CLI.

b) Type **q** and press ENTER.

c) Run the following command: ssh supervisor@<HNAS server IP address>

d) Enter the Supervisor password.

e) Type **Ctrl+C** to enter the Linux console.

f) Type **su** and enter the root password to become a root user.

3. From the Linux prompt, run the following command to obtain the user ID number for the `ADMIN` user:

```
ipmitool user list | grep ADMIN
```

4. Run the following command appending the `ADMIN` user ID number to reset the password:

```
ipmitool user set password <user ID number for ADMIN>
```

This sets the password for the default username which is ADMIN. Once logged in, you can create additional users.

5. Run the following command:

```
ipmitool lan print 1
```

This command displays the IP address. By default, the address is obtained through DHCP

6. Run the following command:

```
ipmitool mc info
```

This command checks the Firmware Revision number. The correct version is 1.78 or higher. If the version is earlier than this, the server requires an update.

7. Run the following commands to specify a static IP address:

```
ipmitool lan set 1 ipsrc static
ipmitool lan set 1 ipaddr <ip address>

ipmitool lan set 1 netmask <netmask>

ipmitool lan set 1 defgw ipaddr <gateway ip

address> ipmitool lan print 1
```

It is also possible to change the IP address using the IPMI Management GUI. The server is now fully manageable remotely using HTTP or HTTPS with the IP address of the IPMI port.

Important: Record the values for future use.

Changing the IP address using a Web browser

To update the IP address using the SUPERMICRO® Web application:

Procedure

1. Navigate to http://<IP address of the IPMI port> using a Web browser. The SUPERMICRO® Web application appears.
2. Enter the IPMI ADMIN username and password. Note that the username and password are both case-sensitive.
3. Click on the Configuration option on the top tool bar.
4. Click on the Network option on the left-hand toolbar.
5. Enter the new IP address as required.
6. Click the logout icon to leave the application.

Checking the IPMI version

You can determine the IPMI version by connecting to the IPMI port address using a Web browser (**System** tab) or by using the following command at the Linux prompt:

```
ipmitool mc info
```

Obtaining the IPMI firmware

Before upgrading the IPMI version, you need to download the IPMI firmware.

To obtain the firmware, navigate to the SUPERMICRO® website, search for X11SSM-F and download the IPMI firmware. If the required version of the firmware is no longer available at the site, contact your Hitachi Vantara support advisor.
Extract the individual firmware file from the compressed file and save it on the system that you use to connect to the NAS server. You should also extract the IPMI Firmware Update document.

Updating an IPMI installation

Use the SUPERMICRO® Web application to update the IPMI version from any earlier version, even where the firmware version differs on each cluster node.

Important: While updating the IPMI firmware, it is important to maintain a power supply to the server.

Important: It is recommended that the current configuration Is saved before updating the IPMI firmware

Important: This procedure can cause the HNAS server to be temporarily out of service. To avoid an unplanned interruption to file serving on a cluster, migrate all EVSs away from the node which is being updated.

To update the IPMI firmware:

Procedure

1. Using a Web browser, navigate to **http://<IP address of the IPMI port>** from the PC containing the new firmware files. The SUPERMICRO® Web application appears.
2. Enter the IPMI ADMIN username and password. Note that the username and password are both case-sensitive.
3. Follow the instructions in the **WEB-GUI** section of the **IPMI Firmware Update** document provided by SUPERMICRO® in the firmware download to install the bin file.
4. The upgrade takes approximately five minutes. If access to the Web page is disrupted during the upgrade process, wait for at least 15 minutes before attempting a reboot of IPMI to allow the upgrade to finish in the background.

Chapter 3: Using IPMI

This section contains instructions on how to use the IPMI features supported on the HNAS server:

Using Remote Console Access

To obtain remote access to the HNAS server firmware console, use a separate Linux PC connected to the same management network as the HNAS server IPMI port.

On the Linux PC, enter the following command:

```
ipmitool -I lanplus -H <IP from IPMI LAN setup> -U ADMIN -P <password> sol
activate
```

Log into the server as supervisor. It is now possible to access the firmware functionality on the HNAS server using the server's standard CLI commands.

To exit the console, enter ~. (tilde dot)

Note that it is also possible to get remote console access from the web interface by selecting **Remote Control** followed **by iKVM/HTML5** and following the on-screen instructions.

Checking the server power status

To check the power status of the server, use a separate Linux PC connected to the same management network as the HNAS server's IPMI port.

On the Linux PC, enter the following command:

```
ipmitool -I lanplus -H <IP from IPMI LAN setup> -U ADMIN -P
<password> power status
```

The power can be 'Off' or 'On'.

Using Power Cycle Server

To reboot the HNAS server, use a separate Linux PC connected to the same management network as the HNAS server IPMIport.

On the Linux PC, enter the following command:

```
ipmitool -I lanplus -H <IP from IPMI LAN setup> -U ADMIN -P
<password> power cycle
```

It is also possible to power cycle the server from a Web browser connected to the IPMI port IP address.

Using Power Off Server - Immediate

To turn off the power to the HNAS server, use a separate Linux PC connected to the same management network as the HNAS server IPMI port.

On the Linux PC, enter the following command:

```
ipmitool -I lanplus -H <IP from IPMI LAN setup> -U ADMIN -P
<password> power off
```

This command performs a shutdown of the server.

It is also possible to perform a shutdown from a Web browser connected to the IPMI port IP address.

Using Power On Server

To turn on the power to the HNAS server, use a separate Linux PC connected to the same management network as the HNAS server IPMI port.

On the Linux PC, enter the following command:

```
ipmitool -I lanplus -H <IP from IPMI LAN setup> -U ADMIN -P
<password> power on
```

It is also possible to power on the server from a Web browser connected to the IPMI port IP address.

Using a Web browser for IPMI power options

The following IPMI power options are supported on the IPMI Web application:

- Power Off Server - Immediate
- Power On Server
- Power Cycle Server

To access the power options:

Procedure

1. Open a Web browser and navigate to the IPMI IP address configured using the ipmitool application. Use the ipmitool lan print 1 command to check the IP address if necessary.
2. Enter the ADMIN username and password.
3. On the menu bar, click Remote Control and then Power Control. The current power status

of the host is reported on the page. The status of the host can either be on or off.

4. Select one of the following options as required:

   - Power Off Server - Immediate
   - Power On Server
   - Power Cycle Server

5. Click the Perform Action button to begin the selected power option. If the power is turned off, the Web browser becomes unavailable for a few seconds.

Setting the IPMI network port to “dedicated”

To improve security the BMC network port should ideally be dedicated to IPMI. To do this then from the HNAS Linux prompt run the following command:

```
ipmitool raw 0x30 0x70 0x0c 1 0
```

To query the current setting then do:

```
ipmitool -raw 0x30 0x70 0x0c 0
```

The value returned can be decoded as follows: 0=dedicated, 1=shared, 2=failover

Chapter 4: Backup and restore overview

IPMI configuration backup

To back up the IPMI configuration use the web interface and select **Maintenance** followed by **IPMI Configuration**. Then select **Save**

IPMI configuration restore

To restore an IPMI configuration use the web interface and select **Maintenance** followed by **IPMI Configuration**. Then select **Choose file** and select the desired file. Finally select **Reload**.

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com