Hitachi Content Platform S Series Node

3.0.1

HCP S11 and S31 Node 3.0.1 Release Notes

HCP S Series Software Version 3.0.1.9
HCP S Series Operating System Version 3.0.0.1218

This document is intended for use by Hitachi Vantara and authorized resellers only and should not be given to customers. Unauthorized duplication or redistribution is prohibited.

RNI-HCPS021-02
July 2019

© 2019 Hitachi Vantara Corporation. 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 Corporation (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 Corporation 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 Corporation.

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 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, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, PowerPC, RS6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

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

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

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

Contents

About this document

This document contains release notes for release 3.0.1 of the **Hitachi Content Platform (HCP) S Series Node**. The document describes new features, product documentation, and resolved and known issues and provides other useful information about this release of the product.

Release highlights for HCP S Series Node 3.0.1

Release 3.0.1 of the HCP S Series Node adds support for 16TB data drives and 800GB database drives. The release also resolves some issues found in previous releases of the product.

Release highlights for HCP S Series Node 3.0

Release 3.0 of the HCP S Series Node introduces two new product models, includes new features and enhancements, and resolves several issues found in previous releases of the product.

HCP S11 and S31 Nodes

As of release 3.0, the HCP S Series Node comes in two new models, the HCP S11 Node and the HCP S31 Node. The S31 Node has more processing power and memory than the S11 Node and also allows for greater storage capacity.

S11 and S31 Nodes use completely different hardware from the hardware used in the older S Series Node models, the S10 Node and the S30 Node. S11 and S31 Node enclosures can hold more drives than the S10 and S30 Node enclosures can hold. S11 and S31 Nodes also support higher-capacity drives than S10 and S30 Nodes support.

The S11 and S31 Node enclosures are not interchangeable with the S10 and S30 Node enclosures.

Four access network ports
Each server module in an HCP S11 or S31 Node has four ports for the access network. You can choose to connect any number of these ports to the customer networking infrastructure. The S11 or S31 Node uses all the connected ports with the bonding mode selected for the network, either IEEE 802.3ad or active-backup.

You can use the HCP S Series Management Console or management API to set a connection expectation for each access network port. If a port that should be connected is not connected or if a port that should not be connected is connected, the S11 or S31 Node issues an alert.

Minimum Transport Layer Security (TLS) version
HCP S Series Nodes support TLS versions 1.0, 1.1, and 1.2. With release 3.0 of the S Series Node, you can use the HCP S Series Management Console or management API to set the minimum TLS version that the S Series Node can use. For example, if you set the minimum TLS version to 1.1, the S Series Node accepts requests that use version 1.1 or 1.2 but rejects requests that use version 1.0.

Note: For a release 7.*x* HCP system to use an S Series Node, the S Series Node must have a minimum TLS version of 1.0.

Revamped storage statistics
In release 3.0 of the HCP S Series Node, the HCP S Series Management Console **Dashboard** page has been updated. The page now shows this information:

- The total amount of storage that can be used for storing, protecting, and repairing object data and metadata.
- The amount of storage currently allocated for storing, protecting, and repairing object data and metadata, along with a ten-day history of this amount.
- The amount of storage that is currently available to be allocated for storing, protecting, and repairing object data and metadata.
- The amount of storage currently in need of repair, along with a ten-day history of this amount.

- The current storage efficiency. This value is a percent representing the ratio between the amount of data ingested for the objects currently stored on the S Series Node and the current amount of used storage on the S Series Node.

- The current percent of used storage out of total storage and the percent of storage that will be used after any outstanding repairs are complete.

The HCP S Series management API /metrics/system resource has been updated to return the new and revised current statistics and also to return a value representing the ideal storage efficiency for the S Series Node.

New bucket statistics
Release 3.0 of the HCP S Series Node includes this new information on the the Management Console **Buckets** page:

- The total amount of data written to the S Series Node for all objects currently in the existing buckets, along with a ten-day history of this amount

- The total number of objects currently in the existing buckets, along with a ten-day history of this amount

New HCP S Series Node Hardware Setup Tool
Release 3.0 of the HCP S Series Node comes with a new Hardware Setup Tool. The new Tool checks that:

- The S11 or S31 Node has the minimum required hardware.

- Each connected Ethernet port is functional.

- Hardware component firmware is at the expected version. If possible, the Tool updates firmware that is not at the expected version.

Using the Hardware Setup Tool is the only way to update firmware on an S11 or S31 Node.

Important notice

The deployment, management, and usage of an HCP S11 or S31 Node that has an expansion enclosure in addition to the base enclosure must follow these critical best practices to ensure the supportability of the S11 or S31 Node and to minimize the risk of data unavailability:

- Always mount the base enclosure and the expansion enclosure in the same rack.
- Always connect the base enclosure and the expansion enclosure to the same pair of power distribution units (PDUs) within the rack. If possible, the two PDUs should be connected to separate power sources.
- Never power off the expansion enclosure unless the base enclosure is powered off first or at the same time. Disconnecting both power cables from the expansion enclosure while the base enclosure is powered on can result in data unavailability and the possibility of data loss.

Additionally, if possible, all data stored on the S11 or S31 Node should be replicated to another HCP system so that the data exists in two physically separate locations.

HCP S Series Node document set

The following documents contain information about HCP S Series Nodes:

- *HCP S Series Node Help* (MK-HCPS022) — This Help system contains information about configuring and managing an HCP S11 or S31 Node. The Help includes information you need to effectively use the HCP S Series Management Console. The Help also describes the physical specifications of and environmental requirements for S11 and S31 Nodes. Additionally, the Help contains a complete reference for using the HCP S Series management API.
- *HCP S11 and S31 Node API Reference* (MK-HCPS023) — This book contains all the information you need to use the HCP S Series management API with an HCP S11 or S31 Node. This RESTful API enables you to configure, monitor, and manage an S11 or S31 Node programmatically.

- *HCP S11 and S31 Node Third-Party Copyrights and Licenses* (MK-HCPS024) — This book contains the copyright and license information for third-party and open source software that's incorporated into the HCP S Series operating system and software.

- *HCP S11 and S31 Node Assembly and Configuration* (FE-HCPS016) — This book contains complete instructions for building an HCP S11 and S31 Node. The book takes you from assembling component hardware to installing the HCP S Series software to packing components for shipping. The book also describes the physical specifications of and environmental requirements for S11 and S31 Nodes and includes information to help you troubleshoot issues that may arise during the assembly and configuration process.

- *HCP S11 and S31 Node On-site Setup* (FE-HCPS017) — This book contains all the information you need to deploy an HCP S11 or S31 Node at a customer site, from installing the S11 or S31 Node in a rack to configuring the S11 or S31 Node for the customer computing environment. The book also describes the physical specifications of and environmental requirements for S11 and S31 Nodes and contains information about configuring S11 and S31 Nodes in DNS and integrating S11 and S31 Nodes with the Hitachi Remote Ops monitor agent.

- *HCP S11 and S31 Node Maintenance* (FE-HCPS018) — This book contains instructions for maintaining the physical components of an HCP S11 or S31 Node, including instructions for adding drives and enclosures to increase capacity and for replacing faulty components.

- *HCP S Series Node Demo Edition Deployment* (FE-HCPS011) — This book contains all the information you need to deploy the HCP S Series Node Demo Edition. The Demo Edition is an S Series Node that runs in a virtual machine in VMware® Player™ or on a VMware ESXi™ host. The Demo Edition can be used to demonstrate the various S Series Node interfaces and APIs.

Upgrade notes

You an upgrade an HCP S11 and S31 Node to release 3.0.1 only from release 3.0. You cannot upgrade to release 3.0.1 from any release earlier than 3.0.

You cannot downgrade an S Series Node to an earlier release.

Important: The upgrade to release 3.0.1 is mandatory for existing S Series Nodes that are at release 3.0.

Hitachi Vantara has tested and supports the HCP S Series software and operating system upgrade listed in the table below.

Release upgrade	From	To
Release 3.0 to 3.0.1 (mandatory upgrade)	Software: 3.0.0.10 OS: 3.0.0.1218	Software: 3.0.1.9 OS: 3.0.0.1218

Supported browsers

The table below lists the web browsers that are qualified for use with the HCP S Series Management Console. Other browsers or versions may also work.

Browser	Client operating system
Microsoft® Internet Explorer® 11	Microsoft Windows®
Mozilla® Firefox® (latest version as of July 2019)	Apple® macOS® Microsoft Windows Linux®
Google® Chrome™ (latest version as of July 2019)	Apple macOS Chrome OS™ Microsoft Windows Linux

Note: To correctly display the HCP S Series Management Console, the browser window must be at least 1,024 pixels wide by 768 pixels high.

Supported hardware

The table below lists the hardware supported for use in HCP S11 and S31 Nodes.

Component	Vendor	Model	Replacement part number
Base enclosure	Seagate®	Cobra+ 4U100	SGH-4U100-NCL-AX.X
Expansion enclosure	Seagate	Cobra+ 4U106	SGH-4U106-NCL-AX.X
Server module (S11 Node)	Seagate	Rockingham	SGH-S11-CTLB-AX.X
Server module (S31 Node)	Seagate	Rockingham	SGH-S31-CTLB-AX.X
OS SSD (256GB M.2 SSD)	Innodisk®	DGM28-B56D81BCBQC-SGA	SGH-M2SD25-AX.X
Four-port SAS PCIe card	Broadcom®	SAS9305-16e	05-25704-00.X
Four-port 10GBase-T Ethernet PCIe card	Intel®	X710-T4	X710T4BLK.X
10TB data drive	Seagate	ST10000NM0096 (Tatsu)	SGH-LFHD10-AX.X
14TB data drive	Seagate	ST14000NM0048 (MobulaBP)	SGH-LFHD14-AX.X
16TB data drive	Seagate	ST16000NM002G (Evans)	SGH-LFHD16-AX.X
400GB database drive	Seagate	XS400LE10003 (Jofa)	SGH-LFSD40-AX.X SGH-SFSD40-AX.X
800GB database drive	Seagate	XS800LE70004 (Lange)	SGH-LFSD80-AX.X SGH-SFSD80-AX.X

Supported firmware versions

The table below lists the supported firmware versions for hardware components of HCP S11 and S31 Nodes.

Component	Firmware version
Base enclosure	5250
Expansion enclosure	524A
Personality module controller	07.00.00.00

(Continued)

Component	Firmware version
Personality module SAS expander	5.2.0.76
Server module BIOS	0.01.0032
Server module BMC	0.00.002f
OS SSD	M16225t
Intel I210 chip for the management and server interconnect networks	3.25
Four-port SAS PCIe card	16.00.01.00
Four-port 10GBase-T Ethernet PCIe card	6.128 (6.80 NVMupdate)
10TB data drive (Seagate ST10000NM0528)	E002
10TB data drive (Seagate ST10000NM0096)	E005
14TB data drive (ST14000NM0048)	E002
16TB data drive (ST16000NM002G)	E002
400GB database drive (Seagate XS400LE10003)	0003
400GB database drive (Seagate ST400FM0303)	0007
800GB database drive (XS800LE70004)	E002

Supported platforms for the HCP S Series Node Demo Edition

The HCP S Series Node Demo Edition runs on these platforms:

- VMware Player version 7.0 or later
- VMware ESXi version 5.1 Update 2
- VMware ESXi version 5.5

Note: The Demo Edition is a release 2.0 S Series Node.

Resolved issues

The following sections describe previously identified HCP S Series Node issues that are now resolved.

Issues resolved in this release

The table below lists previously identified HCP S Series Node issues that have been resolved in the current release. The issues are listed in order by reference number.

Ref. number	SR number	Description
RNO-4115	-	**Upgrade failure due to second reboot of first server module to be upgraded** During an HCP S Series software upgrade, if the server module that was upgraded first reboots while the second server module is being upgraded, the upgrade fails. If you try to restart the upgrade, it fails again. **Fix:** After an upgrade failure due to the first server module to be upgraded rebooting during the upgrade of the second server module, restarting the upgrade no longer causes the upgrade to fail.
RNO-4546 RNO-5451 RNO-6012	04458254 04506478 00647682 00689285 00804348	**Repeated restarts due to multiple writes of same data** When the same data is written to an S Series Node a very large number of times, S Series Node performance degrades. If the same data continues to be written, the S Series Node eventually goes into a cycle of failing and restarting. To recover from this situation, in HCP, delete a large number of the objects with that data. **Fix:** The S Series Node now processes duplicate objects in small batches. The result of this change is that multiple writes of the same data no longer cause performance to degrade or the S Series Node to fail.
RNO-6002	-	**No software restart after enclosure 1 replacement** As part of the procedure for replacing enclosure 1, both server modules must be shut down. After the enclosure is physically replaced, the HCP S Series software does not successfully restart on either module. **Fix:** The HCP S Series software now restarts successfully on both server modules after a replacement of enclosure 1.

(Continued)

Ref. number	SR number	Description
RNO-6013	-	**Unavailable drives due to server module restart during enclosure 2 recovery from unavailability** If a server module restarts while enclosure 2 is recovering after being unavailable, one or more drives in the enclosure that were previously available may be unavailable when the enclosure becomes available again. **Fix:** A server module restart while enclosure 2 is recovering after being unavailable no longer causes previously available drives to become unavailable.

Issues resolved in release 3.0

The table below lists previously identified HCP S Series Node issues that were resolved in release 3.0. The issues are listed in order by reference number.

Ref. number	SR number	Description
RNO-4102	-	**Extra messages about beaconing on and off while beaconing is on** While beaconing is on for an S Series Node component, messages about beaconing being turned on and turned off for that component are written to the event log every ten minutes. The messages stop when beaconing is turned off for the component. **Fix:** The extra beaconing messages were due to a timer issue that is now fixed.

(Continued)

Ref. number	SR number	Description
RNO-4704	-	**Add drives error reported with reused native drives** When you add native drives back to an S Series Node, you can choose to reuse the drives as is. Occasionally, with this choice, one of the server modules doesn't immediately recognize that the drives have been added. As a result, the S Series Node reports that the add drives operation finished with errors. However, within one or two seconds after the operation finishes, the server module in question automatically recognizes the added drives. No additional action is required. **Fix:** Before an add drives operation finishes, if any native drives have been reused, both server modules now recognize that the reused drives have been added.
RNO-4938	-	**Cannot disable allow when used in both lists for Management Console** On the **Configuration ► Console** page in the HCP S Series Management Console, after you enable the **Allow requests when same IP is used in both lists** option, you cannot disable that option. **Fix:** The allow list now includes 0.0.0.0/0 by default. As long as this CIDR value, your client IP address, or a different CIDR value that encompasses your client IP address is in the allow list, you can disable the **Allow requests when same IP is used in both lists** option.
RNO-5003	-	**CVEs: Java SE, Linux kernel, and glibc vulnerabilities** Java SE has these vulnerabilities: • CVE-2017-10053 — Allows unauthenticated remote attackers to cause a partial denial of service of Java SE. • CVE-2017-10067 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10074 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10078 — Allows low-privileged remote attackers to perform unauthorized create, modify, or delete operations on critical data or have complete access to all Java SE accessible data. • CVE-2017-10081 — Allows unauthenticated remote attackers, with interaction from another person, to perform unauthorized update, insert, or delete operations on some Java SE accessible data.

(Continued)

Ref. number	SR number	Description
		• CVE-2017-10086 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10087 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10089 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10090 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10096 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10101 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10102 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10104 — Allows low-privileged remote attackers to perform unauthorized update, insert, or delete operations on some Java Advanced Management Console accessible data, to have unauthorized read access to a subset of Java Advanced Management Console accessible data, and and to have the unauthorized ability to cause a partial denial of service of Java Advanced Management Console. • CVE-2017-10105 — Allows unauthenticated remote attackers, with interaction from another person, to perform unauthorized update, insert, or delete operations on some Java SE accessible data. • CVE-2017-10107 — Allows unauthenticated remote attackers, with interaction from another person, to interact with Java SE. • CVE-2017-10108 — Allows unauthenticated remote attackers to cause a partial denial of service of Java SE. • CVE-2017-10109 — Allows unauthenticated remote attackers to cause a partial denial of service of Java SE. • CVE-2017-10110 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE.

(Continued)

Ref. number	SR number	Description
		• CVE-2017-10111 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10114 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10115 — Allows unauthenticated remote attackers to have unauthorized access to critical data or complete access to all Java SE accessible data. • CVE-2017-10116 — Allows unauthenticated remote attackers, with interaction from another person, to take over Java SE. • CVE-2017-10117 — Allows unauthenticated remote attackers with HTTP access to have unauthorized read access to a subset of Java Advanced Management Console accessible data. • CVE-2017-10118 — Allows unauthenticated remote attackers to unauthorized access to critical data or complete access to all Java SE data. • CVE-2017-10121 — Allows unauthenticated remote attackers, with interaction from another person, to perform unauthorized update, insert or delete operations on some Java Advanced Management Console accessible data and to have unauthorized read access to a subset of Java Advanced Management Console accessible data. • CVE-2017-10125 — Allows attackers with physical access to take over Java SE. • CVE-2017-10135 — Allows unauthenticated remote attackers to have unauthorized access to critical data or complete access to all Java SE accessible data. • CVE-2017-10145 — Allows low-privileged remote attackers to perform unauthorized update, insert or delete operations on some Java Advanced Management Console accessible data, to have unauthorized read access to a subset of Java Advanced Management Console accessible data, and to cause a partial denial of service of Java Advanced Management Console. • CVE-2017-10176 — Allows unauthenticated remote attackers to have unauthorized access to critical data or complete access to all Java SE accessible data.

(Continued)

Ref. number	SR number	Description
		• CVE-2017-10193 — Allows unauthenticated remote attackers, with interaction from another person, to have unauthorized read access to a subset of Java SE accessible data. • CVE-2017-10198 — Allows unauthenticated remote attackers to have unauthorized access to critical data or complete access to all Java SE accessible data. • CVE-2017-10243 — Allows unauthenticated remote attackers to have unauthorized read access to a subset of Java SE accessible data and the unauthorized ability to cause a partial denial of service of Java SE. The Linux kernel has this CVE: • CVE-2017-1000364 — Allows bypass of a stack guard page that is too small. glibc has this CVE: • CVE-2017-1000366 — Allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. **Fix:** HCP S Series Nodes are no longer affected by these vulnerabilities. For more information on these CVEs, see: • https://nvd.nist.gov/vuln/detail/CVE-2017-10053 • https://nvd.nist.gov/vuln/detail/CVE-2017-10067 • https://nvd.nist.gov/vuln/detail/CVE-2017-10074 • https://nvd.nist.gov/vuln/detail/CVE-2017-10078 • https://nvd.nist.gov/vuln/detail/CVE-2017-10081 • https://nvd.nist.gov/vuln/detail/CVE-2017-10086 • https://nvd.nist.gov/vuln/detail/CVE-2017-10087 • https://nvd.nist.gov/vuln/detail/CVE-2017-10089 • https://nvd.nist.gov/vuln/detail/CVE-2017-10090

(Continued)

Ref. number	SR number	Description
		• https://nvd.nist.gov/vuln/detail/CVE-2017-10096 • https://nvd.nist.gov/vuln/detail/CVE-2017-10101 • https://nvd.nist.gov/vuln/detail/CVE-2017-10102 • https://nvd.nist.gov/vuln/detail/CVE-2017-10104 • https://nvd.nist.gov/vuln/detail/CVE-2017-10105 • https://nvd.nist.gov/vuln/detail/CVE-2017-10107 • https://nvd.nist.gov/vuln/detail/CVE-2017-10108 • https://nvd.nist.gov/vuln/detail/CVE-2017-10109 • https://nvd.nist.gov/vuln/detail/CVE-2017-10110 • https://nvd.nist.gov/vuln/detail/CVE-2017-10111 • https://nvd.nist.gov/vuln/detail/CVE-2017-10114 • https://nvd.nist.gov/vuln/detail/CVE-2017-10115 • https://nvd.nist.gov/vuln/detail/CVE-2017-10116 • https://nvd.nist.gov/vuln/detail/CVE-2017-10117 • https://nvd.nist.gov/vuln/detail/CVE-2017-10118 • https://nvd.nist.gov/vuln/detail/CVE-2017-10121 • https://nvd.nist.gov/vuln/detail/CVE-2017-10125 • https://nvd.nist.gov/vuln/detail/CVE-2017-10135 • https://nvd.nist.gov/vuln/detail/CVE-2017-10145 • https://nvd.nist.gov/vuln/detail/CVE-2017-10176 • https://nvd.nist.gov/vuln/detail/CVE-2017-10193 • https://nvd.nist.gov/vuln/detail/CVE-2017-10198 • https://nvd.nist.gov/vuln/detail/CVE-2017-10243

(Continued)

Ref. number	SR number	Description
		• https://nvd.nist.gov/vuln/detail/CVE-2017-1000364
RNO-5080	-	**CVE-2018-8037: Apache Tomcat vulnerability** An Apache Tomcat vulnerability allows the simultaneous completion of an async request and triggering of an async timeout to result in a user seeing a reposnse intended for a different user. **Fix:** HCP S Series Nodes are no longer affected by this vulnerability. For more information on this CVE, see https://nvd.nist.gov/vuln/detail/CVE-2018-8037.
RNO-5103	-	**CVE-2018-5390: Linux kernel vulnerability** A Linux kernel vulnerability allows the kernel to be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_ queue() for every incoming packet, which can lead to a denial of service. **Fix:** HCP S Series Nodes are no longer affected by this vulnerability. For more information on this CVE, see https://nvd.nist.gov/vuln/detail/CVE-2018-5390.
RNO-5128	-	**CVE-2018-11776: Apache Struts vulnerability** An Apache Struts vulnerability makes remote code execution possible when alwaysSelectFullNamespace is true. **Fix:** HCP S Series Nodes are no longer affected by this vulnerability. For more information on this CVE, see https://nvd.nist.gov/vuln/detail/CVE-2018-11776.

Known issues

The table below lists known issues in the current release of the HCP S Series Node. The issues are listed in order by reference number.

Ref. number	SR number	Description
RNO-2205	-	**Incorrect message in catalina.log when server interconnect network changes** When the subnet for the server interconnect network is changed, the server modules are automatically rebooted. During this reboot, a message with severity level SEVERE is written to the catalina.log file, indicating that an update of the IPv4 firewall failed. This message is false and can be safely ignored.
RNO-2266	-	**Alert misplaced for database drive degraded, resyncing, or recovering** The alert that indicates that a database drive is degraded or being resynced or recovered should appear on the details page for the enclosure. Instead, the alert appears on the details page for the applicable server module. Additionally in this case, on the details page for the applicable slot, the row that shows the status of the database partition is not highlighted in red.
RNO-2286	-	**Failed hotfix with powered-off server module** If a server module is powered off during the application of a hotfix, the hotfix application may fail. To recover from this situation, contact your HCP support center for help.
RNO-2287	-	**Time server IPv6 address truncated on server module details page** When the time server being used by the S Series Node is identified by an IPv6 address, the address is truncated in the **Time server** field in the **Core Hardware** section of the server module details page.
RNO-2375	-	**Beaconing off and on during early Sunday mornings** If beaconing is on for an enclosure or a component in an enclosure at 1:00 a.m. on a Sunday, for a brief period after that time, the event log may contain messages indicating that beaconing was turned off and back on a few times. At the end of this period, beaconing remains on.

(Continued)

Ref. number	SR number	Description
RNO-3387	-	**No restart of server module with unavailable database drives** If all the database drives for one server module become unavailable, both server modules may automatically reboot. When this happens, the HCP S Series software doesn't restart on the sever module with the unavailable database drives. To recover from this situation, you need to perform a database recovery operation. For instructions on doing this, contact your HCP support center.
RNO-4332	-	**Degraded read performance for new data on replacement drives** After a drive is replaced, read performance is degraded for objects with data on the new drive.
RNO-4623	-	**False report about unavailable server module during reboot of other server module** Rarely, while one server module is rebooting, the S Series Node incorrectly reports that the other server module is unavailable. A message about the unavailability is written to the event log, and an alert reporting the unavailability is briefly in effect (no more than a few seconds). Despite the report, the server module did not, in fact, become unavailable.
RNO-4942 RNO-5954	-	**Changed bucket owners identified by user ID in event log** When you change the owner of a bucket, the message in the S Series Node event log identifies the old and new bucket owners by their internal user IDs instead of by their usernames.
RNO-5094	-	**False report about MTU after changing network MTU to 9,000** After you change the MTU to 9,000 for the access or management network, the S Series Node falsely reports that a network interface is not operating at the correct MTU. A message about the incorrect operation is written to the event log, and an alert reporting the incorrect operation is briefly in effect (no more than two minutes). Despite the report, the MTU is operating at the correct MTU.
RNO-5207	-	**Prompt for translation with first-time setup wizard in Chrome** When you open the S Series Node first-time setup wizard as the first navigation in a new Google Chrome window, the browser may prompt for whether you want to translate the page. To access the first-time setup wizard, close the prompt.

(Continued)

Ref. number	SR number	Description
RNO-5258 RNO-5618	-	**"Enclosure not found" message with add enclosure procedure** If, in an add enclosure maintenance procedure, you connect a SAS cable to an incorrect port on the new enclosure, the operation fails with the message "Enclosure not found." This message is also returned for some other error conditions. If you see this message, check the SAS cabling. If the cabling is correct, the message is due to a different issue.
RNO-5300	-	**Inconsistent indication of broken SAS connection in diagrams** The diagrams on the enclosure details page show broken SAS connections by changing port colors. However, when you disconnect a SAS cable from enclosure 1, only the SAS port on enclosure 1 turns red. The port the cable is still connected to on the I/O module stays green. Similarly, when you disconnect a SAS cable from an I/O module, only the port on the I/O module turns red. The port on enclosure 1 stays green.
RNO-5310	-	**Object limit due to metadata storage** The S Series Node generates metadata for each object when the object is created. Currently, the S Series Node stores all this metadata on the base enclosure. As a result, when the storage on the base enclosure is full, no more objects can be stored on the S Series Node, even if storage space is available on the expansion enclosure.
RNO-5455	-	**Incorrect maintenance procedure page behavior after reload or navigation away and back** While performing a maintenance procedure, if you reload or navigate away from and then back to the maintenance procedure page after you have clicked Verify, the Done and Verify buttons are incorrectly active, and the page does not automatically refresh when the verification process is complete. In this case, to continue the procedure, you need to periodically refresh the page until the verification process is complete and the button for the next action you need to take is active. If, after reloading or returning to the maintenance procedure page, you click Verify again, the verification process restarts. In this case, when the verification process is complete, the page automatically refreshes.

(Continued)

Ref. number	SR number	Description
RNO-5489	-	**Continuous reboots caused by bad drive** Rarely, repeated write errors on a drive cause one server module to continuously reboot. To recover from this situation, take the drive out of the enclosure without performing a maintenance procedure. Then use a replace drives maintenance procedure to install a new drive in the slot from which you removed the bad drive.
RNO-5527	-	**Deny list with both IPv4 and IPv6 addresses ignored for Management Console access on IPv6 access network** While the access network IP mode is IPv6, if the deny list for access to the HCP S Series Management Console contains both IPv4 and IPv6 addresses, those addresses are not denied access to the Console on the access network.
RNO-5692	-	**Communication with DNS servers or time servers on management network disabled by change of access network to IPv6 mode** With the access network and management network both configured for IPv4 and the *management* network selected for communication with DNS servers or time servers, if you change the IP mode of the *access* network to IPv6, the S Series Node can no longer communicate with the DNS servers or time servers, as applicable, on the *management* network. To re-enable communication with the DNS servers or time servers on the management network, use the HCP S Series Management Console or management API to reboot the S Series Node.
RNO-5716	-	**Reinstalling after software installation failure** To try again to install the HCP S Series software after a software installation failure, you need to perform a reinstallation of both the HCP S Series OS and the software. If you try to install only the software without reinstalling the OS, the services software installation precheck may fail.
RNO-5723	-	**False report about unsupported fan hardware after enclosure power outage** When an enclosure powers back on after losing power, the S Series Node falsely reports that the fan hardware is unsupported for each rear fan and each controller-bay fan. Messages about the unsupported hardware are written to the event log, and alerts reporting the unsupported hardware are briefly in effect. The part number shown for each fan in the full message text is NO_PSN_PRE. Despite the reports, the fan hardware is still supported, and the fans are operating correctly.

(Continued)

Ref. number	SR number	Description
RNO-5758	-	**False report of eth4 down after management network monitoring is enabled** When you enable management network monitoring while the management port is connected to an active network, the S Series Node falsely reports that the eth4 network interface is down. A messsage about the condition is written to the event log, and an alert reporting the condition is in effect. Despite the report, the network interface is connected and operating correctly.
RNO-5783	-	**S Series Node enclosure warning condition reported on HCP** When a component fails in an S Series Node enclosure, the HCP system using the S Series Node receives a message indicating that the enclosure has a warning condition but does not receive a message indicating which component is causing the message. If you see this message on the HCP system, check the S Series Node for more information. The message may be due to an individual drive failure, which is reported at the informational level, not the warning level, on the S Series Node. A message about an individual data drive failure does not mean that the drive needs to be immediately replaced. Data drive replacement is necessary only when the S Series Node issues this alert: "*number-of-drives* data drives have failed or are unavailable."
RNO-5793	-	**False report about inaccessible BMC** Rarely, the S Series Node falsely reports that the BMC on a server module is inaccessible while the BMC is operating correctly. A message indicating that the BMC is inaccessible is written to the event log, and an alert reporting that condition is in effect for a short time. Despite the report, the BMC is accessible. If the alert doesn't clear within 15 minutes, contact your authorized service provider for help.
RNO-5807	-	**False report about power supply with critical status** Rarely, the S Series Node falsely reports that a power supply has a status of critical while the power supply is operating correctly. A message about the critical status is written to the event log, and an alert reporting the critical status is in effect. In response to a report about a power supply with a status of critical, try reseating the power supply. If the alert clears, the power supply is operating correctly. If the alert remains in effect, replace the power supply.

(Continued)

Ref. number	SR number	Description
RNO-5810	-	**Virtual IP address for one server module unavailable after VLAN ID change to zero** When you change the VLAN ID of the access network from a nonzero value to zero, the virtual IP address for one of the S Series Node server modules cannot be used to access the HCP S Series Management Console or to issue management API requests for approximately 10 to 15 minutes.
RNO-5815	-	**Drive not visible after being moved within two minutes during replace drives procedure** If, during a replace drives procedure, you remove a drive from a slot and then insert that drive into a different slot within two minutes, the S Series Node will no longer be able to see that drive. If the slot into which you inserted the drive was selected for the replace drives procedure, the messages resulting from the verification step of the procedure include "Drive not found" for that slot. If the slot was not selected for the replace drives procedure, the messages do not contain any information about the slot. If you remove drives from multiple slots and then insert each of those drives into a different slot within two minutes, the verification messages include "Drive not found" for the first slot into which you inserted one of those drives but may not include that message for the other slots. After the replace drives procedure is complete, an alert reports that the slot has a status of installed, and the enclosure diagram in the HCP S Series Management Console shows the slot as empty. To enable the S Series Node to see the drive: **1.** Use the Management Console or management API to reboot one server module. **2.** After that server module becomes available, use the Management Console or management API to reboot the other server module.
RNO-5826	-	**Active fields grayed on network details pages** On the details page for the access network, the **Duplex**, **Bonding Mode**, and **MTU** fields are grayed, making those fields appear to be inactive. Similarly, on the details page for the management network, the **MTU** field is grayed, making that field appear to be inactive. In fact, these fields are active, and you can select values in them.

(Continued)

Ref. number	SR number	Description
RNO-5837	-	**Slow server module start after management-network update** Rarely, when an S Series Node reboots following a management-network update, one server module takes up to an hour to start.
RNO-5839	-	**No access with primary virtual IP addresses on access network after removing secondary virtual IP addresses** If you remove existing secondary virtual IP addresses from the access network, accessing the S Series Node by using a primary virtual IP address on the access network is no longer possible. To re-enable access with the primary virtual IP addresses, reboot the S Series Node.
RNO-5844	-	**Serial number not modifiable in first-time setup wizard after first specification** When you use the S Series Node first-time setup wizard to configure an S Series Node, if the S Series Node serial number has not yet been set, you can specify a serial number on the **Identification** page. However, if you click **Next** and then click **Back** to return to the **Identification** page, entering a different serial number results in an error when you click **Next** again.
RNO-5856	-	**Uninformative error message on HCP when S Series Node TLS is higher than 1.0** If you try to add an S Series Node to a release 7.*x* HCP system, where the minimum TLS version on the S Series Node is higher than 1.0, an error occurs on the HCP system. The error message displayed in the HCP System Management Console is "peer is not authenticated." This message is also displayed for other types of errors. If you see this message, check the minimum TLS version setting on the S Series Node. If the setting is 1.0, a different error has occurred.

(Continued)

Ref. number	SR number	Description
RNO-5858	-	**Unavailable drives reported after enclosure power outage ends** When an enclosure loses power, the available drives on the enclosure become unavailable, and the S Series Node reports that drives need to be replaced. When the enclosure powers back on, the drives that became unavailable due to the power outage become available again. At the point when the number of drives that have not yet become available plus the number of drives that were already unavailable or failed before the power outage goes below the threshold for requiring drive replacement, the S Series Node writes a message to the event log indicating that a drive replacement is no longer needed. The message specifies the number of drives that remain unavailable or failed. After an enclosure power outage, this message can be safely ignored. The drives that are still unavailable due to the power outage continue to become available.
RNO-5909 RNO-5947	-	**Persistent irreparable objects after brief expansion-enclosure power outage** Occasionally, after an expansion enclosure experiences a power outage that lasts less than 90 seconds, the S Series Node may report some number of irreparable objects. Although the objects are reported as irreparable, the S Series Node may be able to repair some or all of them. If, at two hours after a brief expansion-enclosure power outage, an irreparable objects alert is still in effect, contact your HCP support center for help. Manual intervention may be required for repair of the remaining objects.
RNO-5933	-	**Internal VLAN IDs not shown clearly in Management Console** For internal purposes, the S Series Node uses VLAN IDs of either 700 and 800 or 701 and 801. To determine which pair of VLAN IDs is being used internally, check the network interface name for the server interconnect network in the **Network Interfaces** section on the server module details page in the HCP S Series Management Console. If the name is eth4.800, VLAN IDs 700 and 800 are in use. If the name is eth4.801, VLAN IDs 701 and 801 are in use.

(Continued)

Ref. number	SR number	Description
RNO-5941	-	**Hardware Setup Tool failure to copy logs** If the HCP S Series Node Hardware Setup Tool cannot copy its log files to the FAT32-formated, nonbootable USB flash drive made available for that purpose, the Tool displays a command prompt. You can then use these steps to copy the log files yourself: **1.** Remove the FAT32-formatted USB flash drive from the USB hub. **2.** Either insert a different FAT32-formated, nonbootable USB flash drive into an available port on the USB hub, or reformat the drive you removed and then reinsert that drive into an available port on the hub. **3.** Enter this command at the command prompt: copy_log
RNO-5943	-	**Writes not accepted after enclosure 2 unavailability** Occasionally, after enclosure 2 becomes available again after being unavailable, the S Series Node stops accepting write requests.
RNO-5946	-	**Hardware Setup Tool log files overwritten on USB flash drive** The HCP S Series Node Hardware Setup Tool log files are named `hardware_setup_4u100.log`, `hardware_setup.log`, and `dmesg`. The Tool copies these files to a directory named `hardware_setup_log_`*`server-module-serial-number`* on the FAT32-formated, nonbootable USB flash drive made available for that purpose, where *`server-module-serial-number`* is the serial number of the server module on which you ran the Tool. Because the log directory and file names don't change, if you run the Hardware Setup Tool again on a server module and use the same USB flash drive for the log files, the new log files overwrite the log files from the previous run.

Accessing product documentation

Product 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.

Engineering change notification (ECN)

The ECN for HCP S Series Node release 3.0.1 is available at:

https://support.hds.com/en_us/user/ecn/engineering-change-notice.html

Getting help

Hitachi Vantara Support Portal 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.

Note: If the customer purchased the HCP S Series Node from a third party, please contact the applicable HCP support center.

Comments

Please send us your comments on this document:

HCPDocumentationFeedback@HitachiVantara.com

Include the document title and part number, including the revision (for example, -01), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you!

Hitachi Vantara

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

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact