

Hitachi Content Platform S Series Node

3.2.0

HCP S11 and S31 Node Help

This document is a PDF version of the Help that is built into the HCP S Series Management Console for HCP S11 and S31 Nodes. The Help contains information about configuring, monitoring, and managing an S11 or S31 Node. The Help also describes the physical specifications of and environmental requirements for S11 and S31 Nodes.

© 2019, 2023 Hitachi Vantara LLC. 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.

AIX, 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, z15, z16, 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.

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

Contents

Preface	7
Intended audience.....	7
Product version.....	7
Release notes.....	7
Related document.....	7
Document conventions.....	8
Terminology.....	9
Accessing product documentation.....	9
Getting help.....	9
Comments.....	9
Chapter 1: HCP S Series Nodes	10
Chapter 2: HCP S Series Management Console	11
HCP S Series Management Console URLs.....	11
Management Console page refresh.....	12
Management Console usage considerations.....	13
Chapter 3: Concepts and configuration	14
User accounts.....	14
User account credentials.....	14
Usernames.....	15
Passwords.....	16
User account properties.....	17
User roles.....	17
Permissions granted by roles.....	20
Considerations for working with user accounts.....	23
S Series objects.....	24
Object protection.....	24
Object repair.....	25
Effect of enclosure unavailability.....	25
Effect of adding a fifth enclosure.....	25
Buckets.....	26
Bucket names.....	26
Bucket owners.....	27

Bucket information.....	27
Considerations for working with buckets.....	27
Networking.....	28
Server-module Ethernet ports.....	28
Access network.....	31
Access network IP addresses.....	33
Access network properties.....	34
Management network.....	36
Management network IP addresses.....	36
Management network properties.....	37
Server interconnect network.....	39
Considerations for working with networks.....	39
Transport Layer Security (TLS).....	40
HCP S Series Node identification.....	40
HCP S Series software version.....	41
Licensing.....	42
DNS servers.....	42
Time servers.....	43
Client access.....	44
Management Console configuration.....	44
Management API configuration.....	45
Data access protocol configuration.....	46
Access control list.....	46
SSL server certificates.....	47
Generating a CSR and installing the returned certificate.....	48
Installing an SSL server certificate that's in a PKCS12 file.....	50
Generating and installing a new self-signed SSL server certificate.....	50
Security settings.....	50
Ping.....	51
SSH.....	51
User-account security.....	52
Password requirements and user-account management rules.....	52
Options for password requirements.....	52
Options for user-account management rules.....	55
Common-password dictionary.....	56
SSH keys.....	58
Viewing SSH key information.....	59
Installing exclusive SSH keys.....	59
Revoking exclusive SSH keys.....	60
Chapter 4: DNS configuration.....	62
Zone definitions for an S Series Node.....	62

Configuring a forward lookup zone in Windows.....	63
Creating a forward lookup zone for an S Series Node.....	63
Adding host entries to a forward lookup zone.....	64
Configuring a forward lookup zone in Unix.....	65
Verifying the DNS configuration.....	66
Chapter 5: HCP S11 and S31 Node hardware.....	67
S11 and S31 Node hardware components.....	67
S11 and S31 Node product offerings.....	71
Racking options.....	75
Connectivity options.....	76
Mechanical details.....	77
Enclosure dimensions.....	77
Enclosure weights.....	79
Rack dimensions.....	80
Rack and PDU weights.....	80
Electrical details.....	81
Power system.....	81
Electrical connections.....	82
PDUs.....	82
Power connections.....	83
Electrical specifications.....	83
Environmental details.....	85
RoHS compliance.....	85
BNST compliance.....	85
Temperature, humidity, and altitude.....	85
Shock and vibration.....	86
Cooling and airflow.....	86
Acoustics.....	87
Chapter 6: Monitoring HCP S11 and S31 Nodes.....	88
Dashboard.....	89
Total storage.....	89
Used storage.....	90
Available storage.....	91
Reserved for repair.....	92
Under repair.....	93
Storage efficiency.....	94
Storage-usage bar.....	96
Dashboard graphs.....	96
Resource load.....	97
Resource-load statistics collection.....	97

Resource-load statistics.....	98
System load.....	99
System-load statistics collection.....	100
System-load statistics.....	100
Historical system-load statistics.....	103
Event log.....	103
Alerts.....	104
Syslog logging.....	105
Configuring syslog logging.....	105
Testing syslog server connections.....	106
Management Console hardware information.....	107
Enclosure details.....	107
Server module details.....	111
Physical component status indicators.....	112
Enclosure front LEDs.....	112
Rear SAS port LEDs (base enclosure only).....	115
Power supply LEDs (base enclosure).....	115
Power supply LED (expansion enclosure).....	116
Rear fan LED.....	117
Controller-bay fan LED (base enclosure).....	117
Controller-bay fan LED (expansion enclosure).....	118
Personality module LEDs.....	118
SAS expander LEDs.....	120
Server module LEDs.....	121
I/O module LEDs.....	124
Drive LEDs.....	126
Beaconing.....	126
Internal logs.....	127
Inserting comments into the internal logs.....	128
Downloading the internal logs.....	128
Chapter 7: Managing server modules.....	130
Chapter 8: Maintaining HCP S Series Nodes.....	132
Chapter 9: Alerts and event log messages.....	134
Chapter 10: Supported limits.....	188

Preface

This document is a PDF version of the Help that is built into the HCP S Series Management Console for HCP S11 and S31 Nodes. The Help contains information about configuring, monitoring, and managing an S11 or S31 Node. The Help also describes the physical specifications of and environmental requirements for S11 and S31 Nodes.

Intended audience

This document is intended for people who work with HCP S11 and S31 Nodes and who want to use the HCP S Series Management Console to configure, monitor, and manage an HCP S11 or S31 Node. This audience includes:

- S Series Node administrators and monitors
- Authorized S Series Node service providers

This document assumes that you are familiar with basic computer-storage concepts.

Product version

This book applies to release 3.2.0 or later of the HCP S Series Node.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on the Hitachi Vantara Support Website: <https://knowledge.hitachivantara.com/Documents>.

Related document


HCP S11 and S31 Node API Reference (MK-HCPS023) contains all the information you need for using the HCP S Series management API with an HCP S11 or S31 Node. This RESTful HTTP-based API enables you to configure, monitor, and manage an S11 or S31 Node programmatically. The document explains how to use the management API to retrieve information about and manipulate S11 and S31 Node resources. The document also includes an introduction to the S Series Node concepts that underlie the management API resources.



Document conventions

This document uses the typographic conventions shown in the following table.

Convention	Description
Bold	<ul style="list-style-type: none"> Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. Indicates emphasized words in list items.
<i>Italic</i>	<ul style="list-style-type: none"> Indicates a document title or emphasized words in text. Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <pre>pairdisplay -g group</pre> <p>(For exceptions to this convention for variables, see the entry for angle brackets.)</p>
< > angle brackets	<p>Indicates variables in the following scenarios:</p> <ul style="list-style-type: none"> Variables are not clearly separated from the surrounding text or from other variables. Example: <pre>Status-<report-name><file-version>.csv</pre> Variables in headings.
[] square brackets	Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a b } indicates that you must choose either a or b.
vertical bar	<p>Indicates that you have a choice between two or more options or arguments. Examples:</p> <p>[a b] indicates that you can choose a, b, or nothing.</p> <p>{ a b } indicates that you must choose either a or b.</p>

This document uses the icons shown in the following table to draw attention to information.

Icon	Label	Description
	Note	Calls attention to additional information.

Icon	Label	Description
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.

Terminology

Throughout this Help, the word *Unix* is used to represent all UNIX-like operating systems (such as UNIX itself or Linux), except where Linux is specifically required.

Accessing product documentation

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

Getting help

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

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

Comments

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

Thank you!


Chapter 1: HCP S Series Nodes

A Hitachi Content Platform (HCP) S Series Node is a highly efficient, highly available, cost-effective storage device that supports very large amounts of data. Each S Series Node consists of two cooperating server modules and multiple high-density drives in some number of enclosures.

During normal operation, the two server modules in an S Series Node actively share responsibility for all S Series Node functions. Because the server modules are peers, if one module becomes unavailable, the other can still provide full, uninterrupted S Series Node functionality, although performance may be degraded.

The S Series Node data storage implementation ensures that data is well-protected through the use of erasure coding. Additionally, S Series Nodes use several internal processes to continuously check the integrity of both the stored data and the storage media.

S Series Nodes can provide direct-write storage for HCP systems and for HCP for cloud scale systems. S Series Nodes can also serve as storage tiering platforms for HCP systems. A single HCP system or HCP for cloud scale system can seamlessly store data across multiple S Series Nodes, thereby enabling scalability in both capacity and performance.

 **Important:** HCP and HCP for cloud scale are the only supported clients for the S Series Node.

HCP systems and HCP for cloud scale systems use the S Series Node implementation of the Hitachi API for Amazon S3 to write, retrieve, and otherwise manage objects in an S Series Node. This RESTful, HTTP-based API is compatible with Amazon S3.

For administrative purposes, S Series Nodes provide a web-based Management Console and a RESTful, HTTP-based management API. Using these interfaces, S Series Node administrators and service providers can configure, manage, and monitor an S Series Node. These interfaces can also be used to start and verify certain S Series Node hardware procedures, such as adding and replacing drives.

The current S Series Node models are the S11 Node and the S31 Node. The S31 Node has more processing power and memory than the S11 Node. Additionally, while the S11 Node supports at most two enclosures, the S31 Node can support as many as nine, thereby providing significantly more storage capacity than the S11 Node.

The older S Series Node models are the S10 Node and the S30 Node. The enclosures used in S11 and S31 Nodes can hold more drives than the enclosures used in S10 and S30 Nodes can hold. Also, S11 and S31 Nodes 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.

Chapter 2: HCP S Series Management Console

The HCP S Series Management Console is a web application that lets you monitor and manage an HCP S Series Node. The Management Console shows you the status of the S Series Node in real time so you can take action, when necessary, to ensure the health of the S Series Node. Through the Management Console, you can perform activities such as modifying S Series Node settings, configuring networks, and monitoring the usage of the S Series Node.

To use the Management Console, you need to log in with an S Series Node user account.

To log out of the Management Console, click the person icon (👤) in the upper right corner of the Management Console window. Then select Log Out.



Note: If the S Series Node is using a self-signed SSL server certificate, the Management Console does not work with Mozilla Firefox.

HCP S Series Management Console URLs

The URL for the HCP S Series Management Console can have either of these formats:

```
https://admin.node-domain-name:8000
```

```
https://ip-address:8000/admin
```

In these formats:

- *node-domain-name* is the fully qualified domain name of the S Series Node, as configured in DNS. When you use a URL with the domain name, the DNS response determines which server module the request is directed to.
- *ip-address* is either of:
 - The access network primary or secondary virtual IP address of either server module in the S Series Node
 - The management network IP address of either server module in the S Series Node

In either case, the applicable network must be enabled in the Management Console configuration.

Here's an example of a Management Console URL that uses a domain name:

```
https://admin.s-node-1.example.com:8000
```

Here's an example of a Management Console URL that uses an IPv4 address:

```
https://10.0.0.4:8000/admin
```

Here's an example of a Management Console URL that uses an IPv6 address:

```
https://[2001:0db8::101]:8000/admin
```

With IPv6, the IP address must be enclosed in square brackets.

If you use the S Series Node domain name or an access network virtual IP address and the server module to which the request is directed is unavailable, the request is automatically redirected to the other server module. If you use the physical IP address for a server module on the access or management network and the server module to which the request is directed is unavailable, the request fails.

If a client uses a `hosts` file to map S Series Node hostnames to IP addresses, the client system has full responsibility for converting any hostnames to IP addresses. In a `hosts` file, you can map any number of IP addresses to a single hostname. The way the client uses multiple IP address mappings for a single hostname depends on the client platform. For information about how your client handles these mappings, see your client documentation.

Regardless of whether you access the Management Console by domain name or by IP address, the Management Console must be configured to allow access from your client IP address.

S Series Nodes can support Management Console URLs that use HTTP without SSL security (requires port number 8001). This capability is provided so that the Console can accept requests passed on by load balancers that have terminated the SSL connection. Client requests for access to the Management Console should always use HTTPS, not HTTP, in the URL.



Note: HTTP access to the Management Console without SSL security is possible only if the Management Console is explicitly configured to allow it.

Management Console page refresh

Most HCP S Series Management Console pages do not automatically refresh themselves while they remain open. To see the most recent values on a page, click again on the option that opens that page.



Note: Using the browser reload button to refresh a page that lets you enter information causes the Management Console to resubmit values you previously entered on the page.

Management Console usage considerations

These considerations apply to the use of the HCP S Series Management Console:

- If a Management Console session is inactive for some amount of time, the session may end automatically. Whether the session ends automatically and the number of minutes of inactivity until the session ends are configurable.
- If you try to log in to the Management Console with an invalid password multiple times in a row, your user account may be disabled. Whether the account is disabled and the number of times you can try to log in with an invalid password before the account are disabled are configurable.
- If your user account is disabled due to multiple login attempts with an invalid password, the account may be automatically re-enabled after some number of minutes. Whether the account is automatically re-enabled and the number of minutes after which the account is re-enabled are configurable.
- If you try to log in to the Management Console with an invalid password, you may need to wait before you can try to log in again. Whether you need to wait and the number of seconds you need to wait are configurable.
- If you don't use your user account to access the S Series Node through any supported interface for some number of consecutive days, the account may be disabled. Whether the account is disabled and the number of days after which it is disabled are configurable.



Note: Only users with the security role can make the configuration changes identified above.

Chapter 3: Concepts and configuration

To work with an HCP S Series Node, you need to understand certain concepts. You also need to know which properties of an S Series Node you can configure.

User accounts

To access an HCP S Series Node, you need an S Series Node user account. A *user account* is a set of credentials that gives a user permission to use one or more of these interfaces:

- The HCP S Series Management Console
- The HCP S Series management API
- The Hitachi API for Amazon S3 (the S3 compatible API)

Permissions are granted by the roles associated with a user account.


An S Series Node can have at most 10,000 user accounts.

If you have the administrator or security role, you can use the Management Console or management API to view a list of user accounts. If you have the security role, you can use the Management Console or management API to create, modify, and delete S Series Node user accounts.

To work with user accounts in the Management Console, go to System > User Accounts.

User account credentials

User account credentials consist of a username and password. You can use the HCP S Series Management Console or management API to change the password for your own user account at any time. An S Series Node user with the security role can change the password for any user account at any time.

 **Important:** Passwords for S Series Node user accounts created by HCP systems are generated automatically and are not known to administrators of those systems. If you change the password for such a user account, the applicable system will no longer be able to manage or report on its usage of the S Series Node storage.

Normally, user account passwords expire after a configurable amount of time. However, security administrators can configure individual user accounts so that the password never expires automatically or so that the password expires immediately. A password that is set to expire immediately expires regardless of whether it's subject to automatic expiration.

If your user account password expires, you can use an interface that requires password access only to change that password. An expired password does not prevent the user account from being used for data access with the S3 compatible API.

For you to use the S3 compatible API, your user account must have the data role and additional credentials that consist of an access key and secret key. You can use the Management Console or management API to generate these credentials. However, for you to generate the credentials, your user account must have the data role. Only you can generate the S3 compatible API credentials for your user account.

After generating your S3 compatible API credentials, store the access key and secret key in a secure location. You can use the Management Console or management API to retrieve your access key, but the S Series Node does not provide a way for you to retrieve your secret key.



Note: The only supported users of the S Series Node S3 compatible API are HCP systems and HCP for cloud scale systems.

Access keys and secret keys do not expire. However, if you lose these keys, you can generate new ones. As soon as you generate new keys, the old keys stop working.

To use the Management Console to change your password or generate new keys for the S3 compatible API, click the person icon (👤) in the upper right corner of the Management Console window. Then select the action you want to take.

Usernames

As a security administrator, you can create S Series Node user accounts. When you create a user account, you specify a username for the account. The username uniquely identifies that account on the S Series Node.

Usernames:

- Must be 3 through 128 characters long
- Can contain only valid UTF-8 characters
- Cannot contain uppercase letters
- Cannot contain an opening angle bracket (<) or closing angle bracket (>)
- Cannot start with an opening square bracket ([) or closing square bracket (])
- Cannot contain white space
- Must be unique for the current S Series Node

Additionally, the following strings are reserved and cannot be used as usernames:

- allusers
- authenticatedusers
- internal
- logdelivery
- <http://acs.amazonaws.com/groups/global/allusers>

- <http://acs.amazonaws.com/groups/global/authenticatedusers>
- <http://acs.amazonaws.com/groups/s3/logdelivery>

You can reuse usernames that are not currently in use. For example, if you delete the account for a user, you can create a new account for that user with the same username as the deleted account had.

Passwords

When creating an S Series Node user account, the security administrator specifies a password for the account. You can change your account password at any time. You must change your password if the account password expires.

To use the HCP S Series Management Console to change your password, click the person icon (👤) in the upper right corner of the Management Console window. Then select Change Password.



Important: To prevent other users from using your user account to access the S Series Node, do not share your password with anyone.

Passwords must follow certain rules, some of which are configurable by users with the security role. When a password is changed, it must conform to the password rules that are currently in effect.

Passwords:

- Can be at most 64 characters long.
- Cannot be shorter than the configured minimum password length, which cannot be less than 6.
- Can contain any valid UTF-8 characters.
- Can include white space.
- Are case sensitive.
- Must include at least the configured minimum number of characters from each of these character sets:
 - Uppercase letters: A through Z
 - Lowercase letters: a through z
 - Numbers: 0 through 9
 - Special characters: `~!@#\$\$%^&* ()_+={}[]\|:;'"<> ,.?!/

If the configured minimum number of characters for a character set is zero, passwords can, but do not have to, include characters from that set.



Tip: The longer the password, the stronger it is likely to be. Using a mix of uppercase and lowercase letters, numbers, and special characters creates an even stronger password.

- May be blocked from including the username for the user account. This restriction is configurable.

The username check is case insensitive.

- May be blocked from being any string defined as a common password on the S Series Node. This restriction is configurable.

The common-password check is case insensitive.

When changing the password for a user account, you cannot re-use the current password or the configured number of most recent passwords.

When password rules change, passwords for existing user accounts remain valid until those passwords expire or are changed, even if the passwords don't conform to the new rules.

When a nonconforming password is changed, however, the new password must conform to the new rules.

After an S Series Node is upgraded to release 3.2.0 or later from a release earlier than 3.2.0, passwords for pre-existing user accounts remain valid until they expire or are changed. When the password for a pre-existing account is changed, the new password must conform to the password rules currently in effect.

User account properties

In addition to a username and password, user accounts have these properties:

- Full name. The full name can be used to identify the user for whom the account was created. This name must be 1 through 256 characters long and can contain any valid UTF-8 characters, including white space.
- Description (optional). The description can be at most 1,024 characters long and can contain any valid UTF-8 characters, including white space.
- Whether the account is enabled or disabled. While an account is disabled, it cannot be used for any purpose.

User accounts can be disabled automatically due to consecutive failed login attempts. As a security administrator, you might choose to disable a user account manually, for example, while the user for whom you created the account is on leave.

- Whether the password for the account expires automatically based on the S Series Node security setting for password expiration.
- Whether the account password must be changed before the account can be used for any purpose other than to change the password (that is, whether the password has expired).
- Roles that determine which interfaces the user can use with the user account and what the user can do with those interfaces. Every user account must be associated with at least one role.

User roles

A *role* is a named collection of permissions that can be associated with an S Series Node user account. The roles associated with a user account determine which S Series Node interfaces the user can use and what the user can do with those interfaces. Roles generally correspond to job functions.

Each user account must be associated with one or more roles. The account user has all the permissions granted by each of the associated roles.

The roles that you can associate with a user account are listed below.

Administrator

Grants permission to use the HCP S Series Management Console and management API to:

- View S Series Node configuration, status, and current and past storage-usage, system-load, and resource-load statistics.
- Perform configuration activities (such as changing server module IP addresses).
- View information about the currently active SSH keys.
- View the user account list and bucket list.
- Create, modify, and delete buckets and view the list of irreparable objects in those buckets.
- Power server modules off and on.
- View messages in the event log except for security event messages.
- Insert comments into and download the S Series Node internal logs.

The administrator role does not grant permission to:

- View, create, or manage individual user accounts.
- View or configure security options.
- Install or revoke exclusive SSH keys.
- Store, retrieve, or manage objects in buckets.
- Perform hardware maintenance procedures or update the HCP S Series operating system and software.

Monitor

Grants permission to use the HCP S Series Management Console and management API to:

- View S Series Node configuration, status, and current and past storage-usage, system-load, and resource-load statistics.
- View information about the currently active SSH keys.
- View the bucket list and the list of irreparable objects in those buckets.
- View messages in the event log except for security event messages.
- Insert comments into the S Series Node internal logs.

The monitor role does not grant permission to:

- Perform configuration activities.
- View, create, or manage user accounts.
- View or configure security options.

- Install or revoke exclusive SSH keys.
- Create, modify, or delete buckets.
- Store, retrieve, or manage objects in buckets.
- Power server modules off or on.
- Perform hardware maintenance procedures or update the HCP S Series operating system and software.
- Download the S Series Node internal logs.

Security

Grants permission to use the HCP S Series Management Console and management API to:

- View, create, and manage user accounts.
- Configure security options (such as enabling SSH access to the S Series Node and setting password requirements).
- Install and revoke exclusive SSH keys.
- View information about the currently active SSH keys.
- View security event messages in the event log (such as messages about unsuccessful attempts to log in to the HCP S Series Management Console).
- Insert comments into the S Series Node internal logs.

The security role does not grant permission to:

- View S Series Node configuration, status, and current and past storage-usage, system-load, and resource-load statistics.
- View configuration options that are not related to security.
- Perform configuration activities that are not related to security.
- View the bucket list or the list of irreparable objects in those buckets.
- Store, retrieve, or manage objects in buckets.
- Power server modules off or on.
- Perform hardware maintenance procedures or update the HCP S Series operating system and software.
- View messages in the event log that are not related to security.
- Download the S Series Node internal logs.



Tip: Always have at least two user accounts that have the security role. This configuration ensures that if one of the accounts with the security role becomes disabled, another account that can manage user accounts still exists.

Service

Grants permission to use the HCP S Series Management Console and management API to:

- View S Series Node configuration, status, and current and past storage-usage, system-load, and resource-load statistics.
- Perform most configuration activities.
- Install and revoke exclusive SSH keys.
- View information about the currently active SSH keys.
- View the bucket list and the list of irreparable objects in those buckets.
- Power server modules off or on.
- Perform hardware maintenance activities (such as replacing a failed drive).
- Update the HCP S Series operating system and software.
- View messages in the event log that are not related to security.
- Insert comments into and download the S Series Node internal logs.

The service role does not grant permission to:

- View, create, or manage user accounts.
- View or configure security options.
- Create, modify, or delete buckets.
- Store, retrieve, or manage objects in buckets.



Note: You should associate the service role only with user accounts created for authorized service providers.

Data

Grants permission to use the Hitachi API for Amazon S3 (the S3 compatible API) to:

- Create and manage buckets.
- View a list of the buckets you own.
- Store, retrieve, and manage objects in buckets.

With this role, you can also use the Management Console or management API to generate your S3 compatible API access key and secret key.

All users can use the HCP S Series Management Console and management API to change their own passwords.

Permissions granted by roles

The table below lists activities that can be performed using the S Series Node interfaces and indicates which roles grant permission to perform each of those activities. The column headings for the roles are Adm. (administrator), Mon. (monitor), Sec. (security), Serv. (service), and Data. Unless otherwise indicated, you can perform each activity both in the HCP S Series Management Console and by using the management API.

Activity	Adm.	Mon.	Sec.	Serv.	Data
Perform the initial configuration of the S Series Node (restricted to authorized service providers; no credentials needed; can be successfully done only once)	—	—	—	—	—
View the default settings for the initial configuration of the S Series Node (restricted to authorized service providers; no credentials needed; cannot be done after the initial configuration is complete)	—	—	—	—	—
Log in to the HCP S Series Management Console	✓	✓	✓	✓	✓
View the user account list	✓	X	✓	X	X
View an individual user account	X	X	✓	X	X
Create, modify, and delete user accounts	X	X	✓	X	X
View the rules for passwords	✓	✓	✓	✓	✓
Change your password	✓	✓	✓	✓	✓
Generate your S3 compatible API access key and secret key	X	X	X	X	✓
View your S3 compatible API access key	X	X	X	X	✓
View the bucket list	✓	✓	X	✓	X
View a list of the buckets you own (S3 compatible API only)	X	X	X	X	✓
View an individual bucket with the Management Console or management API	✓	X	X	X	X
View an individual bucket with the S3 compatible API	X	X	X	X	✓
Create, modify, and delete buckets with the Management Console or management API	✓	X	X	X	X
Create and delete buckets with the S3 compatible API	X	X	X	X	✓
Create, manage, and delete objects (S3 compatible API only)	X	X	X	X	✓
View a list or count of irreparable objects in a bucket (management API only)	✓	✓	X	✓	X
View a list or count of all irreparable objects (management API only)	✓	✓	X	✓	X
View the network list	✓	✓	X	✓	X
View an individual network	✓	✓	X	✓	X
Modify a network	✓	X	X	✓	X

Activity	Adm.	Mon.	Sec.	Serv.	Data
View the minimum TLS version setting	✓	✓	X	✓	X
Modify the minimum TLS version setting	✓	X	X	✓	X
View the S Series Node domain name, serial number, and software version	✓	✓	✓	✓	✓
Modify the S Series Node domain name	✓	X	X	✓	X
View S Series Node license information	✓	✓	X	✓	X
View the Management Console configuration	✓	✓	X	✓	X
View the Management Console login message	✓	✓	✓	✓	✓
Configure the Management Console	✓	X	X	✓	X
View the management API configuration	✓	✓	X	✓	X
Configure the management API	✓	X	X	✓	X
View the data access protocol list (management API only)	✓	✓	X	✓	X
View the S3 compatible API configuration	✓	✓	X	✓	X
Configure the S3 compatible API	✓	X	X	✓	X
View the currently installed SSL server certificate	✓	✓	X	✓	X
Generate and install a self-signed SSL server certificate, install a certificate created outside the S Series Node, or generate a certificate signing request and install the returned certificate	✓	X	X	X	X
View and configure S Series Node security settings	X	X	✓	X	X
View information about the currently active SSH keys	✓	✓	✓	✓	X
Install and revoke exclusive SSH keys	X	X	✓	✓	X
View the lists of DNS servers and time servers	✓	✓	X	✓	X
Modify the lists of DNS servers and time servers	✓	X	X	✓	X
View current and historical storage-usage and repair statistics	✓	✓	X	✓	X
View resource-load statistics (management API only)	✓	✓	X	✓	X
View current and historical system-load statistics (management API only)	✓	✓	X	✓	X
View the event log except for security events	✓	✓	X	✓	X
View security events in the event log	X	X	✓	X	X

Activity	Adm.	Mon.	Sec.	Serv.	Data
View alerts that are currently in effect	✓	✓	✓	✓	X
View any current S Series Node status messages	✓	✓	✓	✓	✓
View the syslog logging configuration	✓	✓	X	✓	X
Configure syslog logging	✓	X	X	✓	X
View hardware information	✓	✓	X	✓	X
Turn beaconing on and off	✓	X	X	✓	X
Power on, power off, and reboot server modules	✓	X	X	✓	X
Insert a comment into the internal logs	✓	✓	✓	✓	X
Download the internal logs	✓	X	X	✓	X
Power server modules off and on	✓	X	X	✓	X
View hardware maintenance activity and history	✓	✓	X	✓	X
Perform hardware maintenance procedures	X	X	X	✓	X
View the HCP S Series OS and software update history	✓	X	X	✓	X
Update the HCP S Series OS and software	X	X	X	✓	X

Considerations for working with user accounts

These considerations apply to working with user accounts:

- You cannot change the username for an existing user account.
- At all times, at least one user account must have the security role. Therefore:
 - You cannot remove the security role from the last user account that has that role.
 - You cannot delete the last user account that has the security role.
- The last user account that has the security role cannot be disabled in any of these ways:
 - Manually
 - Automatically due to failed login attempts
 - Automatically due to lack of use
- If you disable the user account you used to log in to the HCP S Series Management Console, the Console session immediately ends.
- You cannot delete a user account that owns any buckets. To delete the account, you first need to change the owner of each applicable bucket to a different user account.

- You cannot delete the user account you're currently using to access the S Series Node.
- Multiple people can use the same user account at the same time to access the same or different S Series Node interfaces. To prevent this from happening, you should create a separate account for each user.

S Series objects

An HCP S Series Node stores objects. An S Series *object* is a combination of:

- An exact digital reproduction of data as it existed before it was stored on the S Series Node.
- Information that describes the object (for example, the data size and the object creation date). This information is called *metadata*.

When data is written to an S Series Node, the S Series Node creates an object from that data.

S Series objects are not the same as HCP objects, and the two types of objects do not have a one-to-one correspondence with each other. Each HCP object tiered to an S Series Node can result in multiple objects on the S Series Node.

Object protection

To ensure that objects are well-protected, the HCP S Series Node uses erasure coding. With erasure coding, data is encoded and broken into multiple chunks that are then stored across multiple locations. Additionally, parity chunks generated from the data chunks are stored across multiple locations. Each data or parity chunk is stored in a different location.

When erasure-coding the data for an object, the S Series Node creates 20 data chunks and 6 parity chunks and stores each chunk on a different drive. This 20+6 configuration results in a data reliability of 15 nines.

The S Series Node can reconstruct the data for an object from any combination of 20 of the data and parity chunks for that object. This ability means that the object is protected as long as at least 21 of the 26 drives used to store the data and parity chunks are available. If only 20 of the drives are available, the S Series Node can reconstruct the object data, but that data is no longer protected. If fewer than 20 of the drives are available, the S Series Node cannot reconstruct the object data, and the object is considered irreparable.

Object repair

When a drive becomes unavailable, the S Series Node immediately starts repairing the objects with data or parity chunks on that drive by re-creating those chunks on other drives. A chunk for an object can be re-created as long as both of these are true:

- At least 20 other chunks for that object are on available drives.
- At least one other drive:
 - Is available
 - Doesn't already have a chunk for that object
 - Has enough space to store the re-created chunk

Because the S Series Node starts repairing objects immediately, the chance of more than six chunks for an object being unavailable at the same time is exceedingly low. Also, when making repairs, the S Series Node gives higher priority to objects that have a higher risk of becoming irreparable.

Effect of enclosure unavailability

When storing the data for an object, the S Series Node spreads the selection of drives for the data and parity chunks across the available enclosures. If the S Series Node has five or more available enclosures and the chunks are distributed optimally across the enclosures, no enclosure will have more than six chunks for the object. In this case, depending on the number of enclosures in the S Series Node, one or more of those enclosures can become unavailable without affecting the ability of the S Series Node to reconstruct the object data.

If the S Series Node has fewer than five enclosures, one enclosure will have more than six chunks for the object. If that enclosure becomes unavailable and the S Series Node cannot access the drives in the enclosure, the object becomes irreparable and remains so until the enclosure becomes available again.

For example, if the S Series Node has four enclosures, three of the enclosures will have six chunks each for the object being stored, and the fourth enclosure will have eight chunks. If the enclosure with eight chunks becomes unavailable and the drives in the enclosure are inaccessible, the object becomes irreparable because only 18 chunks for the object are accessible.

With four enclosures, if one enclosure becomes unavailable and the drives on the enclosure are inaccessible, approximately one-quarter of the objects stored on the S Series Node become irreparable. With three enclosures, if one enclosure becomes unavailable and the drives on the enclosure are inaccessible, approximately one-third of the objects stored on the S Series Node become irreparable.

Effect of adding a fifth enclosure

An S Series Node that has five or more available enclosures stores new objects with an optimal distribution of data and parity chunks. Optimal distribution means that no enclosure has more than six chunks for the data associated with any given object.

With fewer than five enclosures in the S Series Node, the distribution of the data and parity chunks for new objects is not optimal. Without optimal distribution, the S Series Node cannot guarantee object availability if an enclosure becomes unavailable.

When you add a fifth enclosure to an S Series Node, the S Series Node automatically optimizes the distribution of data and parity chunks. The optimization process is similar to the repair process. Object chunks are removed from the enclosures with too many chunks and re-created on the new enclosure.

Object repair has priority over the optimization process. If a repair backlog exists, optimization does not occur until the backlog is gone. However, because object repair entails the relocation of object chunks, repair can result in the optimal distribution of those chunks.

Optimization is a resource-intensive process and can significantly slow data ingest. If this degradation becomes an issue, your authorized service provider can make changes to the optimization process to lessen the impact or temporarily stop the process.

Buckets

An HCP S Series Node stores objects in buckets. A *bucket* is a logical grouping of objects such that the objects in one bucket are not visible in any other bucket.

Buckets have these properties:

- Name.
- Owner. Only users with the data role can own buckets.
- Description (optional). The description can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.

An S Series Node can have at most 10,000 buckets.

If you have the administrator role, you can use the HCP S Series Management Console or management API to create, modify, and delete buckets. If you have the data role, you can use the Hitachi API for Amazon S3 (the S3 compatible API) to create and delete buckets.

To work with buckets in the Management Console, go to System > Buckets.

Bucket names

When you create a bucket, you specify a name for it. This name uniquely identifies that bucket on the S Series Node.

Bucket names:

- Must be 3 through 63 characters long
- Can contain only lowercase letters, digits, hyphens (-), and periods (.)
- Cannot contain consecutive periods
- Must start and end with a lowercase letter or digit
- Can consist of multiple parts delimited by periods, where each part starts and ends with a lowercase letter or digit
- Cannot have the form of an IP address (for example, 192.168.10.4)

Bucket owners

Each S Series Node bucket has an owner that corresponds to an S Series Node user account with the data role. When you create a bucket, you select the bucket owner. Only the owner of a bucket can store and manage objects in that bucket.

If you have the administrator role, you can use the HCP S Series Management Console or management API to change the owner of a bucket to a different user account.

An individual user can own at most 100 buckets.

Bucket information

The **BUCKETS** page of the Management Console shows the summary information listed below for all the buckets that currently exist on the S Series Node.

Ingested

The total number of bytes of data written to the S Series Node for all objects currently in the existing buckets

Objects

The total number of objects currently in the existing buckets

The **BUCKETS** page also contains graphs that show the number of ingested bytes and the number of objects in all existing buckets over the past ten days. If the HCP S Series software was installed less than ten days ago, the graphs show these numbers starting from the day the software was installed.

The S Series Node updates graph statistics at regular intervals. As a result, the graphs may not reflect current values.

Below the graphs, the **BUCKETS** page shows this information for each bucket that currently exists on the S Series Node:

- Bucket name
- Bucket owner
- Total number of ingested bytes for all objects currently in the bucket
- Number of objects currently in the bucket

Considerations for working with buckets

These considerations apply to modifying and deleting buckets:

- You cannot change the name of an existing bucket.
- If you change the owner of a bucket that's used by an HCP system or by an HCP for cloud scale system, you need to provide the applicable system with the credentials for the new owner. Until you provide the new credentials, that system cannot store, retrieve, or otherwise manage objects in the bucket.
- You can delete a bucket only if it's empty (that is, it does not contain any objects).

Networking

An HCP S Series Node makes use of three networks.

Access network

Used for external client access to the S Series Node through the Hitachi API for Amazon S3 (the S3 compatible API). This network can also be used for external client access to the S Series Node through the HCP S Series Management Console and management API.



Note: HCP systems and HCP for cloud scale systems always communicate with S Series Nodes over the access network for both data access and management purposes.

Management network

Used for external client access to the S Series Node through the HCP S Series Management Console and management API. This network cannot be used for access to the S Series Node through the S3 compatible API.

You can use the management network to segregate network traffic for management purposes from network traffic for data access.

Server interconnect network

Used exclusively for communication between the two S Series Node server modules. The two server modules are the only devices on this isolated network.

If you have the administrator or service role, you can use the HCP S Series Management Console or management API to modify S Series Node network configurations.

To work with S Series Node networks in the Management Console, go to Configuration > Networking.

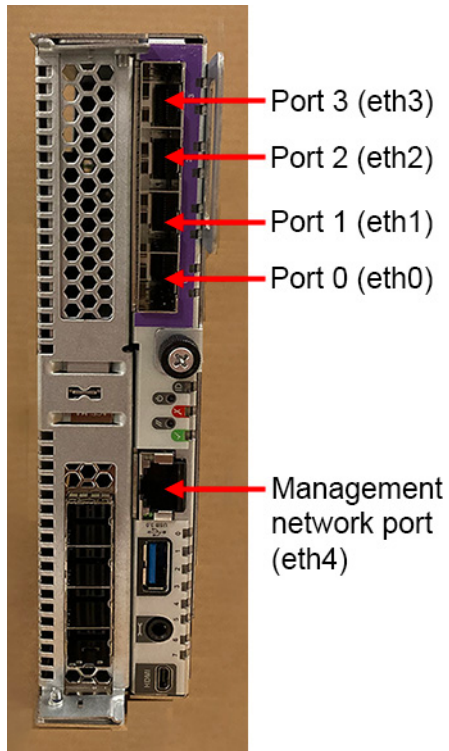
Server-module Ethernet ports

Each server module in an S11 or S31 Node has these Ethernet ports:

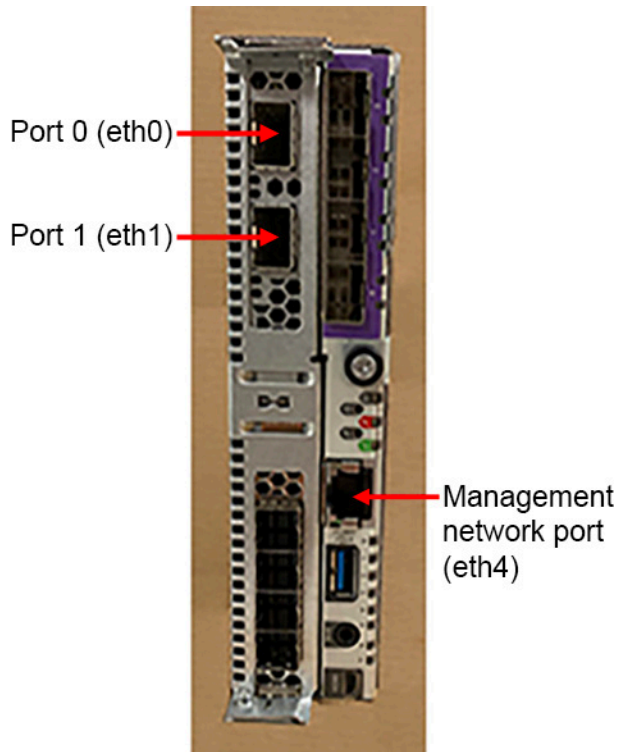
- Four onboard 10Gb SFP+ ports that are used for the access network if neither the optional two-port 25Gb Ethernet SFP28 PCIe card nor the optional four-port 10GBase-T Ethernet PCIe card is present:
 - If the onboard ports are used, the port numbers, from top to bottom, are 3, 2, 1, and 0. The corresponding port device names are eth3, eth2, eth1, and eth0.
 - If the onboard ports are not used, they are disabled.
- Optionally, two 25Gb Ethernet SFP28 ports on a PCIe card. If this card is present, the ports on the card are used instead of the onboard SFP+ ports for the access network. On this card, the port numbers, from top to bottom, are 0 and 1. The corresponding port device names are eth0 and eth1.

- Optionally, four 10GBase-T Ethernet ports on a PCIe card. If this card is present, the ports on the card are used instead of the onboard SFP+ ports for the access network. On this card, the port numbers, from top to bottom, are 3, 2, 1, 0. The corresponding port device names are eth3, eth2, eth1, and eth0.
- One onboard 1000Base-T Ethernet port that is used for the management network. The port device name is eth4. This port does not have a number.

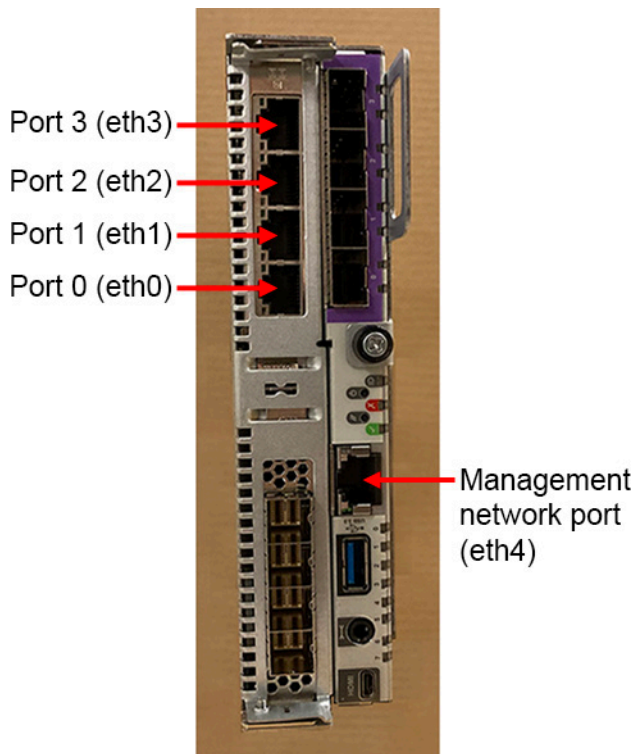
The figure below shows the locations of the Ethernet ports on a server module that does not have either Ethernet PCIe card installed in it.



The figure below shows the locations of the Ethernet ports on a server module that has a 25Gb Ethernet SFP28 PCIe card installed in it.



The figure below shows the locations of the Ethernet ports on a server module that has a 10GBase-T Ethernet PCIe card installed in it.



Access network

The S Series Node server modules can each have either two or four Ethernet ports for the access network, but the number of access network ports should be the same on the two server modules. For communication to occur over the access network, at least one access network port on one server module must be connected to an active Ethernet switch.

Port bonding and transmit hash policy

The access network ports can be configured for active-active bonding using the IEEE 802.3ad Link Aggregation Control Protocol (LACP) or for active-backup bonding. When the bonding mode is active-backup, the active port is the lowest-numbered connected port. All other connected ports are backup ports.

With 802.3ad bonding, the selected S Series Node transmit hash policy determines how the ports in the bond share the workload on the network. The options are layer 2+3 and layer 3+4:

- With layer 2+3, all traffic from any given client port targets the same access network port. Because the target port for a client port is selected independently of the target port selection for any other client port, the workload is not guaranteed to be balanced across the bonded access network ports. However, the greater the number of client ports, the more balanced the workload is likely to be.
- With layer 3+4, an algorithm enables traffic from any given client to span multiple access network ports. The algorithm ensures that the workload is balanced across the bonded access network ports.

With active-backup bonding, the only possible transmit hash policy is layer 2. With the S Series Node, layer 2 by itself is effectively the same as layer 2+3.

Port connections

The access network ports connect the server modules to your networking infrastructure through one or two Ethernet switches. The suggested configurations are:

- Both the access network and two switches configured for active-backup bonding. In this case, all the even-numbered ports (that is, eth0 and, if present, eth2) in use on both server modules connect to one switch. All the odd-numbered ports (that is, eth1 and, if present, eth3) in use on both server modules connect to the other switch.
- Both the access network and one or two switches configured for 802.3ad bonding:
 - With one switch, all the ports being used on both server modules connect to that switch.
 - With two switches, all the ports being used on one server module connect to one switch. All the ports being used on the other server module connect to the other switch.
- Both the access network and two switches configured for 802.3ad bonding and Cisco Virtual Port Channel (vPC). In this case:
 - All the even-numbered ports (that is, eth0 and, if present, eth2) in use on one server module and all the odd-numbered ports (that is, eth1 and, if present, eth3) in use on the other server module connect to one switch.
 - All the odd-numbered ports in use on the first server module and all the even-numbered ports in use on the second server module connect to the other switch.

For the best configuration for your S Series Node, consult your network administrator.

Port connection expectations

You can configure the access network so that the S Series Node expects specific access network ports to be connected to an active switch. You set the connection expectations separately for each server module.

Typically, the connection expectations are the same for the two server modules. However, while the Ethernet cards are being installed in the server modules or being switched from one type of card to the other, the connection expectations for the server modules may differ from each other.

Regardless of the configured expectations, the S Series Node uses each connected port, either as an active port or as a backup port, depending on the bonding mode.



Tip: To prevent the S Series Node from issuing alerts about unexpected or missing port connections, set the connection expectation for each port according to whether the port is actually connected to an active switch.

To work with the access network in the Management Console, go to Configuration > Networking. Then click the edit icon (✎) for the access network.

Access network IP addresses

Each server module has both physical and virtual access network IP addresses. To ensure that access to the HCP S Series Node is not disrupted by the unavailability of a single server module, clients should use the virtual IP addresses to communicate with the S Series Node. Communications that use a virtual IP address for an unavailable server module are automatically redirected to the available server module. When the unavailable server module becomes available again, communications using the virtual IP address for that module revert back to that module.

The access network can have an IP mode of either IPv4 or IPv6. If the IP mode is IPv4, the two server modules must have access network IPv4 addresses on the same IPv4 subnet. If the IP mode is IPv6, the two server modules must have primary access network IPv6 addresses on the same IPv6 subnet. In all cases, the virtual IP address for a server module must be on the same subnet as the physical IP address.

With an IP mode of IPv6, the server modules can also have secondary physical and virtual access network IPv6 addresses. These addresses must be on the same IPv6 subnet, and that subnet must not overlap the primary access network subnet. If one server module has a secondary access network IPv6 address, the other server module must also have a secondary access network IPv6 address.

The table below shows a sample IPv6 configuration for the access network.

Property	Values
Primary IPv6 properties	
Gateway address	2001:db8::ff:ff:ff:0
Prefix length	64
Physical IP addresses	Server module 1: 2001:db8::1:0:0:1 Server module 2: 2001:db8::1:0:0:2
Virtual IP addresses	Server module 1: 2001:db8::1:0:0:3 Server module 2: 2001:db8::1:0:0:4
Secondary IPv6 properties	
Gateway address	2001:db9::ff:ff:ff:0
Prefix length	64
Physical IP addresses	Server module 1: 2001:db9::1:0:0:1 Server module 2: 2001:db9::1:0:0:2
Virtual IP addresses	Server module 1: 2001:db9::1:0:0:3 Server module 2: 2001:db9::1:0:0:4

The access network subnet or subnets cannot overlap the subnets for the S Series Node management and server interconnect networks.



Note: In the zone definition for the S Series Node in DNS, use the virtual IP addresses of the server modules. For information about configuring an S Series Node in DNS, see [DNS configuration \(on page 62\)](#).

Access network properties

The access network has the properties listed below.

IP mode (either IPv4 or IPv6)

By default, the access network has an IP mode of IPv4.

IPv4-specific properties:

IPv4 gateway address

This is the address from which communications initiated by the S Series Node are sent when the access network is the selected network for the particular type of communication and IPv4 addressing is selected.

By default, the access network has an IPv4 gateway address of 10.0.0.254.

IPv4 subnet

With the Management Console, you use the IPv4 gateway address and a four-octet subnet mask to specify the IPv4 subnet. With the management API, you use CIDR notation to specify the IPv4 subnet.

By default, the access network has an IPv4 subnet of 10.0.0.0/24 and a four-octet subnet mask of 255.255.255.0.

Physical IPv4 address for each server module

By default, the access network has physical IPv4 addresses of 10.0.0.1 for server module 1 and 10.0.0.2 for server module 2.

Virtual IPv4 address for each server module

By default, the access network virtual IP addresses are not set. These IP addresses must be set during the initial on-site configuration of the S Series Node.

IPv6-specific properties:

Primary IPv6 gateway address

This is the address from which communications initiated by the S Series Node are sent when the access network is the selected network for the particular type of communication and primary IPv6 addressing is selected.

Primary IPv6 subnet

With the Management Console, you use the primary IPv6 gateway address and an IPv6 prefix length to specify the primary IPv6 subnet. With the management API, you use CIDR notation to specify the primary IPv6 subnet.

Primary physical IPv6 address for each server module

These IP addresses must be set during the initial on-site configuration of the S Series Node.

Primary virtual IPv6 address for each server module

These IP addresses must be set during the initial on-site configuration of the S Series Node.

Optionally, secondary IPv6 settings

Gateway address, subnet, physical address for each server module, and virtual address for each server module.

With the Management Console, you use the secondary IPv6 gateway address and an IPv6 prefix length to specify the secondary IPv6 subnet. With the management API, you use CIDR notation to specify the secondary IPv6 subnet.

Combined speed and duplex

By default, the access network has a speed and duplex setting of auto. With this setting, the S Series Node detects the speed and duplex settings of the device with which it's communicating. The S Series Node then adjusts its own settings to provide the highest possible data rate.

Maximum transmission unit (MTU)

The MTU is the largest packet size supported for data sent on the network.

The MTU for a network can be 1,500 or 9,000. The larger MTU reduces overhead and increases network throughput. An MTU of 9,000 is possible only if it is supported by the networking infrastructure.

By default, the access network has an MTU of 1,500.

Bonding mode and transmit hash policy

The bonding mode and transmit hash policy can be:

- active-backup
- 802.3ad (layer 2+3)
- 802.3ad (layer 3+4)

By default, the access network has a bonding mode of active-backup.

VLAN ID

If the networking infrastructure supports virtual networking, valid values for the VLAN ID are integers in the range 0 through 4,094. If the networking infrastructure doesn't support virtual networking, the VLAN ID must be 0.

If the access network has a nonzero VLAN ID, the applicable switches must be configured to support that ID. Additionally, the networking infrastructure must be configured to allow client requests to be routed to the S Series Node through the access network.

By default, the access network has a VLAN ID of 0.

Connection expectation for each port on each server module

The connection expectation for a port can be On (connection expected) or Off (connection not expected). If a server module has a two-port 25Gb Ethernet SFP28

PCIe card installed in it, you set connection expectations for ports 0 and 1. Otherwise, you set connection expectations for ports 0, 1, 2, and 3.

The S Series Node issues an alert if:

- A port is expected to be connected (that is, the port setting is On) but is not connected to an active port on a network switch.
- A port is not expected to be connected (that is, the port setting is Off) but is connected to an active port on a network switch.

Management network

For the management network, each server module has one 1Gb Ethernet port. These ports connect the server modules to your networking infrastructure through one or two Ethernet switches:

- With one Ethernet switch, the management ports on both server modules connect to the same switch. With this configuration, if connectivity to the switch is lost, access to the S Series Node over the management network is not possible.
- With two Ethernet switches, the management port on each server module connects to a different switch. With this configuration, loss of connectivity to one switch does not prevent access to the S Series Node over the management network.

Use of the management network is not required. If you don't plan to use this network, you can leave the management ports unconnected.



Tip: If you don't connect the management network ports, disable monitoring of the management network. Disabling monitoring prevents the S Series Node from issuing alerts about the network not being connected.

Modifying the management network causes the S Series Node to reboot. Enabling or disabling management-network monitoring does not cause a reboot.

To work with the management network in the Management Console, go to Configuration > Networking. Then click the edit icon (✎) for the management network.

Management network IP addresses

The management network can have an IP mode of either IPv4 or IPv6. If the IP mode is IPv4, the two server modules must have management IPv4 addresses on the same IPv4 subnet. If the IP mode is IPv6, the two server modules must have primary management IPv6 addresses on the same IPv6 subnet.

With an IP mode of IPv6, the server modules can also have secondary management IPv6 addresses. These addresses must be on the same IPv6 subnet, and that subnet must not overlap the subnet for the primary management IPv6 addresses. If one server module has a secondary management IPv6 address, the other server module must also have a secondary management IPv6 address.

The management network subnet or subnets cannot overlap the subnets for the S Series Node access and server interconnect networks.

Management network properties

The management network has the properties listed below.

IP mode (either IPv4 or IPv6)

By default, the management network for a new S Series Node has an IP mode of IPv4.

IPv4-specific properties:

IPv4 gateway address

This is the address from which communications initiated by the S Series Node are sent when the management network is the selected network for the particular type of communication and IPv4 addressing is selected.

By default, the management network has an IPv4 gateway address of 10.2.2.254.

IPv4 subnet

With the Management Console, you use the IPv4 gateway address and a four-octet subnet mask to specify the IPv4 subnet. With the management API, you use CIDR notation to specify the IPv4 subnet.

By default, the management network has an IPv4 subnet of 10.2.2.0/24 and a four-octet subnet mask of 255.255.255.0.

The management network IPv4 subnet cannot start with 192.168.

IPv4 address for each server module

By default, the management network has IPv4 addresses of 10.2.2.1 for server module 1 and 10.2.2.2 for server module 2.



Note: Do not use 10 as the fourth octet for the IPv4 gateway address or server module IPv4 addresses. This value is reserved for use by authorized service providers.

IPv6-specific properties:

Primary IPv6 gateway address

This is the address from which communications initiated by the S Series Node are sent when the management network is the selected network for the particular type of communication and primary IPv6 addressing is selected.

Primary IPv6 subnet

With the Management Console, you use the primary IPv6 gateway address and an IPv6 prefix length to specify the primary IPv6 subnet. With the management API, you use CIDR notation to specify the primary IPv6 subnet.

Primary IPv6 address for each server module

Optionally, secondary IPv6 settings

Gateway address, subnet, and address for each server module.

With the Management Console, you use the secondary IPv6 gateway address and an IPv6 prefix length to specify the secondary IPv6 subnet. With the management API, you use CIDR notation to specify the secondary IPv6 subnet.



Note: Do not use 000A as the last segment for the primary or secondary IPv6 gateway address or primary or secondary server module IPv6 addresses. This value is reserved for use by authorized service providers.

Combined speed and duplex setting

By default, the management network has a speed and duplex setting of auto. This setting cannot be changed.

With a setting of auto, the S Series Node detects the speed and duplex settings of the device with which it's communicating. The S Series Node then adjusts its own setting to provide the highest possible data rate.

Maximum transmission unit (MTU)

The MTU is the largest packet size supported for data sent on the network.

The MTU for a network can be 1,500 or 9,000. The larger MTU reduces overhead and increases network throughput. An MTU of 9,000 is possible only if it is supported by the networking infrastructure.

By default, the management network has an MTU of 1,500.

VLAN ID

If the networking infrastructure supports virtual networking, valid values for the VLAN ID are integers in the range 0 through 4,094. If the networking infrastructure doesn't support virtual networking, the VLAN ID must be 0.

If the management network has a nonzero VLAN ID, the management network switches must be configured to support that ID. Additionally, the networking infrastructure must be configured to allow client requests to be routed to the S Series Node through the management network.

By default, the management network has a VLAN ID of 0.



Note: For internal purposes, the S Series Node uses VLAN IDs of either 700 and 800 or 701 and 801. You cannot use the HCP S Series Management Console or management API to change the management network VLAN ID to a VLAN ID that's being used internally. If the management network requires the use of a VLAN ID that's being used internally, contact your authorized service provider to have the VLAN ID changed. In this case, changing the VLAN ID entails rebooting the S Series Node. While the S Series Node reboots, it is unavailable for both management and data access purposes.

Management network monitoring

If you don't physically connect the management network to the your networking infrastructure, you should disable monitoring for the network. If monitoring is enabled without the physical connections present, the S Series Node reports that the network

is not functioning properly, and the HCP S Series Management Console displays alerts to that effect. By default, management network monitoring is enabled.

Server interconnect network

Each server module has a single internal Ethernet port for the server interconnect network. An internal link connects these ports to each other.

The server interconnect network has an IP mode of IPv4. By default, the subnet for this network is 10.1.1.0/24.

You can change the subnet for the server interconnect network. However, you should do this only if a conflict exists.

The server interconnect network subnet cannot overlap the subnets for the S Series Node access and management networks. Additionally, the server interconnect network subnet cannot overlap any subnet used in the networking environment.

The number of bits in the server interconnect network subnet prefix must be 24 (indicated by the suffix /24 in CIDR notation).

The server interconnect network subnet cannot start with 192.168.

Modifying the server interconnect network subnet causes the S Series Node to reboot.

To work with the server interconnect network in the Management Console, go to Configuration > Networking. Then click the edit icon (✎) for the server interconnect network.

Considerations for working with networks

These considerations apply to modifying networks:

- You cannot change the names of the S Series Node networks.
- You can modify all properties of the access network and management network except their names. To modify a subnet, change the applicable gateway address, subnet mask, or prefix length.
- When you modify the access network, communication with the S Series Node is briefly disrupted. However, the S Series Node does not reboot.
- When you modify the management network, the S Series Node reboots. Enabling or disabling management-network monitoring does not cause a reboot.
- You can change the physical or virtual IP address of the server module that's servicing the change request. If the IP address you change is the one the request is using and you're making the change in the HCP S Series Management Console, the Console session immediately ends.
- You can change the subnet for the server interconnect network, but you cannot change the fourth octet of the server-module IP addresses on that network.
- When you change the subnet for the server interconnect network, both S Series Node server modules automatically reboot. Until the reboot is complete, no communication can occur between the S Series Node and other devices.

- Multiple S Series Nodes can have the same server interconnect network subnet and the same server interconnect network IP addresses for their server modules. This configuration is possible because the server interconnect network on any given S Series Node is isolated from the server interconnect network on every other S Series Node.
- When you correctly change the configuration of a network, the HCP S Series Management Console displays a success message. However, this message is displayed before the change is fully implemented. To ensure that the change succeeded, check the S Series Node event log. If you do not see the following message, the change succeeded:

```
Network configuration change could not be applied
```

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol for secure communication over computer networks. When a client request to an HCP S Series Node specifies HTTPS in the URL, both the client request and the response from the S Series Node are secured by TLS.

S Series Nodes support TLS versions 1.0, 1.1, 1.2, and 1.3, but you can set the minimum version that the S Series Node can use. For example, if you set the minimum TLS version to 1.2, the S Series Node accepts requests that use version 1.2 or 1.3 but rejects requests that use version 1.0 or 1.1.

By default, the minimum TLS version for an S Series Node is 1.2.

If you have the administrator or service role, you can use the HCP S Series Management Console or management API to change the minimum TLS version. Changing the minimum TLS version causes the S Series Node to reboot.

To change the minimum TLS version in the Management Console, go to Configuration > TLS Version.



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

HCP S Series Node identification

Each HCP S Series Node is identified by both a domain name and a serial number.

The domain name and serial number are displayed in the bottom right corner of each page in the HCP S Series Management Console. If you have the administrator, monitor, or service role, you can also see the domain name and serial number on the **IDENTIFICATION** page of the Management Console or by using the S Series Node management API.

Domain name

If DNS is in use at your site, the domain name for the S Series Node must be a fully qualified DNS domain name that can be used for access to that S Series Node (for example, `s-node-1.example.com`). Valid domain names:

- Can contain only letters, numbers, and hyphens (-)
- Must consist of at least three segments, separated by periods, where each segment is 1 through 63 characters long
- Can be at most 127 characters long, including the periods between segments

The domain name cannot be `rhino-name.domain.com`.

For clients to access the S Series Node by domain name, the domain must be defined as a primary zone in DNS.

Even if DNS is not in use, the S Series Node must have a domain name. This dummy domain name must comply with the rules for valid domain names.

If you have the administrator or service role, you can use the HCP S Series Management Console or management API to change the domain name for an S Series Node.

To change the domain name in the Management Console, go to Configuration > Identification.

If DNS is in use and you change the domain name, also change the domain name in DNS. If any clients access the S Series Node by domain name, change the domain name in those clients.

For information about configuring an S Series Node in DNS, see [DNS configuration \(on page 62\)](#).

Serial number

The serial number for an S Series Node uniquely identifies the S Series Node. On a base enclosure, the serial number is on a label on the right in the first indentation from the front on the top of the main-bay cover. On an expansion enclosure, the serial number appears on the enclosure number label, which is also on the right in the first indentation from the front on the top of the main-bay cover.

You cannot change the serial number for an S Series Node.

HCP S Series software version

The bottom right corner of each page in the HCP S Series Management Console shows the version number of the currently installed HCP S Series software.

If a hotfix has been applied to the S Series Node, the hotfix number follows the software version number, as in this example:

```
v3.2.0.2-HF1
```

If multiple hotfixes have been applied to the S Series Node, only the number of the most recently applied hotfix is shown.

The **UPDATE** page of the Management Console shows the history of the HCP S Series software on the S Series Node, starting from the most recent installation or reinstallation of the software. Each time the software is upgraded on the S Series Node or a hotfix is applied to the S Series Node, the software history is updated.

If you have the administrator or service role, you can use the Management Console or management API to see the software update history list.

To see the software update history list in the Management Console, go to System > Update.

Licensing

When used in conjunction with an HCP or HCP for cloud scale system, HCP S Series Node storage must be covered by the HCP or HCP for cloud scale license. The license key must be installed on the HCP or HCP for cloud scale system. On the S Series Node, the license status is External. The installation of a license key on the S Series Node is not required.



Note: On a release 7.x HCP system that's using an S Series Node for storage, the HCP S Series Management Console reports that HCP cannot find license information for the S Series Node.



Important:

- The amount of storage used on an S Series Node is subject to the limit specified by the HCP or HCP for cloud scale license. The S Series Node will continue to function if this limit is exceeded but will be in violation of the license agreement.
- Use of an S Series Node as a standalone storage device is not supported and is a violation of the terms of sale.

If you have the administrator, monitor, or service role, you can use the HCP S Series Management Console or management API to view the license status.

To view the S Series Node license status in the Management Console, go to System > License.

DNS servers

Optionally, you can make up to three DNS servers known to an S Series Node. You identify each DNS server by its IP address.

You can choose the network (access or management) to be used for communication between the S Series Node and the DNS servers you specify. The default is the access network.

The S Series Node uses the selected network in the IP mode in which the network is configured. If the network is configured for IPv6 and a secondary IPv6 gateway is configured for the network, you can choose to use either the primary or secondary IPv6 gateway.

For the S Series Node to communicate with the specified DNS servers, the IP mode of the selected network must match the IP mode of the DNS server IP addresses.

The S Series Node issues an alert if communications to the DNS servers fail.

If you have the administrator or service role, you can use the HCP S Series Management Console or management API to modify DNS-server settings for the HCP S Series Node.

To work with DNS-server settings in the Management Console, go to Configuration > DNS Servers.

Time servers

S Series Nodes use external time servers to set and maintain their internal clock times. An S Series Node always needs to know how to access at least one external time server.

You can specify up to three external time servers for use by an S Series Node. You identify each time server by its IP address. You cannot use DNS hostnames to identify time servers to an S Series Node.

The time servers you specify should be the same time servers as those that are used by the clients accessing the S Series Node.

Regardless of the time servers used, S Series Node time is always expressed in UTC.

You can choose the network (access or management) to be used for communication between the S Series Node and the time servers you specify. The default is the access network.

The S Series Node uses the selected network in the IP mode in which the network is configured. If the network is configured for IPv6 and a secondary IPv6 gateway is configured for the network, you can choose to use either the primary or secondary IPv6 gateway.

For the S Series Node to communicate with the specified time servers, the IP mode of the selected network must match the IP mode of the time server IP addresses.

Changing the list of time servers used by an S Series Node causes the S Series Node to restart.

The S Series Node issues an alert in the event of a time synchronization error.

If you have the administrator or service role, you can use the HCP S Series Management Console or management API to modify time-server settings for the HCP S Series Node.

To work with time-server settings in the Management Console, go to Configuration > Time Servers.

Client access

An HCP S Series Node has three interfaces for client access:

- The web-based HCP S Series Management Console supports only management functions.
- The RESTful HCP S Series management API supports only management functions.
- The RESTful Hitachi API for Amazon S3 (the S3 compatible API) supports only data access functions.



Note: The only supported data access protocol for the S Series Node is the Hitachi API for Amazon S3.

To support the use of HTTPS with these interfaces, the S Series Node must have an SSL server certificate. Using HTTPS with the S3 compatible API is possible only if the S Series Node is configured to support the use of SSL for data access.

If you have the administrator or service role, you can use the HCP S Series Management Console or management API to configure the interfaces that enable access to the S Series Node.

Management Console configuration

You can enable access to the HCP S Series Management Console on both the access network and the management network. At any given time, at least one of these networks must be enabled for Console access. By default, both networks are enabled for Console access.

By default, for both the access and management networks, only HTTPS is enabled for Management Console access. For each of these networks individually, you can also enable HTTP for Console access. You cannot disable HTTPS for either network without disabling all access to the Management Console through that network.

Support for HTTP without SSL security is provided so that the Management Console can accept requests passed on by load balancers when the load balancer has terminated the SSL connection. Client requests for access to the Management Console should always use HTTPS, not HTTP.



Note: When you enable or disable HTTP or HTTPS for the access or management network in the Management Console configuration, the same change occurs automatically to the corresponding setting in the management API configuration. When you disable HTTP or HTTPS for the access or management network in the management API configuration, the same change occurs automatically to the corresponding setting in the Management Console configuration. However, when you enable HTTP or HTTPS for the access or management network in the management API configuration, the corresponding setting in the Management Console configuration does not change.

By default, users can access the Management Console from any IP address. You can choose to allow access only from specific IP addresses. Similarly, you can choose to deny access from specific IP addresses. You control how the S Series Node handles IP addresses that are both allowed and denied access or neither allowed nor denied access.

You can specify message text to appear on the login page of the Management Console. This text is optional. If specified, it can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.

The text you specify appears above the fields for the username and password on the login page. You can use this text, for example, for messages such as "Authorized Users Only" or "For support, contact hcpsseries-admin@example.com."

To work with the Management Console configuration in the Management Console, go to Configuration > Console.

Management API configuration

You can enable access to an S Series Node through the HCP S Series management API on both the access network and the management network. At any given time, at least one of these networks must be enabled for management API access. By default, both networks are enabled for management API access.



Note: HCP always communicates with S Series Nodes over the access network. If the access network is disabled for the management API, HCP systems cannot use the S Series Node.

By default, for both the access and management networks, only HTTPS is enabled for access to the S Series Node through the management API. For each of these networks individually, you can also enable HTTP for management API access. You cannot disable HTTPS for either network without disabling all management API access through that network.

For security reasons, client requests for access to the S Series Node through the management API should always use HTTPS, not HTTP.



Note:

- When you enable or disable HTTP or HTTPS for the access or management network in the Management Console configuration, the same change occurs automatically to the corresponding setting in the management API configuration. When you disable HTTP or HTTPS for the access or management network in the management API configuration, the same change occurs automatically to the corresponding setting in the Management Console configuration. However, when you enable HTTP or HTTPS for the access or management network in the management API configuration, the corresponding setting in the Management Console configuration does not change.
- In releases earlier than 3.2.0, HTTP could be enabled in the Management Console configuration and, at the same time, disabled in the management API configuration. This combination is not supported in release 3.2.0. If this combination is present before an upgrade to release 3.2.0 or later, HTTP is automatically enabled in the management API configuration during the upgrade.

By default, users can use the management API to access an S Series Node from any IP address. You can choose to allow access only from specific IP addresses. Similarly, you can choose to deny access from specific IP addresses. You control how the S Series Node handles IP addresses that are both allowed and denied access or neither allowed nor denied access.

To work with the management API configuration in the Management Console, go to Configuration > MAPI.

Data access protocol configuration

You can enable or disable use of the S3 compatible API. If you disable use of this API, clients cannot read, write, modify, or delete data stored on the S Series Node.

By default, if the S Series Node supports the use of SSL for data access, both HTTP and HTTPS are enabled for access to the S Series Node through the S3 compatible API. You can disable the use of HTTP with the S3 compatible API, but you cannot disable the use of HTTPS.

If the S Series Node does not support the use of SSL for data access, HTTP is the only option for access through the S3 compatible API.

By default, clients can use the S3 compatible API to access an S Series Node from any IP address. You can choose to allow access only from specific IP addresses. Similarly, you can choose to deny access from specific IP addresses. You control how the S Series Node handles IP addresses that are both allowed and denied access or neither allowed nor denied access.

To work with the S Series Node data access protocol configuration in the Management Console, go to Configuration > Protocols.

Access control list

The access control list for a given interface specifies IP addresses that are allowed or denied access to the S Series Node through that interface. Each entry in an access control list can be:

- A single IP address
- A range of IPv4 addresses specified as *ip-address/subnet-mask* (for example, 192.168.100.197/255.255.255.0) or in CIDR format (for example, 192.168.100.0/24)
- A range of IPv6 addresses specified in CIDR format (for example, 2001:0db8::/32)

The CIDR entry that matches all IPv4 addresses is 0.0.0.0/0. The CIDR entry that matches all IPv6 addresses is 0::0/0.

Each entry in the list has an access setting of Allow or Deny. An individual IP address can end up with both settings if, for example, the IP address is in an address-range entry and also is an entry by itself.

To control how the S Series Node handles IP addresses that have neither, one, or both of the Allow and Deny settings for a given interface, you use the Allow access from IP address with both Allow and Deny settings option for that interface. The table below describes how this option works.

Access control list entries	Allow access from IP address with both Allow and Deny settings	
	Yes	No
Allow: none Deny: none	All IP addresses have access.	No IP addresses have access.
Allow: at least one entry Deny: none	All IP addresses have access.	IP addresses with the Allow setting have access. All other IP addresses do not have access.
Allow: none Deny: at least one entry	IP addresses with the Deny setting do not have access. All other IP addresses have access.	No IP addresses have access.
Allow: at least one entry Deny: at least one entry	IP addresses with only the Deny setting do not have access. All other IP addresses have access.	IP addresses with only the Allow setting have access. All other IP addresses do not have access.

At all times, at least one IP address must be allowed access to the HCP S Series Management Console, either explicitly or due to the list-handling option.

You cannot add the IP address from which you're currently accessing an S Series Node to the access control list for the interface you're using. Similarly, you cannot change the setting for allow-list and deny-list handling for that interface so that access would be denied from that IP address.

SSL server certificates

For HTTPS access to an HCP S Series Node through the HCP S Series Management Console, management API, or S3 compatible API, the S Series Node must have an SSL server certificate. To meet this need, each S Series Node comes with a self-signed certificate already installed. This certificate is valid for five years from the time the HCP S Series software was installed on the S Series Node. The common name in this certificate is **.node-domain-name*, where *node-domain-name* is the domain name configured for the S Series Node.

Self-signed SSL server certificates are not automatically trusted by web browsers and other HTTP client tools. However, clients can choose to trust them.



Note: If the S Series Node is using a self-signed SSL server certificate, the Management Console does not work with Mozilla Firefox.

You can use the Management Console or management API to get information about the currently installed SSL server certificate, including the expiration date. When the certificate is close to expiring, the S Series Node issues an alert about the upcoming expiration.

You can install a new SSL server certificate at any time. To install a new certificate, you can use any of these methods:

- Use the Management Console or management API to generate a certificate signing request (CSR). Then submit the generated CSR to a certificate authority (CA). When you receive the CA-signed certificate, use the Management Console or management API to install the certificate on the S Series Node.



Important: An S Series Node can store only one CSR at a time. If you generate a CSR, send that CSR to a CA, and then generate a different CSR, the certificate returned by the CA won't match the current CSR, and you won't be able to install the returned certificate.

- Create a PKCS12 file that contains an SSL server certificate. Then use the Management Console or management API to install the new certificate on the S Series Node.
- Use the HCP S Series Management Console or management API to generate and install a new self-signed certificate on the S Series Node. The new certificate has an expiration date of five years from the date on which the certificate was generated.



Tip: For greater security, if you're using self-signed certificates, periodically generate and install a new certificate.



Important: After an upgrade of an S Series Node from a release earlier than 3.2.0, if the S Series Node is using a self-signed SSL server certificate, use one of the methods listed above to install a new certificate.

An S Series Node can have only one SSL server certificate at a time. When you install a new certificate, that certificate replaces the existing certificate.

Also, when you install a new certificate, the S Series Node restarts. While restarting, the S Series Node is unavailable for both management and data access purposes.

After a new SSL server certificate is installed on the S Series Node, clients such as HCP must accept the new certificate to be able to continue accessing the S Series Node.

If you have the administrator role, you can use the HCP S Series Management Console or management API to install a new SSL server certificate on an S Series Node.

To view the currently installed SSL server certificate or work with SSL server certificates in the Management Console, go to Configuration > SSL Server Certificates.

Generating a CSR and installing the returned certificate

A CSR contains the information that a CA needs in order to generate an SSL server certificate for your organization. To know exactly which information is required, you need to check with the CA that you plan to use.

The procedure below uses the HCP S Series Management Console to generate a CSR and install the returned certificate.

Procedure

1. Log in to the Management Console using a user account with the administrator role.
2. Go to **Configuration > SSL Server Certificates**.
3. On the **SSL SERVER CERTIFICATES** page, click **Update Certificate**.
4. On the **UPDATE CERTIFICATE** page, click **Select** under **Generate Certificate Signing Request**.
5. On the **GENERATE CERTIFICATE SIGNING REQUEST** page, fill in the fields with the information needed by the CA.

By default, these fields contain the applicable values from the currently installed SSL server certificate.

Except where otherwise noted, the values you specify can be at most 64 characters long and can contain only letters, numbers, hyphens (-), periods (.), forward slashes (/), and spaces. The CA, however, may place other restrictions on these values.

To fill in the fields:

- In the **Common Name (CN)** field, type the common name for the certificate you want.

The common name must be the fully qualified domain name of the S Series Node, preceded by an asterisk and a period (*.). The common name can be at most 255 characters long and cannot contain underscores (_).
- In the **Organizational Unit (OU)** field, type the name of the organizational unit that will use the certificate (for example, the name of a business division or a name under which your organization does business).
- In the **Organization (O)** field, type the full legal name of your organization. Do not abbreviate.
- In the **Locality (L)** field, type the name of the city or other locality in which your organization is legally located.
- In the **State/Province (ST)** field, type the full name of the state or province in which your organization is legally located. Do not abbreviate.
- In the **Country (C)** field, type the two-letter ISO 3166-1 abbreviation for the country in which your organization is legally located (for example, US for the United States).

6. Click **Generate**.
7. When prompted, save the generated CSR to the location of your choice.
8. Send the CSR to the CA.
9. When you receive the CA-signed SSL server certificate, on the **SSL SERVER CERTIFICATES** page in the Management Console, click **Update Certificate**.
10. On the **UPDATE CERTIFICATE** page, click **Select** under **Upload Certificate**.
11. On the **UPLOAD CERTIFICATE** page, in the **CA-Signed Certificate** section, take one of these actions:
 - Drag the file containing the CA-signed certificate from a file browser to the **Certificate** field.
 - Click in the **Certificate** field. Then select the file containing the CA-signed certificate.
12. Click **Upload and Install**.

13. In response to the confirming message, click **OK**.

Installing an SSL server certificate that's in a PKCS12 file

The procedure below uses the HCP S Series Management Console to install an SSL server certificate that's in a PKCS12 file.

Procedure

1. Use a tool such as OpenSSL to create a PKCS12 file that contains an SSL server certificate. Optionally, associate a password with the file.
2. Log in to the Management Console using a user account with the administrator role.
3. Go to **Configuration > SSL Server Certificates**.
4. On the **SSL SERVER CERTIFICATES** page, click **Update Certificate**.
5. On the **UPDATE CERTIFICATE** page, click **Select** under **Upload Certificate**.
6. On the **UPLOAD CERTIFICATE** page, if the PKCS12 certificate has a password, in the **PKCS12 Password** field, type the password.
7. On the **UPLOAD CERTIFICATE** page, in the **PKCS12 Certificate** section, take one of these actions:
 - Drag the file containing the PKCS12 certificate from a file browser to the **Certificate** field.
 - Click in the **Certificate** field. Then select the file containing the PKCS12 certificate.
8. Click **Upload and Install**.
9. In response to the confirming message, click **OK**.

Generating and installing a new self-signed SSL server certificate

The procedure below uses the HCP S Series Management Console to generate and install a new self-signed SSL server certificate.

Procedure

1. Log in to the Management Console using a user account with the administrator role.
2. Go to **Configuration > SSL Server Certificates**.
3. On the **SSL SERVER CERTIFICATES** page, click **Update Certificate**.
4. On the **UPDATE CERTIFICATE** page, click **Select** under **Generate New Self-Signed Certificate**.
5. On the **GENERATE NEW SELF-SIGNED CERTIFICATE** page, click **Generate**.
6. In response to the confirming message, click **OK**.

Security settings

If you have the security role, you can use the HCP S Series Management Console or management API to control security for the S Series Node server modules and for S Series Node user accounts.

Ping

Ping is a UNIX program that checks whether a particular networked computer is operating and can accept requests.

You can enable or disable the use of ping with an S Series Node. Enabling ping lets you use the `ping` command to check the availability of and network connectivity to the S Series Node server modules.

Ping is enabled by default. If you have the security role, you can use the HCP S Series Management Console or management API to change this setting at any time while the HCP S Series software is running on at least one server module.

To enable or disable ping in the Management Console, go to Configuration > Security.

SSH

Secure Shell (SSH) is a network communication protocol that enables two computers to securely communicate with each other in a client/server relationship.

You can enable or disable the use of SSH with the S Series Node server modules. Enabling SSH access facilitates troubleshooting when you request support. If, due to an unexpected event, access to an S11 or S31 Node through the HCP S Series Management Console or management API is not possible, the service provider can use SSH to log in to either server module for the purpose of diagnosing and resolving the issue.

Disabling SSH access enhances the security of the S11 or S31 Node but can increase the amount of time required to diagnose and resolve issues. If the HCP S Series software is not running on either server module and SSH access is disabled, you cannot change the SSH setting. In this case, the service provider must come to your site to physically access the S11 or S31 Node and manually enable SSH access.

You should carefully consider whether you want SSH access enabled or disabled. Keeping SSH access enabled can prevent delays in diagnosing and resolving issues with the S11 or S31 Node, thereby minimizing the S11 or S31 Node downtime.

SSH access is initially enabled or disabled during the on-site setup of the S Series Node. If you have the security role, you can use the HCP S Series Management Console or management API to change this setting at any time while the HCP S Series software is running on at least one server module.

After a reinstallation of the HCP S Series OS and software, SSH access is disabled. To allow SSH access, you need to use the Management Console or management API to enable it.

To enable or disable SSH in the Management Console, go to Configuration > Security.

While SSH access is enabled, this message appears first in the alert list in the Management Console:

```
SSH is enabled.
```

If you have the security role, this alert is a link to the Configuration > Security page.

User-account security

The requirements you can set for S Series Node user-account passwords and the rules you can set for managing S Series Node user accounts were enhanced in release 3.2.0 of the HCP S Series software to provide greater security for user accounts.

If you have the security role, you can use the HCP S Series Management Console or management API to change the settings for password requirements and user-account management rules at any time.

To work with password requirements and user-account management rules in the Management Console, go to Configuration > Security.

Password requirements and user-account management rules

Initially, on a new S Series Node, all options for password requirements and user-account management rules have default values.

When an S Series Node is upgraded, the values of pre-existing options for requirements and rules do not change, but options that did not exist before the upgrade are either disabled or set to zero, as applicable. Passwords for pre-existing user accounts still work, even after you enable or change the value of any new options.

Password requirements apply whenever users change their passwords. If you change the password requirements, existing passwords that don't meet the new requirements work until the password expires.

Options for password requirements

The options for user-account password requirements are described below.

Minimum password length

Minimum number of characters that a password must contain. Valid values are integers in the range 6 through 64. On a new S Series Node, the default is 8.

The longer the minimum password length, the stronger user account passwords are likely to be. To encourage even stronger passwords, set a minimum number of characters for each of the four character sets listed below.

Uppercase letters (A-Z)

Minimum number of uppercase letters that a password must include. Valid values are integers in the range 0 through 64. On a new S Series Node, the default is 1.

A value of 0 means that the password can, but does not have to, include any uppercase letters.



Note:

- This option is new with release 3.2.0.
- The sum of the four character-set minimums cannot be greater than the minimum password length.

Lowercase letters (a-z)

Minimum number of lowercase letters that a password must include. Valid values are integers in the range 0 through 64. On a new S Series Node, the default is 1.

A value of 0 means that the password can, but does not have to, include any lowercase letters.



Note: This option is new with release 3.2.0.

Numbers (0-9)

Minimum number of numbers that a password must include. Valid values are integers in the range 0 through 64. On a new S Series Node, the default is 1.

A value of 0 means that the password can, but does not have to, include any numbers.



Note: This option is new with release 3.2.0.

Special characters

Minimum number of special characters that a password must include. The special characters are: `~!@#\$\$%^&*()-_+={}|:\;'"<>,.?/

Valid values are integers in the range 0 through 64. On a new S Series Node, the default is 1.

A value of 0 means that the password can, but does not have to, include any special characters.



Note: This option is new with release 3.2.0.

Force password change (days)

Number of days passwords are valid before they automatically expire. Valid values are 0 and integers in the range 3 through 999. On a new S Series Node, the default is 90.

A value of 0 disables this option, meaning that passwords never expire automatically.



Note: An HCP system that's configured to use storage on an S Series Node automatically changes the password for its S Series Node user account every 30 days. If you set the password expiration interval on the S Series Node to fewer than 30 days, the HCP system won't be able to access the S Series Node after the specified number of days have passed. To ensure that the HCP system doesn't lose access to the S Series Node, turn off automatic password expiration for the S Series Node user account created by HCP.

Block password re-use (previous passwords)

Number of previously used passwords for a user account that cannot be re-used when the account owner changes the password for that account. Valid values are integers in the range 1 through 99. On a new S Series Node, the default is 5.

The specified number includes the current password. For example, if the value of this option is 8, the new password cannot be the same as the current password or the last seven passwords used before the current password.

Regardless of the value of this option, the S Series Node stores the 99 most recently used passwords for each user account, or fewer if fewer passwords have been used. Therefore, if you increase the number of blocked passwords users immediately cannot re-use the new number of passwords. For example, if you increase the value of this option from 5 to 7, users who have used seven or more passwords are immediately blocked from using the seven most recently used passwords because the sixth and seventh passwords have already been stored.

All passwords, both current and previously used, are stored in an encrypted format.



Note:

- This option is new with release 3.2.0.
- In releases earlier than 3.2.0, for each user account, the S Series Node stored only the current password and the password used immediately before the current password. After an upgrade to release 3.2.0, the first time the account owner changes the password for the account, only those two stored passwords cannot be re-used, regardless of the value of the block password re-use option.

Block common passwords

Whether to prevent the terms in the common-password dictionary from being used as passwords. For information about the common-password dictionary, see [Common-password dictionary \(on page 56\)](#).

By default, on a new S Series Node, this option is disabled.

You can save security settings with this option enabled only after a common-password dictionary source file has been uploaded. If the contents of the common-password dictionary are deleted, this option is automatically disabled.



Note: This option is new with release 3.2.0.

Block username in password

Whether to prevent passwords from containing or being the same as the username for the applicable user account.

The username comparison is case insensitive. For example, if the username for the account is lgreen, none of these can be the password for the account: lgreen, Lgreen, lgreEn, lgreen953, 8?lgreen!

By default, on a new S Series Node, this option is enabled.



Note: This option is new with release 3.2.0.

Options for user-account management rules

The options for user-account management rules are described below.

Log user out if inactive more than (minutes)

Number of consecutive minutes an HCP S Series Management Console session can be idle before it automatically ends. Valid values are 0 and integers in the range 5 through 720. On a new S Series Node, the default is 10.

A value of 0 disables this option, meaning that Console sessions never automatically end due to inactivity.

Prevent retry after failed login for (seconds)

Number of seconds during which a user account cannot be used to log in to the HCP S Series Management Console after each failed login attempt with that account. Valid values are integers in the range 0 through 300. On a new S Series Node, the default is 5.

A value of 0 disables this option, meaning that user accounts can be used in new login attempts without any delay after failed login attempts.



Note: This option is new with release 3.2.0.

Disable user account after failed login attempts

Number of consecutive times a user can try to access the S Series Node with an incorrect or missing password before the applicable user account is automatically disabled. This limit takes into account both attempts to log in to the HCP S Series Management Console and attempts to access the S Series Node through the HCP S Series management API.

Valid values are 0 and integers in the range 3 through 99. On a new S Series Node, the default is 5.

A value of 0 disables this option, meaning that user accounts are not automatically disabled due to failed login attempts.

When a user account is re-enabled after being disabled due to failed login attempts, the count of failed login attempts starts again from zero.

The last user account with the security role is never automatically disabled due to failed login attempts.

Automatically re-enable user account after (minutes)

Number of minutes until a user account is automatically re-enabled after being disabled due to consecutive failed login attempts. Valid values are integers in the range 0 through 60. On a new S Series Node, the default is 60.

A value of 0 disables this option, meaning that user accounts are not automatically re-enabled after being disabled due to consecutive failed login attempts. In this case, the affected user accounts must be re-enabled manually.



Note: This option is new with release 3.2.0.

Disable user account if inactive more than (days)

Number of consecutive days a user account can be unused before it is automatically disabled. Valid values are integers in the range 0 through 999. On a new S Series Node, the default is 180.

A value of 0 disables this option, meaning that user accounts are never automatically disabled due to inactivity.

The last user account with the security role is never automatically disabled due to inactivity.



Note: This option is new with release 3.2.0.

Common-password dictionary

The common-password dictionary consists of a set of terms that are likely to be used as passwords (for example, *password*, *Qwerty*, or *12345678*). While the option to block common passwords is enabled, the S Series Node rejects new passwords that match any of the terms in the dictionary.

Dictionary terms

A dictionary term is a text string consisting of at most 64 UTF-8 characters. This value does not include the delimiter at the end of the term.

The comparison between a new password for a user account and the terms in the common-password dictionary is case insensitive. For example, the passwords *HitachiVantara123!*, *Hitachivantara123!*, *hitachivantara123!*, and *hitaCHlvanTARA123!* all match the term *HitachiVantara123!*.

To be the same, the specified password and the dictionary term must contain exactly the same sequence of case-insensitive letters, numbers, special characters, and white space. For example, the password *HitachiVantara123!* does not match the terms *HitachiVantara*, *Hitachi Vantara123!*, *123hitachivantara!*, or *HitachiVantaraLLC123!*.

Dictionary management

Initially, the common-password dictionary is empty. To populate the dictionary, you upload a `.txt` file containing the terms you want to block from being used as passwords. If the dictionary is not empty when you upload the file, the terms in that file replace the current contents of the dictionary.

The S Series Node treats new-line characters in the uploaded file as term delimiters. Special characters, including commas, spaces, and other white-space characters are treated as part of the delimited terms.

Uploading a file in which any terms contain non-UTF-8 characters can have an unpredictable effect on the dictionary.

The S Series Node stores the name of the most recently uploaded file used to populate the common-password dictionary, the date and time the file upload finished, and the file size. The maximum size for a file containing dictionary terms is 104,857,600 bytes. This size includes the new-line delimiter characters.

You cannot modify the contents of the common-password dictionary directly on the S Series Node. Instead, to add or remove terms from the dictionary, download the dictionary contents to a file, modify the file, and then upload the modified file. Downloading the dictionary contents does not remove the contents from the S Series Node.



Tip: If you still have the most recently uploaded file used to populate the common-password dictionary, you don't need to download the contents of the dictionary. Instead, you can modify and upload the file you already have.

Using the HCP S Series management API, you can delete the contents of the common password dictionary. Deleting the dictionary contents leaves the dictionary completely empty. Deleting the contents also removes the record of the most recently uploaded file used to populate the dictionary.



Tip: To allow the use of common passwords, instead of deleting the contents of the common-password dictionary, disable the option to block common passwords. That way, if you decide to re-enable that option, the dictionary contents are still present on the S Series Node.

If you have the security role, you can use the HCP S Series Management Console or management API to work with the common-password dictionary.

To work with the common-password dictionary in the Management Console, go to Configuration > Security.

Uploading terms to the common-password dictionary

The procedure below uses the HCP S Series Management Console to upload terms to the common-password dictionary.

Procedure

1. Create or get a file containing the terms you want to store in the common-password dictionary.
2. Log in to the Management Console using a user account with the security role.
3. Go to **Configuration > Security**.
4. On the **SECURITY** page:
 - a. Set **Block common passwords** to **On**.
 - b. Take one of these actions:
 - Drag the .txt file containing the dictionary terms from a file browser to the **Upload common-password source file** field.
 - Click in the **Upload common-password source file** field. Then select the .txt file containing the dictionary terms.

The name of the selected file appears below the **Upload common-password source file** field.

5. Click **Upload Common-Password Source File**.

6. In response to the confirming message, click **OK**.

If the upload is successful, the name of the uploaded file appears below the **Upload common-password source file** field.

Downloading the contents of the common-password dictionary

The procedure below uses the HCP S Series Management Console to download the contents of the common-password dictionary.

Procedure

1. Log in to the Management Console using a user account with the security role.
2. Go to **Configuration > Security**.
3. On the **SECURITY** page, if **Block common passwords** is set to **Off**, set the option to **On**.
4. In the **Common-password source file** field, click the download icon (↓).
5. If prompted, specify a file name and location for the downloaded dictionary content. Then click **Save**.

The default name for the downloaded file is the name of the uploaded file, followed by a timestamp indicating when the upload of the file finished. The time stamp has this format, where Z means that the time is in UTC:

```
yyyy-MM-ddT hh_mm_ss.msecZ
```

For example, if the name of the uploaded file is `CommonPasswords.txt`, the default name for the downloaded file would look like `CommonPasswords-2023-03-23T15_25_09.578Z.txt`.

If the name of the uploaded file includes a path, which is possible if the file was uploaded using the HCP S Series management API, the separators in the path are converted to underscores (`_`) in the default name for the downloaded file. For example, if the name of the uploaded file is `S-Series/Dictionary/CommonPasswords-rev1.txt`, the default name for the downloaded file would look like `S-Series_Dictionaries_CommonPasswords-rev1-2023-03-23T15_25_09.578Z.txt`.

SSH keys

SSH uses keys to ensure that only authorized clients have access to a given server. SSH keys come in pairs. One of the keys, the public key, is installed on the server. The other key, the private key, is installed on the clients. For SSH access to the server, the client must present the private key and, if defined, the passphrase for that key.

S Series Nodes make use of a set of SSH key pairs. Each key pair enables authorized service providers and support personnel to use SSH to log directly in to the S Series Node server modules using a specific user account.

The S Series Node comes with a set of default SSH keys already installed on it. These keys are installed during the initial installation of the HCP S Series OS and software. The default SSH keys are not unique to any single S Series Node.

On any S Series Node, you can install a set of SSH keys that are exclusive to that S Series Node. When you install exclusive SSH keys, they become active, and the previously active keys are no longer valid. If the previously active SSH keys were exclusive, those keys are removed from the S Series Node.

If, after installing exclusive SSH keys, you want to make the default SSH keys active, you can revoke the exclusive SSH keys. When you revoke exclusive SSH keys, they are removed from the S Series Node, and the default SSH keys become active.

If you have the administrator, monitor, security, or service role, you can use the HCP S Series Management Console or management API to view information about the currently active SSH keys. If you have the security or service role, you can use the Management Console or management API to install and revoke exclusive SSH keys.

To work with SSH keys in the Management Console, go to System > SSH Keys.

Viewing SSH key information

If exclusive SSH keys are active, the **SSH KEYS** page in the HCP S Series Management Console shows the fields listed below.

Customer name

Name of the customer that owns the S Series Node for which the exclusive SSH keys were generated.

Active SSH keys

Exclusive. This is a fixed value for exclusive SSH keys.

SSH key package ID

ID of the SSH key package containing the exclusive SSH keys. The package is in a file that gets uploaded to the S Series Node.

SSH key package creation date

Time at which the package containing the exclusive SSH keys was created. The package is created immediately after the SSH keys are generated.

SSH key activation date

Time at which the exclusive SSH keys were installed on the S Series Node.

If the default SSH keys are active, the **SSH KEYS** page shows only the Active SSH keys field. The value in this field is the word Default followed, in parentheses, by the identifier for the set of default SSH keys installed on the S Series Node.

Installing exclusive SSH keys

Exclusive SSH keys come packaged in a file. The file name has this format:

```
HCP-S-SSHKeyPackage-<customer-name>-SN<s-series-node-serial-number>-timestamp.plk
```

In this format:

- `<customer-name>` is the name of the customer that owns the S Series Node, with no spaces between words.
- `<s-series-node-serial-number>` is the full serial number of the S Series Node.
- `timestamp` is the date and time when the SSH key package was generated, in this format:

```
yyyy-MM-dd-hh-mm-ss
```

For example:

```
HCP-S-SSHKeyPackage-ExampleCompany-SNHHCA310000001-04-19-2023.plk
```

The SSH keys in a package work only on the S Series Node for which the package was created.

To install exclusive SSH keys, you upload the SSH key package on the S Series Node. If the S Series Node is the one for which the package was created, the S Series Node automatically installs the SSH keys. If the SSH key package was created for a different S Series Node, the S Series Node rejects the package and does not install the SSH keys.

The procedure below uses the HCP S Series Management Console to install exclusive SSH keys.

Before you begin

Ask your authorized service provider for an SSH key package for the S Series Node on which you want to install exclusive SSH keys.

Procedure

1. Log in to the Management Console using a user account with the security or service role.
2. Go to **System > SSH Keys**.
3. On the **SSH KEYS** page, in the **UPLOAD EXCLUSIVE SSH KEY PACKAGE** section, take one of these actions:
 - Drag the file containing the SSH key package from a file browser to the **SSH key package file** field.
 - Click in the **SSH key package file** field. Then select the file containing the SSH key package.

The name of the selected file appears below the **SSH key package file** field.

4. Click **Upload Exclusive SSH Key Package**.
5. In response to the confirming message, click **OK**.

Revoking exclusive SSH keys

The procedure below uses the HCP S Series Management Console to revoke exclusive SSH keys.

Procedure

1. Log in to the Management Console using a user account with the security or service role.
2. Go to **System > SSH Keys**.
3. On the **SSH KEYS** page, click **Revoke Exclusive SSH Keys**.
4. In response to the confirming message, click **OK**.

Chapter 4: DNS configuration

To be accessible by domain name, an HCP S Series Node must be configured in DNS. This configuration entails adding host entries to a forward lookup zone, where the host entries associate IP addresses for the S Series Node with the interfaces available for accessing the S Series Node.

Zone definitions for an S Series Node

To configure an S Series Node in DNS, you can take either of these actions:

- Create a forward lookup zone for the S Series Node and add host entries to that zone. In this case, the name of the zone looks something like `s-node-1.example.com`.
- Add host entries for the S Series Node to an existing forward lookup zone. In this case, the name of the zone looks something like `example.com`.

In either case, the zone must be configured as a primary zone.

Host entries

Each host entry for an S Series Node associates the IP address of a server module on one of the S Series Node networks with one of the three S Series Node interfaces or with a wildcard (*) that represents any of the interfaces.

The hostnames that correspond to the S Series Node interfaces are:

- For the Management Console: `admin`
- For the management API: `mapi`
- For the Hitachi API for Amazon S3 (the S3 compatible API): `hs3`

If the zone for the S Series Node has entries for both the wildcard hostname and one or more of the specific interface hostnames:

- The interface-specific host entries are used for the applicable interfaces.
- The wildcard host entry is used for the interfaces for which no interface-specific entries exist.

Normally, a wildcard host is associated with the virtual IP addresses for the server modules on the access network. If that network is using IPv6, the host can be associated either with only the primary virtual IPv6 addresses or with both the primary and secondary virtual IPv6 addresses.

Access network disabled

If the access network is disabled for the Management Console and you want to allow access to the Management Console by domain name, the zone must have entries specifically for the admin host. These entries must specify the IP addresses for the server modules on the management network.

Similarly, if the access network is disabled for the management API and you want to allow the use of this API with a domain name, the zone must have entries specifically for the mapi host. These entries must specify the IP addresses for the server modules on the management network.



Note: HCP systems and HCP for cloud scale systems always communicate with S Series Nodes over the access network. If the access network is disabled for the management API, HCP systems and HCP for cloud scale systems cannot get status and usage information from the S Series Node.

Configuring a forward lookup zone in Windows

To configure a forward lookup zone in Windows, you first create the zone. Then you add host entries to the zone.

The instructions in this section explain how to create a forward lookup zone specifically for an S Series Node. You don't need to do that if you're planning to add the host entries to an existing zone.

You can use either the GUI or a command line to configure zones in a Windows DNS server. The instructions in this section are for the Windows 2022 DNS server GUI. For a Windows 2003, 2008, 2012, 2016, or 2019 DNS server, the procedure is basically the same as the procedure here.

Creating a forward lookup zone for an S Series Node

Procedure

1. In the **Start** menu on the Windows server that's hosting the DNS server, click **Server Manager**.
2. In the **Server Manager** window, select **Tools > DNS**.
3. On the left side of the **DNS Manager** window, right-click **Forward Lookup Zones** under the higher-level zone within which you want to create the zone for the S Series Node. Then select **New Zone**.
4. In the **New Zone Wizard** window, click **Next**.
5. On the **Zone Type** page:
 - Select **Primary zone**.
 - If your site uses Active Directory, select **Store the zone in Active Directory**. Otherwise, deselect this option.

Then click **Next**.

6. If the **Active Directory Zone Replication Scope** page appears, select the applicable option for the Active Directory configuration at your site. Then click **Next**.
7. In the **Zone name** field on the **Zone Name** page, type the name of the S Series Node domain (for example, `s-node-1.example.com`). Then click **Next**.
8. If the **Zone File** page appears, click **Next** to accept the default file name.
9. On the **Dynamic Update** page, select **Do not allow dynamic updates**. Then click **Next**.
10. On the **Completing the New Zone Wizard** page, click **Finish**.

Adding host entries to a forward lookup zone

Procedure

1. On the left side of the **DNS Manager** window, select the applicable forward lookup zone. Then right-click the zone and select **New Host (A or AAAA)**.
2. In the **New Host** window:
 - In the **Name** field, type the hostname for the entry. For example:
 - If you're using a forward lookup zone created specifically for the S Series Node, type `*` or `admin`.
 - If you're using a different forward lookup zone, type `*` or `admin` followed by the S Series Node domain name (for example, `*.s-node-1` or `admin.s-node-1`).
 - In the **IP address** field, type the IP address for the entry.
 - To add the IP address to a reverse lookup zone that already exists, select **Create associated pointer (PTR) record**.Then click **Add Host**.
3. In response to the confirming message, click **OK**.

If you selected **Create associated pointer (PTR) record** and the reverse lookup zone does not exist, the host entry is added to the forward lookup zone but not to a reverse lookup zone.
4. Take either of these actions:
 - To add another host entry, repeat steps 2 and 3.
 - If you're done adding host entries, click **Done**.

Configuring a forward lookup zone in Unix

With BIND in Unix, zones are defined in the `/etc/named.conf` file on the DNS servers. In this file, the statement that defines the forward lookup zone to be used for an S Series Node must include:

- A domain name:
 - If the zone is specifically for an S Series Node, the domain name looks something like `s-node-1.example.com`.
 - If you're using an existing domain, the domain name looks something like `example.com`.
- The zone type (master).
- The name of the file containing the A records for the zone. The A records specify the host entries for the zone.

Each A record for an S Series Node associates an S Series Node interface or the wildcard (*) with the IP address of one of the S Series Node server modules on one of the S Series Node networks.

Each fully qualified domain name that can be used for access to an S Series Node is the concatenation of the hostname in an A record with the specified domain name. For example:

- If the domain name is `s-node-1.example.com`, the hostname for the Management Console is `admin` by itself.
 - If the domain name is `example.com`, the hostname for the Management Console is `admin.s-node-1`.
- A specification not to allow dynamic updates of the A records.

Here's a sample zone statement that defines a forward lookup zone specifically for the S Series Node with domain name `s-node-1.example.com`:

```
zone "s-node-1.example.com" {
    type master;
    file "/var/named/data/s-node-1.example.com";
    allow-update {none;};
};
```

Here are sample contents for the file named in the zone statement above:

```
$TTL 900
@      IN SOA dnsserver.example.com. dns-admin.example.com. (
        1412260762    ; serial
        10800         ; refresh  (3 hours)
        15            ; retry   (15 seconds)
        304800        ; expire  (1 week)
        10800         ; minttl  (3 hours)
    )
; Name Servers
```

```
@      IN          NS           dnsserver.example.com.
;Zone Data

admin      IN      A      10.0.0.3
admin      IN      A      10.0.0.4
mapi       IN      A      10.0.0.3
mapi       IN      A      10.0.0.4
hs3        IN      A      10.0.0.3
hs3        IN      A      10.0.0.4
```

In the sample file above, the admin, mapi, and hs3 hosts are all associated with the virtual IP addresses of the server modules on the access network.

If the forward lookup zone is not specifically for the S Series Node, the A records in the file look something like this:

```
admin.s-node-1      IN      A      10.0.0.3
admin.s-node-1      IN      A      10.0.0.4
mapi.s-node-1       IN      A      10.0.0.3
mapi.s-node-1       IN      A      10.0.0.4
hs3.s-node-1        IN      A      10.0.0.3
hs3.s-node-1        IN      A      10.0.0.4
```

Verifying the DNS configuration

You can verify that an S Series Node primary zone is working properly from either a Windows command-prompt window or a Unix shell. In both cases, you can use either the `dig` or `nslookup` command, depending on which is available.

The syntax for verifying the primary zone configuration is:

```
{dig|nslookup} {admin|mapi|hs3|*}.node-domain-name
```

The response to this command should be a list of the server module IP addresses specified for the requested interface in the S Series Node forward lookup zone.

Here's an example of the command and response in Windows:

```
C:\>nslookup admin.s-node-1.example.com
Server:  dnsserver.example.com
Address: 10.0.201.55

Name:    admin.s-node-1.example.com
Addresses: 10.0.0.3
           10.0.0.4
```

If you don't see the expected IP addresses, the zone is not defined correctly.

Chapter 5: HCP S11 and S31 Node hardware

HCP S11 and S31 Nodes use the same hardware and have the same hardware considerations.

S11 and S31 Node hardware components

An *enclosure* is a container for drives that store data written to the S11 or S31 Node and drives that store the S11 or S31 Node internal database. An HCP S11 Node includes one *base enclosure* and, optionally, one *expansion enclosure*. An HCP S31 Node includes one base enclosure and, optionally, up to eight expansion enclosures. The base enclosure for both S11 and S31 Nodes contains the two server modules that run the HCP S Series software.

Each enclosure has a *main bay* and a *controller bay*. The main bay holds most of the drives. The controller bay holds the server modules (base enclosure) or I/O modules (expansion enclosures) and some additional drives.

Enclosure hardware

Each enclosure includes the hardware listed below.

Rail kit

The rail kit, with left and right rails, is used to mount the enclosure in a rack. The rail kit includes inner mounting rails that attach to the enclosure and outer mounting rails that attach to the rack.

Cable management arm

The cable management arm is used to neatly arrange the power cables that connect the enclosure to the power distribution units (PDUs), the SAS cables that connect expansion enclosures to other enclosures, and, for base enclosures only, the network cables that connect the server modules to your networking infrastructure. The cable management arm also keeps the cables securely connected to the enclosure when the enclosure is pulled partway out of the rack for service.

The cable management arm comes with two brackets, one that attaches to the enclosure and one that attaches to the right outer mounting rail.

The cable management arms differ for base and expansion enclosures.

Stabilizer bar

The stabilizer bar, which is attached to the left and right outer mounting rails at the rear of the rack, provides support for the rails.

Two power supplies

The two redundant power supplies at the rear of the enclosure provide power for the enclosure. Each 3200W power supply in a base enclosure has two inlets to provide the extra level of power required by the server modules. Each 2000W power supply in an expansion enclosure has one inlet.

The power supplies are not interchangeable between base and expansion enclosures.

The newest power supplies are ecodesign-compliant power supplies that comply with the European Union (EU) ecodesign regulations regarding active efficiency and no-load power consumption. These power supplies are required in S11 and S31 Nodes located in EU member countries.

Four rear fans

The four fans at the rear of the enclosure provide cooling for the drives and SAS expanders in the main bay.

Two controller-bay fans

In base enclosures, the fans in the controller bay provide cooling for the server modules, personality modules, and drives in the controller bay. In expansion enclosures, the fans in the controller bay provide cooling for the I/O modules and drives in the controller bay.

The controller-bay fans are not interchangeable between base and expansion enclosures.

Data drives

These 10TB, 14TB, 16TB, 18TB, or 20TB SAS hard disk drives (HDDs), with drive carriers, store object data and object and system metadata. A base enclosure holds 30, 62, or 94 data drives, all in the main bay. An expansion enclosure holds 42, 74, or 106 data drives, 10 in the controller bay and the rest in the main bay.

Six database drives (base enclosures only)

These 400GB or 800GB SAS solid state drives (SSDs), with drive carriers, store the internal database used by the S11 or S31 Node to hold information such as user-account and bucket definitions and various configuration settings. Database drives also store information that helps ensure high availability and data reliability. In the remaining space, database drives can store object data and object and system metadata.

Four of the database drives are in small form factor (SFF) drive carriers in the controller bay. The other two are in large form factor (LFF) drive carriers in the main bay.

Two personality modules (base enclosures only)

Each of the two personality modules, located in the controller bay, provides connectivity between one of the server modules and the drives in the base enclosure. Each personality module contains a SAS controller and two SAS expanders.

Two I/O modules (expansion enclosures only)

The two I/O modules, located in the controller bay, enable communication with the drives in that enclosure. Each I/O module contains two SAS expanders and has four 4-lane 12Gb SAS ports.

Each I/O module also has one serial port, which can be used for diagnostic functions, and two Ethernet ports, which are not used with an S11 or S31 Node.

Eight SAS expanders

The eight SAS expanders in the main bay connect the personality modules (base enclosures) or I/O modules (expansion enclosures) to the drives in the main bay.

The SAS expanders are configured in four pairs. One SAS expander in each pair connects one of the personality or I/O modules to 24 drives. The other SAS expander in each pair connects the other personality or I/O module to the same 24 drives.

Four 12Gb SAS ports (base enclosures only)

The four 4-lane SAS ports on the back of the enclosure are used to connect the base enclosure to the I/O modules in an expansion enclosure.

Four IEC 320 C13 to IEC 320 C14 power cables with up-angle connectors (base enclosures only)

These power cables are used to connect the power supplies in a base enclosure to two different PDUs. For all regions except India, two of the cables are 6 feet (1.83 meters) long, and two are 8 feet (2.44 meters) long. For India, all four cables are 2.4 meters long.

Four IEC 320 C13 to IEC 320 C14 power cable extensions (base enclosures only)

These power cable extensions, which are 2.3 feet (0.7 meters) long in all regions, are used only if the base-enclosure power cables aren't long enough to reach the applicable PDU outlets.

Two IEC 320 C19 to IEC 320 C20 power cables with left-angle connectors (expansion enclosures only)

These power cables are used to connect the power supplies in an expansion enclosure to two different PDUs. For all regions except India, one of the cables is 6 feet (1.83 meters) long, and the other is 8 feet (2.44 meters) long. For India, both cables are 2.4 meters long.

Two IEC 320 C19 to IEC 320 C20 power cable extensions (expansion enclosures only)

These power cable extensions, which are 3 feet (0.91 meters) long in all regions, are used only if the expansion-enclosure power cables aren't long enough to reach the applicable PDU outlets.

Two 4-meter SAS cables (expansion enclosures only)

The two SAS cables are used to connect the expansion enclosure either to the base enclosure or to two other expansion enclosures.

Server module hardware

Each of the two server modules in an S11 or S31 Node includes the hardware listed below.

One (S11 Nodes) or two (S31 Nodes) CPUs

These CPUs provide the processing power for the server module.

Two (S11 Nodes) or eight (S31 Nodes) 32GB memory cards

These memory cards provide an S11 Node with a total of 64 GB of RAM. They provide an S31 Node with a total of 256 GB of RAM.

Two 256GB M.2 SSDs

The two SSDs store the HCP S Series operating system (OS). They also store logs and software used by the S11 or S31 Node.

One four-port 12Gb SAS PCI Express (PCIe) card (S31 Nodes only)

The four ports on the SAS PCIe card are used to connect the server module to an I/O module in one or two expansion enclosures.

Four onboard 10Gb Ethernet SFP+ ports

The four onboard 10Gb SFP+ ports are used for the access network, which provides external access to the S11 or S31 Node for data access and, optionally, management purposes.

If the optional two-port or four-port Ethernet PCIe cards are installed in the server modules, the four onboard 10Gb SFP+ ports are not used.

Optionally, one two-port 25Gb Ethernet SFP28 PCIe card

The optional 25Gb Ethernet SFP28 PCIe card has two ports that can be used for the access network in place of the four onboard 10Gb SFP+ ports.

If this card is installed in the server module, the S11 or S31 Node uses the two 25Gb Ethernet SFP28 ports on the card for the access network.

With this option, one two-port 25Gb Ethernet SFP28 PCIe card should be installed in each server module.

Optionally, one four-port 10GBase-T Ethernet PCIe card

The optional 10GBase-T Ethernet PCIe card has four ports that can be used for the access network in place of the four onboard 10Gb SFP+ ports.

If this card is installed in the server module, the S11 or S31 Node uses the four 10GBase-T Ethernet ports on the card for the access network.

With this option, one four-port 10GBase-T Ethernet PCIe card should be installed in each server module.



Note: To facilitate switching between the two-port and four-port Ethernet PCIe cards in the server modules, the S11 and S31 Nodes support having the two-port card in one server module and the four-port card in the other server module at the same time.

One onboard 1000Base-T Ethernet port

The onboard 1000Base-T port is used for the management network, which provides external access to the S11 or S31 Node for management purposes.

One USB 3.0 port

The USB port lets you connect USB devices to the server module. A USB hub is required for connecting multiple USB devices to the server module at the same time (for example, for connecting a keyboard and the installation USB flash drive during installation of the HCP S Series OS and software).

One serial port

The serial port lets you connect a laptop computer to the server module at the customer site for the purpose of reinstalling the HCP S Series OS and software or performing other service functions.

One Micro HDMI port

The Micro HDMI port lets you connect a VGA monitor to the server module by means of a Micro HDMI to VGA adapter. The monitor is used, for example, to display the server module console during the installation of the HCP S Series OS and software.

Additional hardware

Additionally, an S11 or S31 Node comes with the items listed below.

One Micro HDMI to VGA adapter

Used for connecting a VGA monitor to the Micro HDMI port on a server module

One four-port USB hub

Used for connecting multiple USB devices to a server module at the same time

One USB flash drive

Used by authorized service providers to perform maintenance procedures at the customer site

One serial cable

Used for connecting a laptop computer to a server module or I/O module

S11 and S31 Node product offerings

An S11 or S31 Node comes with one base enclosure and, optionally, one expansion enclosure (S11 Nodes) or one through eight expansion enclosures (S31 Nodes). Each enclosure contains an initial set of drives and, optionally, one or two capacity upgrade drive sets:

- The initial drive set for a base enclosure consists of 30 data drives and six database drives.
- The initial drive set for an expansion enclosure consists of 42 data drives.
- A capacity upgrade drive set consists of 32 data drives.

Data drives are 10TB, 14TB, 16TB, 18TB, or 20TB HDDs. Database drives are 400GB or 800GB SSDs.

The tables below show information about the initial drive sets and capacity upgrade drive set for 10TB, 14TB, 16TB, 18TB, and 20TB drives. Each table shows the information listed below.

Total raw capacity

The total of the manufacturer-specified capacities of the data drives.

Total storage

The total amount of storage that the S11 or S31 Node can use for storing, protecting, and repairing object data and object and system metadata. For the base-enclosure initial drive set, total storage includes the space that can be used for data and metadata on the database drives.

Total storage is not the same as the amount of data that can be written to an S11 or S31 Node. The space required for metadata, protection, and repair reduces the amount of storage available for the data written to the S11 or S31 Node. However, single-instancing of data enables the amount of data written to exceed the total amount of storage.

Licensable storage

The maximum amount of storage that can be licensed on the S11 or S31 Node. This value is the amount of storage available for storing and repairing object data and object and system metadata. Licensable storage does not include the additional storage required for protecting data and metadata. For the base-enclosure initial drive set, licensable storage includes the space that can be used for data and metadata on the database drives.

10TB data drives

Drive set	Total raw capacity (data drives only) ¹	Total storage ²	Licensable storage ¹
Base-enclosure initial drive set with 400GB database drives	300 TB	273.13 TB	231 TB
Base-enclosure initial drive set with 800GB database drives	300 TB	275.30 TB	233 TB
Expansion-enclosure initial drive set	420 TB	380.48 TB	322 TB
Capacity upgrade drive set	320 TB	289.89 TB	245 TB
Notes:			
1. The values for total raw capacity and licensable storage are base 10 (that is, they are multiples of 1,000).			
2. The values for total storage are base 2 (that is, they are multiples of 1,024).			

14TB data drives

Drive set	Total raw capacity (data drives only) ¹	Total storage ²	Licensable storage ¹
Base-enclosure initial drive set with 400GB database drives	420 TB	381.82 TB	323 TB
Base-enclosure initial drive set with 800GB database drives	420 TB	383.99 TB	325 TB
Expansion-enclosure initial drive set	588 TB	532.65 TB	451 TB
Capacity upgrade drive set	448 TB	405.83 TB	343 TB
Notes:			
1. The values for total raw capacity and licensable storage are base 10 (that is, they are multiples of 1,000).			
2. The values for total storage are base 2 (that is, they are multiples of 1,024).			

16TB data drives

Drive set	Total raw capacity (data drives only) ¹	Total storage ²	Licensable storage ¹
Base-enclosure initial drive set with 400GB database drives	480 TB	436.18 TB	369 TB
Base-enclosure initial drive set with 800GB database drives	480 TB	438.36 TB	371 TB
Expansion-enclosure initial drive set	672 TB	608.75 TB	515 TB
Capacity upgrade drive set	512 TB	463.81 TB	392 TB
Notes:			
1. The values for total raw capacity and licensable storage are base 10 (that is, they are multiples of 1,000).			
2. The values for total storage are base 2 (that is, they are multiples of 1,024).			

18TB data drives

Drive set	Total raw capacity (data drives only) ¹	Total storage ²	Licensable storage ¹
Base-enclosure initial drive set with 400GB database drives	540 TB	490.51 TB	415 TB
Base-enclosure initial drive set with 800GB database drives	540 TB	492.69 TB	417 TB
Expansion-enclosure initial drive set	756 TB	684.82 TB	579 TB
Capacity upgrade drive set	576 TB	521.76 TB	441 TB
Notes:			
1. The values for total raw capacity and licensable storage are base 10 (that is, they are multiples of 1,000).			
2. The values for total storage are base 2 (that is, they are multiples of 1,024).			

20TB data drives

Drive set	Total raw capacity (data drives only) ¹	Total storage ²	Licensable storage ¹
Base-enclosure initial drive set with 400GB database drives	600 TB	544.87 TB	461 TB
Base-enclosure initial drive set with 800GB database drives	600 TB	547.05 TB	463 TB
Expansion-enclosure initial drive set	840 TB	760.92 TB	644 TB
Capacity upgrade drive set	640	579.75 TB	490 TB
Notes:			
1. The values for total raw capacity and licensable storage are base 10 (that is, they are multiples of 1,000).			
2. The values for total storage are base 2 (that is, they are multiples of 1,024).			

Approximate total storage on an S11 or S31 Node

To estimate the total storage on an S11 or S31 Node, add together the storage provided by the applicable drive sets. Here are some examples of total storage, where the totals are calculated using exact numbers of bytes and then rounded to terabytes instead of being calculated using the rounded values shown in the tables above:

- The total storage on a two-enclosure S11 Node that uses 10TB data drives and 400GB database drives and has two capacity upgrade drive sets in each enclosure is approximately 1,813.18 TB.
- The total storage on a five-enclosure S31 Node that uses 14TB data drives and 800GB database drives and has two capacity upgrade drive sets in each of the first four enclosures and one capacity upgrade drive set in the fifth enclosure is approximately 6,167.07 TB.
- The total storage on a nine-enclosure S31 Node that uses 16TB data drives and 800GB database drives and has two capacity upgrade drive sets in each enclosure is approximately 13,657.12 TB.
- The total storage on a nine-enclosure S31 Node that uses 18TB data drives and 800GB database drives and has two capacity upgrade drive sets in each enclosure is approximately 15,363.12 TB.
- The total storage on a nine-enclosure S31 Node that uses 20TB data drives and 800GB database drives and has two capacity upgrade drive sets in each enclosure is approximately 17,070.09 TB.

Racking options

If your order for one or more S11 or S31 Nodes includes a rack, a Hitachi Universal V3 Rack is shipped to your site with no more than three S11 or S31 Node enclosures already installed in the rack. If the total number of enclosures for the S11 or S31 Nodes included in the order is greater than three, each additional enclosure is packaged and shipped separately from the rack. These additional enclosures must be racked at your site.

If your order includes PDUs in addition to a rack, the PDUs are also installed in the rack before the rack is shipped.

If your order doesn't include a rack, the customer must supply a Universal V3 Rack, a Universal V2B Rack, a Universal V2 Rack, or another rack that meets the rack requirements for one or more S11 or S31 Nodes. In this case, all the enclosures for the S11 or S31 Nodes included in the order must be racked at your site.

To accommodate the depth of the S11 or S31 Node enclosures, each rack included in your order is modified before any enclosures are mounted in that rack. The modifications include repositioning the front vertical mounting rails in the rack.

Customer-supplied Hitachi Universal Racks must be modified on site if they cannot already accommodate the depth of the your order for one or more S11 or S31 Node enclosures. Other customer-supplied racks may also need to be modified on site.

If an S11 or S31 Node includes one or more expansion enclosures, the base and expansion enclosures must be mounted in the same rack. The expansion enclosures must be racked above the base enclosure. To allow for cable management, exactly one rack unit must be left empty between the base enclosure and the lowest expansion enclosure.

Multiple S11 or S31 Nodes can be installed in the same rack. However, to allow for future growth of an S11 or S31 Node, you can choose to install that model in its own rack.

S11 or S31 Nodes can be mounted in the same rack as components of other products, as long as the rack has enough available space, weight capacity, and power capacity to accommodate the S11 or S31 Node enclosures and the other mounted components. In this case, the S11 or S31 Node enclosures must be mounted at the bottom of the rack, with all components of other products mounted above them.

A customer-supplied Hitachi Universal Rack may already contain components of products other than S11 or S31 Nodes. Before any S11 or S31 Node enclosures can be mounted in the rack, those other components must be temporarily removed from the rack while the front vertical mounting rails in the rack are repositioned. Existing components must also be temporarily removed from other customer-supplied racks that require similar modification.

Connectivity options

An S11 or S31 Node has two networks for connecting to your networking infrastructure: an access network and a management network. Both the access network and the management network can be used for management functions. Only the access network can be used for data access.

Access network

For the access network, each server module comes with four bonded onboard 10Gb Ethernet SFP+ ports. These ports can be used only if the networking infrastructure supports SFP+. If the networking infrastructure does not support SFP+:

- For an SFP28 networking infrastructure, a two-port 25Gb Ethernet SFP28 PCIe card must be installed in each server module.
- For a 10GBase-T networking infrastructure, a four-port 10GBase-T Ethernet PCIe card must be installed in each server module.

If either Ethernet PCIe card is present in the server modules, the S11 or S31 Node uses the ports on those cards for the access network. If the server modules do not contain Ethernet PCIe cards, the S11 or S31 Node uses the onboard SFP+ ports for the access network.

In any case, the access network ports can be configured as active-active (802.3ad) or active-backup. To create a highly available infrastructure, the ports can be connected to different physical switches.

You can choose not to connect one or more of the access network ports to the networking infrastructure. In this case, the S11 or S31 Node uses only the connected ports, with each of those ports either an active port or a backup port, depending on the bonding mode.

Management network

For the management network, each server module has one 1Gb Ethernet 1000Base-T port. You can choose not to connect the management port. In this case, only the access network is available for management functions.

Available additional components

To meet your network connectivity requirements when the onboard SFP+ ports are used for the access network, Hitachi Vantara offers the additional components listed below.

25Gb SFP28 optical transceiver

If you have a 25Gb Ethernet network and are using fiber optic cables for the access network connections, a 25Gb SFP28 optical transceiver is required on both ends of each fiber optic cable. The 25Gb SFP28 optical transceiver has an LC type connector. Hitachi Vantara offers a 25Gb SFP28 optical transceiver from Intel.

The Intel 25Gb SFP28 optical transceiver is the only SFP28 optical transceiver supported for use with an S11 or S31 Node.

10Gb SFP+ optical transceiver

If you have a 10Gb Ethernet network and are using fiber optic cables for the access network connections, a 10Gb SFP+ optical transceiver is required on both ends of each fiber optic cable. The 10Gb SFP+ optical transceiver has an LC type connector. Hitachi Vantara offers a 10Gb SFP+ optical transceiver from Intel.

The Intel 10Gb SFP+ optical transceiver is the only SFP+ optical transceiver supported for use with an S11 or S31 Node.

Multimode fiber optic cable

If you have a 25Gb or 10Gb Ethernet network and the distance between the server modules and the Ethernet switches is greater than 10 meters, fiber optic cables must be used for the access network connections. Hitachi Vantara offers multimode fiber optic cables in various lengths in both plenum and LSZH jacketing.

25Gb or 10Gb Twinax cable

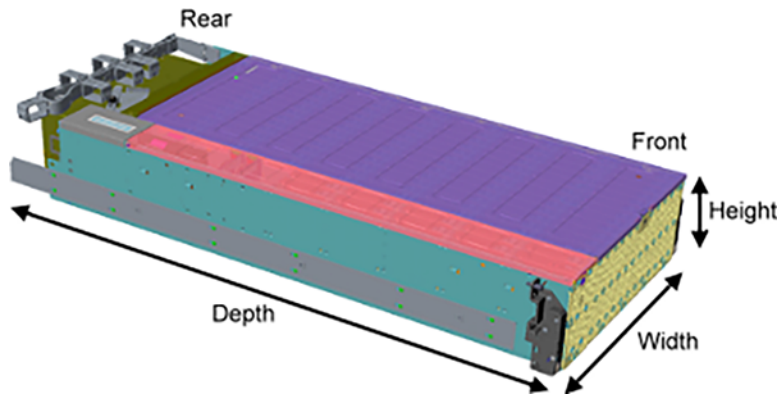
If you have a 25Gb or 10Gb Ethernet network and the distance between the server modules and the Ethernet switches is less than 10 meters, Twinax cables can be used instead of fiber optic cables for the access network connections. Hitachi Vantara offers 25Gb Twinax cables in various lengths up to five meters and 10Gb Twinax cables in various lengths. The Twinax cables come from both Brocade and Cisco.

Mechanical details

The topics below describe the mechanical specifications and requirements for HCP S11 or S31 Nodes.

Enclosure dimensions

The figure below shows an S11 or S31 Node base or expansion enclosure. Use this figure as a reference for the table of dimensions that follows.



The table below shows the physical dimensions of the enclosures.

Measurement	Inches	Millimeters
Width of enclosure, excluding front side brackets and inner mounting rails	17.37	441.0
Width of enclosure, including front side brackets and inner mounting rails	19.00	482.6
Depth of enclosure, from front of enclosure to rear end of inner mounting rails	45.04	1,144.0
Depth of handle assembly, equal to the depth of the part of the enclosure that extends beyond the front vertical mounting rails when the enclosure is all the way back in the rack	2.33	59.0
Depth of the part of the enclosure that extends beyond the front vertical mounting rails when the enclosure is extended as far as possible out of the rack; enclosure handles folded up	37.13	943.0
Depth of the part of the enclosure that extends beyond the front vertical mounting rails when the enclosure is extended as far as possible out of the rack; enclosure handles extended	40.26	1,022.4
Depth of the part of the enclosure that extends beyond the front face of the rack when the enclosure is extended as far as possible out of the rack; enclosure handles folded up	34.13	866.8
Depth of the part of the enclosure that extends beyond the front face of the rack when the enclosure is extended as far as possible out of the rack; enclosure handles extended	37.26	946.2

Measurement	Inches	Millimeters
Height of base enclosure without cable management arm or expansion enclosure with or without cable management arm; requires 4U in the rack	7.01	178.0
Height of base enclosure with cable management arm; requires 5U in the rack	8.76	222.5

Enclosure weights

The table below shows the weights of the building blocks for an S11 or S31 Node. The enclosure weights include the weights of the applicable initial drive set, the enclosure mounting rails, the applicable cable management arm, and the enclosure power cables.



Note: The power cables used in calculating the enclosure weights are for all regions except India. For India, add 0.4 lbs (0.18 kg) to the weight of a base enclosure. Add 0.2 lbs (0.09 kg) to the weight of an expansion enclosure.

The weight of each base enclosure includes the weight of the two server modules installed in the enclosure, with the optional two-port 25Gb Ethernet SPF28 PCIe card or four-port 10GBase-T Ethernet PCIe card and, for S31 Nodes only, the SAS PCIe card installed in each server module.

The weight of the expansion enclosure includes the weight of the two SAS cables that connect the enclosure to one or two lower-numbered enclosures.

The 10TB, 14TB, 16TB, 18TB, and 20TB data drives weigh the same as each other. The 400GB database drives weigh slightly less than the 800GB database drives. The weights in the table below include the weight of the 800GB database drives.

Enclosure	Weight in lbs	Weight in kg
S11 Node base enclosure	191.68	86.94
S31 Node base enclosure	195.87	88.85
Expansion enclosure	168.19	76.29
Capacity upgrade drive set	52.91	24.00

To calculate the total weight of an S11 or S31 Node, add together the weights of the applicable components. For example:

- A two-enclosure S11 Node that has two capacity upgrade drive sets in each enclosure weighs, in pounds, $191.68 + 168.19 + 4(52.91)$, which equals 571.51 (259.23 kg).
- A five-enclosure S31 Node that has two capacity upgrade drive sets in each of the first four enclosures and one capacity upgrade drive set in the fifth enclosure weighs, in pounds, $195.87 + 4(168.19) + 9(52.91)$, which equals 1,344.82 (610.00 kg).
- A nine enclosure S31 Node that has two capacity upgrade drive sets in each enclosure weighs, in pounds, $195.87 + 8(168.19) + 18(52.91)$, which equals 2,493.77 (1,131.16 kg).

Rack dimensions

The table below shows the physical dimensions of the Hitachi Universal V3 Rack used with S11 and S31 Nodes. The dimensions are the same for the Universal V2B Rack and Universal V2 Rack, both of which can also be used with an S11 or S31 Node.

Measurement	Inches	Millimeters
Width	23.62	600.00
Depth	47.24	1,200.00
Height	79.93	2,030.30

Rack and PDU weights

The table below shows the weights of an empty Hitachi Universal V3 Rack, an empty Universal V2B Rack, an empty Universal V2 Rack, the PDUs that can be used with S11 or S31 Nodes in these racks, and the power cable extensions that may be needed when multiple S11 or S31 Node enclosures are mounted in a single rack.

The rack weights include the side panels, front and rear doors, rear service tray, and accessory kit. The weight for a Universal V3 Rack also includes the door-open arm and bracket and the PDU brackets.

A rack containing one or more S11 or S31 Nodes normally has six PDUs installed in it.

Component	Weight in lbs	Weight in kg
Hitachi Universal V3 Rack	302.70	137.30
Hitachi Universal V2B Rack, excluding brake handle	234.53	106.38
Brake handle for Hitachi Universal V2B Rack	2.00	0.91
Hitachi Universal V2 Rack	225.53	102.30
Americas single-phase PDU for Universal V3 Rack	6.79	3.10

Component	Weight in lbs	Weight in kg
Americas three-phase PDU for Universal V3 Rack	8.21	3.73
EMEA/APAC single-phase PDU for Universal V3 Rack	5.51	2.50
EMEA/APAC three-phase PDU for Universal V3 Rack	5.86	2.66
Americas single-phase PDU for Universal V2B Rack or Universal V2 Rack	7.94	3.60
Americas three-phase PDU for Universal V2B Rack or Universal V2 Rack	8.82	4.00
EMEA/APAC single-phase PDU for Universal V2B Rack or Universal V2 Rack	7.05	3.20
EMEA/APAC three-phase PDU for Universal V2B Rack or Universal V2 Rack	7.05	3.20
Base-enclosure power-cable extension for all regions	0.31	0.14
Expansion-enclosure power-cable extension for all regions	0.99	0.45

Electrical details

The topics below describe the power requirements and electrical specifications for S11 and S31 Nodes.

Power system

For maximum redundancy in the power system for an HCP S11 or S31 Node:

- The two power supplies in each enclosure should be plugged into two different PDUs.
- The two PDUs should be plugged into two different power sources.

This setup ensures that the entire power system has no single point of failure.

If only one power source is available, the two power supplies for an enclosure should be connected to separate circuits. If only one circuit is available, the two power supplies can be connected to the same PDU as a last resort, assuming the PDU has two available outlets and enough power capacity.

In any case, the power sources and PDUs used with an S11 or S31 Node must deliver the required amount of electricity:

- In the Americas geography: 208 volts
- In the EMEA/APAC geography, with single-phase PDUs: 230 volts
- In the EMEA/APAC geography, with three-phase PDUs: 400 volts

Each PDU must be powered from an appropriately rated circuit.

The power system input can be single-phase or three-phase.

Electrical connections

In a base enclosure, each power supply has two IEC 320 C14 inlets and requires a PDU with at least two IEC 320 C13 outlets. To connect the power supplies to the PDUs, you need four IEC 320 C13 to IEC 320 C14 power cables.

In an expansion enclosure, each power supply has one IEC 320 C20 inlet and requires a PDU with at least one IEC 320 C19 outlet. To connect the power supplies to the PDUs, you need two IEC 320 C19 to IEC 320 C20 power cables.

PDUs

If your order includes both a rack and PDUs, six PDUs come already installed in the rack. If the order doesn't include a rack, the PDUs are shipped separately.

If your order doesn't include PDUs, you must supply Hitachi PDUs of the applicable type or other PDUs that meet the PDU requirements for S11 and S31 Nodes.

The Hitachi PDUs used with Hitachi Universal Racks that hold one or more S11 or S31 Nodes are the short, single-phase or three-phase PDUs. In either case, the outlets on the PDUs are single-phase. The specific PDU model used depends on the input-phase requirements, on where the S11 or S31 Node is located, and on the rack model.

PDUs for the Hitachi Universal V3 Rack

The table below shows information about the Hitachi PDUs that can be used with S11 and S31 Nodes in a Hitachi Universal V3 Rack.

Geography	Phase	Housing length	Description	C13 outlets	C19 outlets
Americas	Single	23.4 in. (594 mm)	208V, 30A, NEMA L6-30P	10	2
Americas	Three	24 in. (611 mm)	208V, 30A, NEMA L15-30	8	3
EMEA/APAC	Single	21.8 in. (554 mm)	230V, 32A, IEC309 2P+E	10	2
EMEA/APAC	Three	23.5 in. (596 mm)	400V, 16A, IEC309 3P+N+E	9	3

PDUs for the Hitachi Universal V2B Rack or Universal V2 Rack

The table below shows information about the Hitachi PDUs that can be used with S11 or S31 Nodes in a Hitachi Universal V2B Rack or Universal V2 Rack.

Geography	Phase	Length	Description	C13 outlets	C19 outlets
Americas	Single	24.49in (622mm)	208V, 30A, NEMA L6-30P	8	3
Americas	Three	24.49in (622mm)	208V, 30A, NEMA L15-30	8	3
EMEA/APAC	Single	23.46in (596mm)	230V, 32A, IEC309 2P+E	9	3
EMEA/APAC	Three	23.46in (596mm)	400V, 16A, IEC309 3P+N+E	9	3

Power connections

The power connections on the Hitachi PDUs used with the Hitachi Universal Racks differ by region and input phase:

- For the Americas:
 - The single-phase, 208V, 30A PDU has a NEMA L6-30P three-wire plug.



- The three-phase, 208V, 30A PDU has a NEMA L15-30 four-wire plug.



- For EMEA/APAC:
 - The single-phase, 230V, 32A PDU has an IEC 309 three-wire plug.



- The three-phase, 400V, 32A PDU has an IEC 309 five-wire power plug.



Electrical specifications

Base enclosures and expansion enclosures for S11 and S31 Nodes have two power supplies each. However, the power supplies differ between the two types of enclosures:

- To accommodate the power requirements of the server modules, each power supply in a base enclosure has two cores.
- Each power supply in an expansion enclosure has one core.

When an enclosure is operating normally, each power supply supplies half the power that the enclosure requires. However, if one power supply is unavailable, the enclosure can run on the other power supply alone.

Base enclosure

The table below shows the electrical specifications for a power supply in a base enclosure.

Parameter	Value
Input voltage	100 VAC to 240 VAC
Input frequency	50 Hz to 60 Hz
Maximum input current (two cores)	18 A at 208 VAC
Typical input current (two cores)	8.28 A at 208 VAC
Maximum average power (two cores)	3,200 W
Peak inrush current (5 ms)	55 A
Minimum efficiency per core (1,600 W at 100% TDC)	93%
Minimum efficiency per core (643 W at 20% TDC)	92%
Maximum average output power per core	1,600 W
Maximum peak output power per core (10ms)	2,379 W
Typical average output power per core	800 W
Maximum AC leakage current	< 1 mA
Harmonics, emissions, and immunity	Meets IEC EN61000-3-2 (EU)

Expansion enclosure

The table below shows the electrical specifications for a power supply in an expansion enclosure.

Parameter	Value
Input voltage	200 VAC to 240 VAC
Input frequency	50 Hz to 60 Hz
Maximum input current	11.5 A at 208 VAC
Typical input current	5.11 A at 208 VAC

Parameter	Value
Peak inrush current (5 ms)	55 A
Minimum efficiency (2,000 W @100% TDC)	91%
Minimum efficiency (400 W @20% TDC)	93%
Maximum average output power	2,000 W
Maximum peak output power (10 ms)	2,379 W
Typical average output power	1,000 W
Maximum AC leakage current	< 1 mA
Harmonics, emissions, and immunity	Meets IEC EN61000-3-2 (EU), EN31000-3-3 (EU), EN55024 (EU), and KN24/KN35 (S. Korea)

Environmental details

The topics below describe the environmental specifications and requirements for S11 and S31 Nodes.

RoHS compliance

S11 and S31 Nodes, including all their components, are compliant with the European Union Restriction of Hazardous Substances (RoHS) Directive (Directive 2011/65/EU), with no exceptions or exemptions.

BNST compliance

The lubricants used in S11 and S31 Node components do not contain any benzenamine, *N*-phenyl-, reaction products with styrene and 2,4,4-trimethylpentene (BNST) and are, therefore, compliant with the Canadian Prohibition of Certain Toxic Substances Regulations, 2012.

Temperature, humidity, and altitude

The table below shows the acceptable ranges for temperature and humidity and the derating for altitude for an S11 or S31 Node base or expansion enclosure under these conditions:

- Normal operation
- Powered off in a data center

Parameter	Operating	Powered off
Temperature*	5°C to 35°C (41°F to 95°F)	-40°C to 70°C (-40°F to 158°F)
Relative humidity (noncondensing)	80%	100%
Altitude	-100 m to 3,048 m (-328 ft to 10,000 ft)	-100 m to 12,192 m (-328 ft to 40,000 ft)
*The maximum operating temperature value is specified at 900 meters and is derated 1°C per 300 meters of increased altitude (ASHRAE 2015 Class A2).		

Shock and vibration

The table below shows the tested limits for shock and vibration for an S11 or S31 Node base or expansion enclosure. The measurements in the table apply to fully populated enclosures (that is, enclosures that contain the applicable initial drive set and two capacity upgrade drive sets).

Parameter	Value
Operating shock	3.0 g, 11 ms per axis
Operating vibration	0.18 Grms, 5Hz to 500Hz, 30 mins per axis
Non-operating shock	20.0 g, 7 ms, 10 shock pulses (2 shocks per X axis and per Y axis in positive and negative directions; 2 shocks on Z axis in positive direction) (ISTA 3H)
Non-operating vibration	0.54 Grms, 6 Hz to 200 Hz (ISTA 3E/3H)

Cooling and airflow

Each S11 or S31 Node enclosure has four rear fans that cool the main bay and two controller-bay fans that cool the controller bay. For effective cooling in each bay, the applicable cover must be on the enclosure. At any given time, an enclosure can tolerate at most a single fan failure in one bay or concurrent single fan failures in the main bay and controller bay.

The airflow in S11 and S31 Node enclosures is from front to back in both the main bay and the controller bay. To ensure proper airflow, the air pressure at the front of an enclosure must be greater than the air pressure at the rear of the enclosure. The back pressure created by the rear rack door or other obstacles must not exceed 5 Pa (0.5mm H₂O).

Acoustics

The operating sound power level of an S11 or S31 Node enclosure does not exceed 8.5 Bels LWAd @23°C under a fan-failure or cover-open condition.

Chapter 6: Monitoring HCP S11 and S31 Nodes

An HCP S Series Node provides information about its status through a variety of mechanisms:

- The HCP S Series Management Console displays:
 - Information about storage usage on the **Dashboard** page
 - Information about bucket usage on the **BUCKETS** page
 - Detailed information about the S Series Node hardware components and the status of those components on the **HARDWARE OVERVIEW** page and on the pages accessible from that page
 - Messages about events that have occurred on the S Series Node
 - Alerts that notify you about conditions that the S Series Node is currently experiencing

Status information that's available in the Management Console is also available through the HCP S Series management API.

- You can configure the S Series Node to send event log messages, log messages for data access requests, and log messages for management API requests to one or more syslog servers.
- Through the management API, you can get current and historical information about the use of S Series Node storage.
- Through the management API, you can get current information about the load on certain S Series Node resources.
- Through the management API, you can get current and historical information about the load on resources used by various S Series Node processes.
- Many hardware components have LEDs that light up to indicate certain conditions.
- Some LEDs serve as beacons. Beacons enable you to easily identify components in your data center.

You can use the HCP S Series Management Console or management API to turn beaconing on or off for certain components.

- The S Series Node internal logs contain detailed records of the status and activity of various components of the software running on the S Series Node. Error conditions reported in the internal logs can be an indication of hardware issues.

You can use the HCP S Series Management Console or management API to insert comments into or to download the internal logs.

- If in use by an HCP system, the S Series Node notifies that system about certain abnormal conditions as they occur.
- If the Hitachi Remote Ops monitor agent is configured to monitor the S Series Node, the S Series Node sends status information to the monitor agent in response to periodic requests from the agent.

Dashboard

The **Dashboard** page of the HCP S Series Management Console shows information about the storage on the HCP S Series Node:

- The labeled boxes across the top of the page show various current storage statistics:
 - Total storage
 - Used storage
 - Available storage
 - Storage reserved for repair
 - Storage under repair
 - Storage efficiency

Most of the boxes have links to more detailed statistics.

- The bar below the boxes shows storage usage.
- The graphs show three different storage statistics over time:
 - Used storage and ingested data, on a single graph
 - Storage under repair

Storage statistics take both data and database drives into account. However, space used for system overhead on either type of drive is not included in the calculations of storage statistics.

All storage statistics are base 2 (that is, they are multiples of 1,024).



Note: If any SAS cables are disconnected, reported storage statistics may be incorrect.

Total storage

The Total Storage value on the **Dashboard** page is the total amount of storage, in bytes, that can be used for storing, protecting, and repairing object data and object and system metadata. Total storage includes storage only on drives that are known to the S Series Node and are available. If a drive is removed from the S Series Node or becomes unavailable (for example, due to drive failure), the storage on that drive is not included in the calculation of total storage.

When drives are added to the S Series Node, total storage increases. Similarly, when an unavailable drive becomes available, total storage increases.

The Total Storage box has a link to the more detailed statistics listed below.

Raw drive storage

The Raw drive storage value is the total of the vendor-specified capacity, in bytes, of all the data and database drives known to the S Series Node, including both available and unavailable drives. Raw drive storage does not include space partitioned for purposes other than storage. This partitioned space is unavailable to systems that incorporate the drive.

System overhead

The System overhead value is the total amount of storage, in bytes, that the S Series Node reserves for internal purposes on all the data and database drives, including both available and unavailable drives. System overhead includes the internal database, information used in storage management, and information used in data and metadata recovery, should that become necessary.

The amount of space reserved for system overhead on any given drive is fixed and is relative to the amount of raw storage on the drive. On data drives, which have a raw storage amount of 10 TB or higher, system overhead is insignificant, using approximately 0.4 percent of raw capacity. Database drives have a smaller amount of raw storage, under 1 TB. System overhead on a database drive can use as much as 37 percent of raw capacity.

System storage

The System storage value is the total amount of storage, in bytes, that remains when system overhead is subtracted from raw drive storage. System storage includes storage on all drives, both available and unavailable, that are known to the S Series Node.

Unavailable storage

The Unavailable storage value is the total amount of storage, in bytes, on data and database drives that are known to the S Series Node but are currently unavailable. The S Series Node cannot use unavailable storage for any purpose.

Total storage

Total storage equals raw drive storage minus system overhead minus unavailable storage, in bytes. The S Series Node uses system storage for storing, protecting, and repairing object data and object and system metadata.

If no drives are unavailable, total storage equals system storage.

Used storage

The Used Storage value on the **Dashboard** page is the total amount of storage, in bytes, that is currently occupied by object data, object or system metadata, scavenging metadata, or data or metadata protection overhead.

The Used Storage box has a link to the more detailed statistics listed below.

Object data

The Object data value is the total amount of storage, in bytes, that is currently occupied by object data. Object data is the exact digital reproduction of data as it existed before it was stored on the S Series Node.

The Object data value does not include the storage used for the parity chunks the S Series Node generates for object data.

Object and system metadata

The Object and system metadata value is the total amount of storage, in bytes, that is currently occupied by object and system metadata:

- Object metadata is information that describes an object (for example, data size and object creation date).
- System metadata is information that the S Series Node uses to manage the use of allocated storage. Allocated storage is the part of total storage that has been formatted for storing object data, object and system metadata, scavenging metadata, and protection overhead. The S Series Node allocates storage as needed.

The Object and system metadata value does not include the storage used for the parity chunks the S Series Node generates for object and system metadata.

Scavenging metadata

The Scavenging metadata value is the total amount of storage, in bytes, that is currently occupied by metadata that can be used to recover objects whose object metadata has been lost or corrupted.

The S Series Node does not erasure-code scavenging metadata.

Protection overhead

The Protection overhead value is the total amount of storage, in bytes, that is currently used for the parity chunks that the S Series Node generates for object data and object and system metadata.

Used storage

The Used storage value is the sum of the amounts of storage used for object data, for object and system metadata, for scavenging metadata, and for protection overhead, in bytes. However, because the values for these components are derived from used storage rather than directly observed, the values may be inexact. The sum of the component values may therefore differ from the observed used storage value by as much as several megabytes.

The amount of used storage is also shown as a percent of total storage.

Available storage

The Available Storage value on the **Dashboard** page is the total amount of storage, in bytes, that is currently available for storing and protecting object data and object and system metadata. Available storage does not include storage that is reserved for use in repairing damaged storage.

The Available Storage box has a link to the more detailed statistics listed below.

Total storage

The Total storage value is the total amount of storage, in bytes, that can be used for storing, protecting, and repairing object data and object and system metadata. Total storage includes storage on available drives only.

Reserved for repair

The Reserved for repair value is the amount of storage, in bytes, that is reserved for use in repairing damaged or otherwise unavailable storage. The amount of storage reserved for repair depends on the total amount of storage on the S Series Node.

Storage reserved for repair cannot be used for storing and protecting new data.

Used storage

The Used storage value is the total amount of storage, in bytes, that is currently occupied by object data, object or system metadata, scavenging metadata, or data or metadata protection overhead.

Available storage (ideal)

Available storage (ideal) equals total storage minus storage reserved for repair minus used storage, in bytes.

Under repair

The Under repair value is the amount of storage, in bytes, that is in need of repair. Storage needs to be repaired if it is allocated storage on drives that are no longer available (for example, due to a drive failure), regardless of whether that allocated storage contains data.

Available storage

Like Available storage (ideal), Available storage equals total storage minus storage reserved for repair minus used storage, in bytes. However, if the amount of storage under repair is greater than or equal to the ideal amount of available storage, the Available storage value is zero.

The amount of available storage is also shown as a percent of total storage.

With insufficient available storage, the S Series Node cannot ingest any new data.

Reserved for repair

The Reserved for Repair value on the **Dashboard** page is the amount of storage, in bytes, that is currently reserved for use in repairing damaged or otherwise unavailable storage. Storage reserved for repair can be used only for repairing object data and object and system metadata when one or more drives become unavailable. This storage cannot be used for storing and protecting new data.

Reserving storage for repair helps ensure that space is always available for repairing allocated storage on unavailable drives.

The amount of storage reserved for repair is calculated as a percent of total storage relative to the number of drives in the S Series Node. This percent, which can be between as high as five, decreases as drives are added to the S Series Node. If all the storage reserved that was for repair is used, this percent is zero.

Storage reserved for repair is a logical amount of storage. This storage does not have a specific physical location.

When repairing storage, the S Series Node first uses available storage. When no more available storage exists, the S Series Node uses the storage reserved for repair. At this point, the S Series Node cannot ingest any new data.

Under repair

The Under Repair value on the **Dashboard** page is the total amount of storage, in bytes, that is in need of repair. Storage needs to be repaired if it is allocated storage on drives are damaged or otherwise unreachable (for example, due to a drive failure), regardless of whether that allocated storage contains data. While any storage is in need of repair, that storage is referred to as the *repair backlog*.

When a drive with allocated storage becomes unavailable:

- The repair backlog increases by the size of that allocated storage.
- The amount of used storage decreases by the amount of used storage on that allocated storage.

To repair storage, the S Series Node re-creates that storage on available drives. As storage is repaired, the repair backlog decreases, and the amount of used storage increases.

Because allocated storage can contain storage that is not used, as storage is repaired, the repair backlog decreases more quickly than used storage increases. For example, suppose a failed drive has 5 TB of allocated storage. Also suppose that 3 TB of that allocated storage is used. Assuming no additional storage fails, as storage is repaired, the repair backlog decreases from 5 TB to 0 TB, and used storage increases by 3 TB in the same amount of time.

The Under Repair box has a link to the more detailed statistics listed below.

Under repair

The Under repair value is the total amount of storage, in bytes, that is in need of repair.

Repair rate

The Repair rate value is the estimated rate at which the S Series Node is currently working through the repair backlog, in bytes per second. This value is calculated as an average of the rates of repair starting from the most recent increase in the repair backlog and ending at the current time. In other words, when the repair backlog increases, the repair rate is reset to zero, and averaging starts fresh from that time.

If the repair backlog is empty, the repair rate is zero.

Data-access activity on the S Series Node can decrease the repair rate.

Repair time to completion

The Repair time to completion value is the estimated amount of time, in minutes, until the repair backlog is empty. This value is calculated as the size of the current repair backlog divided by the current repair rate. If the repair backlog is empty, the repair time to completion is set to zero.

If the repair rate is zero, the value of Repair time to completion is Unknown.

Projected used storage

The Projected used storage value is the amount of used storage, in bytes, that is estimated to be on the S Series Node when the current repair backlog is empty. Projected used storage is the sum of the current amount of used storage and the amount of used storage on the allocated storage in the repair backlog. The accuracy of projected used storage increases as the amount of storage under repair decreases.

The projected amount of used storage is also shown as a percent of total storage.

Storage efficiency

The Storage Efficiency value on the **Dashboard** page 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 and under-repair storage on the S Series Node.

Normally, due to metadata and to data protection, the amount of storage required to store an object is greater than the size of the data ingested for the object. However, S Series Nodes can single-instance object data, including the data protection. Single-instancing means storing and protecting only one copy of the data for multiple objects that have the same ingested data.

The S Series Node does not single-instance object metadata. As a result, when the data ingested for multiple objects is single-instanced, the amount of used storage increases only by the size of one copy of the protected object data plus the size of the metadata for each of those objects. As a result, a large amount of single-instancing can increase storage efficiency.

If no objects stored on the S Series Node have duplicate data, storage efficiency is typically around 77%. Storing mostly small objects without duplicate data can decrease storage efficiency due to the amount of metadata stored for each object. Storing mostly large objects with single-instancing can result in a storage efficiency that's greater than 100% because the amount of ingested data is larger than the amount of storage used to store and protect that data.

Ingest rate, object size, object deletion rate, and the amount of storage under repair can all affect the estimates of storage efficiency. The process of repairing storage can temporarily increase storage efficiency.

Before any objects are stored on the S Series Node, the **Dashboard** shows N/A for storage efficiency.

The Storage Efficiency box has a link to the more detailed statistics listed below.

Ingested data

The Ingested data value is the total number of bytes of data written to the S Series Node for all objects currently stored on the S Series Node.

Used storage

The Used storage value is the total amount of storage, in bytes, that is currently occupied by object data, object or system metadata, scavenging metadata, or data and metadata protection overhead.

Under repair

The Under repair value is the amount of storage, in bytes, that is in need of repair. Storage needs to be repaired if it is allocated storage on drives that are no longer available (for example, due to a drive failure), regardless of whether that allocated storage contains data.

Storage efficiency

The Storage efficiency 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 and under-repair storage on the S Series Node.

Object data

The Object data value is the total amount of data, in bytes, stored for all objects currently stored on the S Series Node. Due to single-instancing, the amount of object data stored on the S Series Node can be less than the amount of ingested data.

Storage overhead

The Storage overhead value is a fixed multiplier used in calculating the amount of storage saved by single-instancing.

Single-instance savings

The Single-instance savings value is the total amount of storage, in bytes, saved by the single-instancing of existing objects. Single-instancing means storing only one copy of the data for two or more objects that have the same data.

The S Series Node stores the metadata for each object independently of any other object. No part of object metadata is ever single-instanced.

The amount of storage saved by single instancing is calculated as the amount of ingested data minus the amount of used storage, multiplied by the storage overhead value. The storage overhead multiplier accounts for the savings generated by protecting only the single copy of the data.

Available storage

The Available storage value is the total amount of storage, in bytes, that is currently available for storing and protecting object data and object and system metadata. Available storage does not include storage that is reserved for use in repairing damaged storage.

Unique-data storage efficiency

The Unique-data storage efficiency value is a fixed percent (approximately 76.92%) representing the ratio between the amount of data ingested for any given object and the amount of storage required to store and protect that data, assuming that single-instancing is not in effect.

Ingestible at current efficiency

The Ingestible at current efficiency value is the estimated amount of data, in bytes, that can be ingested into the S Series Node before no more data can be stored or protected, assuming that ingest patterns and the rate of single-instancing remain constant.

Ingestible with unique data

The Ingestible with unique data value is the estimated amount of data, in bytes, that can be ingested into the S Series Node before no more data can be stored or protected, assuming that ingest patterns remain constant and that no duplicate data is ingested.

Time until full

The Time until full value is the estimated amount of time, in days, until the amount of available storage is zero. This value is based on historical ingest trends.

When no storage is available, the S Series Node becomes read-only, and no more data can be ingested.

Storage-usage bar

The storage-usage bar on the **Dashboard** page shows the relative amounts of storage currently in these categories:

- Storage used for object data, object and system metadata, scavenging metadata, and protection overhead (shown in blue).
- Storage under repair (shown in orange). If any storage is under repair, the section for storage under repair overlies the applicable length of the section for available storage. The current amount of available storage is not affected by this overlay. However, because the S Series Node uses available storage to repair damaged storage, while repairs are in progress, the amount of storage available for ingestion of new data decreases.
- Storage available for storing and protecting new objects and object and system metadata (shown in gray).
- Storage reserved for repairing damaged storage (shown in black).

To see the amount of storage in any of the above categories as a percent of total storage, hover over the applicable colored section of the bar. The sum of the percents of used storage, available storage, and storage reserved for repair is 100. However, because the section for storage under repair is an overlay, the sum of the percents for all four categories can be greater than 100.

The relative amounts of storage shown on the storage-usage bar and the corresponding percents can change when drives are added or become unavailable, objects are stored or deleted, or storage is repaired.

Dashboard graphs

The **Dashboard** page has two graphs, one showing amounts of stored and ingested data and the other showing amounts of storage under repair. The graphs show amounts in bytes over the past ten days. If the HCP S Series software was installed less than ten days ago, the graphs show amounts starting from the day the software was installed.

The S Series Node updates graph statistics at regular intervals. As a result, the graphs may not reflect current values.

In each graph, the x-axis marks the passage of time. The y-axis marks the number of bytes in measurement units that increase or decrease (for example, from GB to TB or from TB to GB) as the number of bytes increases or decreases.

The list below describes the graphs on the **Dashboard** page.

Used/Ingested graph

The Used/Ingested graph is a visual representation of the changes in storage efficiency over time, where storage efficiency is shown as the relationship between used storage and ingested data. Used storage is all the storage that is occupied by object data, object or system metadata, scavenging metadata, or data and metadata protection overhead at any given time. Ingested data is the data that was written to the S Series Node for all the objects that exist on the S Series Node at any given time.

In the graph, used storage is represented by blue shading. Ingested data is represented by a black line.

Due to single-instancing, at any given time, the amount of used storage can be less than the amount of ingested data, resulting in greater storage efficiency. If no objects have duplicate data, the amount of used storage is greater than the amount of ingested data, resulting in lower storage efficiency.

Under Repair graph

The Under Repair graph shows the changes in the amount of storage in need of repair over time. This amount of storage is called the *repair backlog*.



Note: While the repair backlog is very small, the size of the backlog looks like zero on the graph.

Resource load

Clients of an HCP S Series Node can use the HCP S Series management API to request information about the current load on certain S Series Node resources. Clients storing data on more than one S Series Node can use the resource-load information to balance data storage operations across the S Series Nodes. Storing new objects, tiering objects, and rebalancing used storage can all be fine-tuned using the resource-load information returned by each S Series Node.

Resource-load statistics collection

When a client requests resource-load information, the S Series Node returns statistics for storage, CPU, and bandwidth usage. If no request has been made for this information in the past minute, the S Series Node uses values from both server modules to calculate the applicable statistics. The S Series Node returns the calculated statistics to the client and also caches the individual server-module values and the calculated statistics in memory. If the S Series Node receives the same request within one minute after the last request, the S Series Node responds with the cached calculated statistics.

The S Series Node sends a timestamp with each response to the client. The timestamp is the earlier of the times when the applicable values were provided by each server module. The older the timestamp is, the less reliable the statistics are.

If a server module has not updated its values for three or more minutes, the values are considered stale. If the values for only one server module are stale, the S Series Node uses the cached values for that server module and the current values for the other server module to calculate the resource-load statistics. In this case, the S Series Node does not update the timestamp, so the timestamp returned with the statistics is the time when the server module with the stale values last updated those values.

If the values for both server modules are stale, the S Series Node returns the cached statistics to the client. In this case, the timestamp returned with the statistics is the earlier of the times each server module last updated the applicable values.

If a server module is unavailable when the S Series Node receives a request for resource-load information, the S Series Node uses default values for that server module and the current values for the other server module to calculate the resource-load statistics. In this case, the S Series Node returns an updated timestamp with the statistics.

After a restart of the S Series Node, until both server modules have finished their startup processing, a request for resource-load information returns an HTTP 503 (Service Unavailable) status code.

Resource-load statistics

You use the management API `/metrics/resourceLoad` resource to request resource-load information from an S Series Node. The S Series Node response to this request includes statistics for:

- The total storage capacity of the S Series Node, in bytes. This value is the total amount of storage that can be used for storing, protecting, and repairing object data and metadata.

The default total-storage-capacity value for an unavailable server module is 0. However, because each server module can see all the S Series Node storage, the reported total storage capacity is always the total storage capacity of the S Series Node, regardless of whether one server module is unavailable.

- The amount of free storage on the S Series Node, in bytes. This value is the total amount of storage that is currently available to be allocated for storing and protecting object data and metadata. This value does not include storage that is reserved for repairing object data and metadata.

The default free-storage value for an unavailable server module is 0. However, because each server module can see all the free storage on the S Series Node, the reported amount of free storage is always the total amount of free storage, regardless of whether one server module is unavailable.

- The average of the larger of these two statistics on each server module:
 - The average CPU utilization, as a percent
 - The average thread pool utilization, as a percent

In either case, the default value for an unavailable server module is 100%.

The reported overall average represents the percent of S Series Node processing capacity that's either in use or unavailable across both server modules. The remaining percent represents the available processing capacity.

For example, if one server module is using 75% of its processing capacity and the other server module is using 63% of its processing capacity, the reported value is 69% (the average of 75% and 63%), and the available processing capacity on the S Series Node is 31%.

If one server module is using 75% of its processing capacity and the other server module is unavailable, the reported value is 87.5% (the average of 75% and 100%), and the available processing capacity on the S Series Node is 12.5%.

- The total amount of network bandwidth provided by the access network ports on the two server modules, in bits per second (bps). Only ports that have a functioning connection to an active switch are included in the total-bandwidth calculation.

With IEEE 802.3ad bonding, the total-bandwidth value for a server module is the total of the bandwidth on all functioning access-network connections. With active-backup bonding, the total-bandwidth value for a server module is the bandwidth on only the connection to the active port in the bond.

The default total-bandwidth value for an unavailable server module is 0.

- The total amount of free network bandwidth available on the access network ports on the two server modules, in bits per second (bps). Only ports that have a functioning connection to an active switch are included in the free-bandwidth calculation.

With IEEE 802.3ad bonding, the free-bandwidth value for a server module is the total of the free bandwidth on all functioning access-network connections. With active-backup bonding, the free-bandwidth value for a server module is the free bandwidth on only the connection to the active port in the bond.

The default free-bandwidth value for an unavailable server module is 0.

System load

You can use the HCP S Series management API to request information about the current load on HCP S Series Node processing resources or about this load over time. The load on processing resources, called the *system load*, relates to the use of resources such as CPUs, network bandwidth, and memory. For each processing resource, usage statistics are available for the individual server modules and for the S Series Node as a whole. You can use system-load information to evaluate the use of these resources and to draw conclusions about the performance of the S Series Node.

System-load statistics collection

When you request system-load information, the S Series Node returns statistics for a variety of processing resources for each server module and for the S Series Node as a whole. On receiving a request for system-load information, the S Series Node uses values stored by both server modules to calculate the statistics to return for the individual server modules and for the S Series Node. The S Series Node returns the calculated statistics in the management API response and also caches the individual server-module values and the calculated statistics in memory.

Each server module updates its system-load values once a minute. As a result, multiple requests made for system-load information within the same one-minute interval return the same statistics.

The S Series Node includes a timestamp in the response to a request for system-load statistics. The timestamp is the earlier of the times when the applicable values were provided by each server module. The older the timestamp is, the less reliable the statistics are.

If a server module has not updated its values for three or more minutes, the values are considered stale. If the values for only one server module are stale, the S Series Node uses the cached values for that server module and the current values for the other server module to calculate the system-load statistics. In this case, the S Series Node does not update the timestamp, so the timestamp returned with the statistics is the time when the server module with the stale values last updated those values. With stale values from one server module, the calculated system-load statistics are not fully reliable.

If the values for both server modules are stale, the S Series Node returns the cached statistics to the client. In this case, the timestamp returned with the statistics is the earlier of the times each server module last updated the applicable values. With stale values from both server modules, the calculated system-load statistics may not accurately reflect the current load on the S Series Node processing resources.

If a server module is unavailable when the S Series Node receives a request for system-load information, the S Series Node uses zero as the default value for each statistic for that server module and uses the current values for the other server module to calculate the system-load statistics. In this case, the S Series Node returns an updated timestamp with the statistics.

After a restart of the S Series Node, until both server modules have finished their startup processing, a request for system-load information returns an HTTP 503 (Service Unavailable) status code.

System-load statistics

You use the management API `/metrics/systemLoad` resource to request system-load information from an S Series Node. The S Series Node response to this request includes statistics for the processing resources listed below. Each returned statistic is either for a point in time or for a duration of approximately one minute.

CPUs

The statistics for CPU usage are:

- Percent of CPU processing power in use on each server module and on the S Series Node as a whole. The S Series Node value is the average of the two server module values.
- Percent of CPU processing time spent waiting for I/O operations to finish or waiting to acquire processing resources on each server module since the server module last started and on the S Series Node as a whole. The S Series Node value is the average of the two server module values.

Network bandwidth

The statistics for network-bandwidth usage are:

- For each server module:
 - Rate of data transmission on each access network port on each server module during the past minute, in bits per second
 - Rate of data reception on each access network port on each server module during the past minute, in bits per second
 - Larger of the total rate of data transmission and total rate of data reception on each server module during the past minute, in bits per second
 - Total of the bandwidth capacity that can be used for data transmission on each access network port on each server module, in bits per second
 - Total of the bandwidth capacity that can be used for data reception on each access network port on each server module, in bits per second
 - Larger of the total bandwidth capacity that can be used for data transmission and the total bandwidth capacity that can be used for data reception on each server module, in bits per second
 - Percent of the total bandwidth capacity in use for data transmission or data reception on each server module
- For the S Series Node as a whole:
 - Sum of the larger of the total rate of data transmission and total rate of data reception on each server module during the past minute, in bits per second.
 - Sum of the larger of the total amount of bandwidth that can be used for data transmission and the total amount of bandwidth that can be used for data reception on each server module, in bits per second.
 - Percent of the total amount of bandwidth in use for data transmission or data reception on both server modules. The S Series Node value is calculated independently of the values for the two server modules.

I/O threads

The statistics for I/O-thread usage are:

- Number of I/O threads in use on each server module and on the S Series Node as a whole. The S Series Node value is the sum of the two server module values.
- Total number of I/O threads on each server module and on the S Series Node as a whole. The S Series Node value is the sum of the two server module values.
- Percent of I/O threads in use on each server module and on the S Series Node as a whole. The S Series Node value is calculated independently of the values for the two server modules.

Memory

The statistics for memory usage are:

- Amount of memory in use on each server module and on the S Series Node as a whole, in bytes. The S Series Node value is the sum of the two server module values.
- Total amount of memory on each server module and on the S Series Node as a whole, in bytes. The S Series Node value is the sum of the two server module values.
- Percent of memory in use on each server module and on the S Series Node as a whole. The S Series Node value is calculated independently of the values for the two server modules.

Hitachi API for Amazon S3 (S3 compatible API)

The statistics for usage of the S3 compatible API are, for each of the PUT, GET, DELETE, HEAD, and POST operations:

- Rate of throughput for operations of the given type on each server module and on the S Series Node as a whole during the past minute, in operations per second. The S Series Node value is the sum of the two server module values.
All operations of the applicable type are included in the rate calculation, regardless of whether the operations succeeded or ended with errors.
- Rate of data throughput for operations of the given type on each server module and on the S Series Node as a whole during the past minute, in bytes per second. The S Series Node value is the sum of the two server module values.
All operations of the applicable type are included in the rate calculation, regardless of whether the operations succeeded or ended with errors.
- Percent of operations of the given type that succeeded on each server module and on the S Series Node as a whole. The S Series Node value is calculated independently of the values for the two server modules.
- Percent of operations of the given type that terminated with errors on each server module and on the S Series Node as a whole. The S Series Node value is calculated independently of the values for the two server modules.
- Average latency of the operations of the given type on each server module and on the S Series Node as a whole during the past minute, in milliseconds. The S Series Node value is the sum of the two server module values.

Historical system-load statistics

Every five minutes, the S Series Node issues an internal request for system-load statistics and saves the returned statistics, along with a timestamp, in the internal database. Once an hour, these minute statistics are rolled up into hourly statistics, and, a week later, the minute statistics are deleted. Once a day, the hourly statistics are rolled up into daily statistics, and, three weeks later, the hourly statistics are deleted. Once a month, the daily statistics are rolled up into monthly statistics, and, three months later, the daily statistics are deleted. Monthly statistics are kept for two years.

Each rollup consists of the average, minimum, and maximum for each type of statistic for each of server module 1, server module 2, and the S Series Node as a whole during the applicable period. For example, suppose the five-minute values for CPU load on the S Series Node in a given hour are 25%, 50%, 30%, 90%, 25%, and 50%. Based on these values, the rollup for the S Series Node for the hour would have a minimum value of 25%, a maximum value of 90%, and an average value of 45%.

You use the management API `/metrics/systemLoad/history` resource to request historical system-load information from an S Series Node. In the request, you specify the start and end times for the period of statistics you want. You can also specify the granularity (minute, hour, day, or month) of the statistics you want. If you don't specify the granularity, the S Series Node returns hourly statistics.

The response to a request for the `/metrics/systemLoad/history` resource can be quite long. You can use query parameters to limit the response in these ways:

- Omitting the S3 compatible API statistics
- Omitting the minimum and maximum values for rolled-up statistics
- Omitting the server-module-specific statistics
- Including only statistics you specifically request (for example, if you request only CPU and memory statistics, no statistics are returned for network bandwidth, I/O threads, or the S3 compatible API)
- Paging through the response by repeatedly issuing the request, each time specifying a limited number of results to include in the response

Omitting the S3 compatible API statistics and including only statistics you specify are mutually exclusive options.

Event log

An HCP S Series Node maintains a log that contains messages about events that occur on the S Series Node. The event times associated with log messages are in UTC.

If you have the administrator, monitor, security, or service role, you can view the event log in the HCP S Series Management Console. You can also use the HCP S Series management API to retrieve the contents of the log. The event messages you can see depend on the roles associated with your user account.

If you have the administrator or service role, you can configure the S Series Node to send event log messages to one or more syslog servers.

Event log views

The Management Console provides several views of the event log:

- On the **EVENTS** page, you can choose to see all messages or only messages about events related to a particular aspect of the S Series Node (for example, security events (see below) or events related to data or database drives).
- On the **Dashboard** page, the event log includes only messages about major events (for example, user account creations but not user logins to the Console).
- On the **HARDWARE OVERVIEW** page, the event log includes only messages about events related to the S Series Node hardware components. On each page for an individual hardware component, the event log includes only messages about events related to that component.
- On the **MAINTENANCE** page, the event log includes only messages about events related to maintenance procedures.
- On the **UPDATE** page, the event log includes only messages about events related to software update procedures.
- On the **SSL SERVER CERTIFICATES** page, the event log includes only messages about events related to SSL server certificates.

To see more information about an event in the Management Console, including what action to take, if any, in response to the event, click the down arrow to the left of the event message.


When you use the management API to retrieve event log messages, you can use query parameters to specify which messages you want to see.

Security events

Security event messages report actions that require the security role (such as the creation of a user account). These messages also report attempts to log in to the HCP S Series Management Console with invalid credentials or to use the HCP S Series management API with invalid credentials. Only users with the security role can see messages about security events.

Alerts

Alerts contain information about the current state of the HCP S Series Node. Typically, an alert requires you to take an action.

If any alerts are currently in effect, the HCP S Series Management Console displays a red circle showing the number of those alerts next to a bell icon () in the top right corner of each Console page. To see the alerts, click on the bell icon. To see the full text of a truncated alert, hover over the visible alert text.

You can also use the S Series Node management API to retrieve the alerts that are currently in effect.

The S Series Node does not automatically update the number that shows how many alerts are currently in effect. To update this number, either reload the current page or navigate to a different page. Regardless of the number shown, clicking the bell icon opens a list of all the alerts that are currently in effect.

Alerts are triggered by events. However, although messages about events are always logged at the time the event occurs, some alerts may not be issued until up to five minutes after the triggering event occurs. Similarly, some alerts may persist up to five minutes past the resolution of the triggering event.



Tip: The text for alerts is the same as the detailed form of messages in the event log. For more information about an alert, find the corresponding event-log message. Then look at the message details.

Syslog logging

You can have the HCP S Series Node send log messages to one or more syslog servers as the messages are logged. You can then use tools in your syslog environment to perform functions such as sorting, querying, and forwarding the messages.

The types of log messages you can send to syslog servers are:

- Event log messages
- Log messages for data access requests
- Log messages for management API requests

You can test the connections to the syslog servers you specify to ensure that those servers can receive the log messages that the S Series Node sends.

If you have the administrator or service role, you can use the HCP S Series Management Console or management API to configure and test syslog logging.

To work with the syslog logging configuration in the Management Console, go to Configuration > Syslog.

Configuring syslog logging

You can specify up to ten syslog servers. You identify each one by its IP address (optionally, with an appended port number). If you specify multiple servers, the S Series Node sends each message to all of them.

Specifying which messages to send

You select the types of log messages to send to the specified syslog servers. You can select any number of message types. However, if you don't select any message types, no log messages are sent, even if you have specified one or more syslog servers.

For each message type you select, you can specify the syslog local facility to which that type of log message will be directed. The default for all types is local0.

You can control which event log messages are sent to the syslog servers in these ways:

- By setting the minimum severity level to one of the levels listed below.
 - NOTICE. Send messages with a severity level of notice, warning, or error.
 - WARNING. Send messages with a severity level of warning or error.
 - ERROR. Send only messages with a severity level of error.
- By specifying that only messages about major events should be sent. Major events are those that are displayed on the **Dashboard** page of the HCP S Series Management Console.
- By including security event messages in the messages to be sent. Security event messages report actions that require the security role (such as the creation of a user account) and events that are exposed only to users with the security role (such as a login attempt with an incorrect password).

Selecting a network

You can choose the network (access or management) to be used for communication between the S Series Node and the syslog servers you specify. The default is the access network.

The S Series Node uses the selected network in the IP mode in which the network is configured. If the access network is configured for IPv6 and a secondary IPv6 gateway is configured for the network, you can choose to use either the primary or secondary IPv6 gateway.

For the S Series Node to communicate with the specified syslog servers, the IP mode of your network selection must match the IP mode of the syslog server IP addresses.



Note: If all these conditions are true, the S Series Node sends messages to the syslog servers over both the access and management networks:

- The access and management networks have different IP modes.
- The syslog configuration specifies two or more syslog servers.
- At least one specified syslog server has an IPv4 address, and at least one specified syslog server has an IPv6 address.

Testing syslog server connections

After specifying one or more syslog servers and selecting the network you want, you can click Test on the **SYSLOG** page to test the connections to those servers. Testing the connections causes the S Series Node to send this test message, with the applicable IP addresses, to each specified server:

```
A test message has been sent to the syslog servers at the following IP addresses:
[159.73.15.49,159.73.42.17]
```

If the S Series Node successfully sends the test message, this message appears in the event log:

```
Syslog test message sent
```

If the syslog server receives the test message, the connection works.

You can specify the syslog local facility to which the test message should be directed. The message goes to this facility on each specified syslog server. The default facility is local0.



Note: When you use the management API to test syslog server connections, you specify the local facility as part of the name of the requested resource. If the local facility specified in the management API request differs from the local facility in the syslog configuration, the S Series Node changes the local facility in the syslog configuration to the local facility specified in the management API request.

Management Console hardware information

The **HARDWARE OVERVIEW** page of the HCP S Series Management Console displays high-level information about the status of the S11 or S31 Node enclosures and server modules. From this page, you can display more detailed information about the S11 or S31 Node hardware components.

On the **HARDWARE OVERVIEW** page, the information about each enclosure or server module is displayed in a separate box. If an alert that applies to the enclosure or server module is in effect, a blue (ⓘ), orange (⚠), or red (🚫) icon is displayed in the upper right corner of the box, and the box has a line of the same color across the top. Blue indicates that the alert is informational only, orange indicates that the alert is a warning, and red indicates an error condition. If more than one alert for the enclosure or server module is in effect, only the icon for the most severe alert is displayed.

To see the text of an alert, hover over the alert icon.

Enclosure details

To see detailed information about an enclosure and its components, go to Hardware > Overview. Then, to open the ENCLOSURE page, click the enclosure you want.

In addition to information such as the enclosure status, vendor, and hardware model, the ENCLOSURE page has diagrams that show top, back, and front views of an enclosure and, for an expansion enclosure, the front view of both I/O modules in the enclosure. Colors and patterns indicate component status.

For an explanation of the colors and patterns used in a diagram, click Legend below the diagram.

The ENCLOSURE page also shows log messages for events related to the applicable enclosure.

To see details and event log messages for the data or database drive in a slot or for an empty slot in an enclosure, click the slot in the top view of the enclosure. To see details for a SAS port on an enclosure, click the port in the back view of the enclosure.

To see detailed information about the enclosure itself and various enclosure components, in the ENCLOSURE DETAILS section on the ENCLOSURE page, click the applicable component type. The component types are listed below.

Enclosure

Shows information about the enclosure itself.

Door

Shows the status of the enclosure main-bay cover and of the enclosure controller-bay cover. If a cover is correctly closed, the status for that cover is normal.

Power Supplies

Shows information about the power inlets on the enclosure power supplies. Each inlet is identified by a power supply number and an inlet letter.

When viewed from the rear of the enclosure, power supply 0 is on the left and power supply 1 is on the right. On each power supply in a base enclosure, power inlet A is on the left, and power inlet B is on the right. On each power supply in an expansion enclosure, the only power inlet is A.

Voltage Sensors

Shows information about the voltage sensors in the enclosure power supplies. Each power supply has two voltage sensors for each power inlet. The power inlet identifiers are listed below. In the Management Console, the number (0 or 1) following each power inlet identifier is the identifier for one of the voltage sensors for the applicable power inlet.

PCM0

Left power supply, left power inlet (base enclosure) or only power inlet (expansion enclosure).

PCM1

Left power supply, right power inlet (base enclosure). For an expansion enclosure, each voltage sensor listed for PCM1 has a status of Not installed.

PCM2

Right power supply, left power inlet (base enclosure) or only power inlet (expansion enclosure).

PCM3

Right power supply, right power inlet (base enclosure). For an expansion enclosure, each voltage sensor listed for PCM3 has a status of Not installed.

Current Sensors

Shows information about the current sensors in the enclosure power supplies. Each power supply has two current sensors for each power inlet. The current-sensor identifiers have the same format as the voltage-sensor identifiers.

Service Modules

For a base enclosure, shows information about the server modules. For an expansion enclosure, shows information about the I/O modules.

When viewed from the rear of the enclosure, server module 1 or I/O module 1 (IOM 1) is on the right, and server module 2 or I/O module 2 (IOM 2) is on the left.

Fans

Shows information about the fans in the enclosure. The fans in the back of the enclosure are numbered 0 through 3, going from left to right, when viewed from the rear of the enclosure. The fans in the controller bay are numbered 4 and 5, going from the rear of the enclosure to the front.

Each rear fan in an enclosure has two sets of blades, identified as A and B. In a base enclosure, each controller-bay fan also has two sets of blades, identified as A and B. In an expansion enclosure, each controller-bay fan has one set of blades.

SAS Expanders

Shows information about:

- The eight SAS expanders (also called sideplane expanders) that are in the right side of the enclosure, when viewed from the front of the enclosure. These SAS expanders are numbered from 0 through 7, going from the front of the enclosure to the rear. The SAS expanders labeled A are associated with server module 1 (base enclosure) or I/O module 1 (expansion enclosure). The SAS expanders labeled B are associated with server module 2 (base enclosure) or I/O module 2 (expansion enclosure).
- For a base enclosure only, the two SAS expanders, A and B, in each of the two personality modules. When viewed from the front of the enclosure, personality module 0 is on the left, and personality module 1 is on the right.
- For an expansion enclosure only, the two SAS expanders in each of the two I/O modules. Each I/O module has both a primary and a secondary SAS expander. On I/O module 1, both of these SAS expanders are identified as A. On I/O module 2, both of these SAS expanders are identified as B.

SAS Connectors

Shows information about:

- For a base enclosure, the SAS ports on the back of the enclosure. Each port is identified by:
 - The server module (1 or 2) that controls the port.
 - The SAS expander (A or B) through which the server module communicates with the port. These SAS expanders are in the personality module associated with the applicable server module.
 - The port number. The port numbers, from left to right, are 2, 3, 0, and 1.
- For an expansion enclosure, the SAS ports on the I/O modules. Each port is identified by:
 - The I/O module (1 or 2) where the port is located.
 - The port number on the I/O module. The port numbers, from top to bottom, are 0, 1, 2, and 3.

Temperature Sensors

Shows information about the temperature sensors in the enclosure. The temperature sensors are in these components:

- The two midplanes located between the main bay and the rear fans. Each midplane has one temperature sensor.

The temperature sensor for the midplane associated with server module 1 (base enclosure) or I/O module 1 (expansion enclosure) is identified as MP0:0. The temperature sensor for the midplane associated with server module 2 (base enclosure) or I/O module 2 (expansion enclosure) is identified as MP0:1.

- The eight SAS expanders that are in the right side of the enclosure, when viewed from the front of the enclosure. Each SAS expander has one temperature sensor.

The temperature sensors for the SAS expanders associated with server module 1 (base enclosure) or I/O module 1 (expansion enclosure) are identified as SP0:0, SP1:0, SP2:0, and SP3:0. The temperature sensors for the SAS expanders associated with server module 2 (base enclosure) or I/O module 2 (expansion enclosure) are identified as SP0:1, SP1:1, SP2:1, and SP3:1.

- The eight backplanes in the main bay and the backplane in the controller bay. Each backplane in the main bay has one temperature sensor. The backplane in the controller bay of a base enclosure has two temperature sensors. The backplane in the controller bay of an expansion enclosure has one temperature sensor.

The temperature sensors for the main-bay backplanes associated with server module 1 (base enclosure) or I/O module 1 (expansion enclosure) are identified as BP0:0, BP1:0, BP2:0, and BP3:0. The temperature sensors for the main-bay backplanes associated with server module 2 (base enclosure) or I/O module 2 (expansion enclosure) are identified as BP0:1, BP1:1, BP2:1, and BP3:1.

The temperature sensors for the controller-bay backplane in a base enclosure are identified as BP5:0 and BP5:1. The temperature sensor for the controller-bay backplane in an expansion enclosure is identified as BP4:0.

- For a base enclosure only, the two personality modules. Each personality module has two temperature sensors.

The temperature sensors for the personality module on the left, when viewed from the front of the enclosure, are identified as PM0:0 and PM0:1. The temperature sensors for the personality module on the right, when viewed from the front of the enclosure, are identified as PM1:0 and PM1:1.

- The power inlets on the enclosure power supplies. Each power inlet has three temperature sensors.

Each temperature sensor for the power inlets is identified by the applicable power inlet identifier (for example, PCMO), as described for voltage sensors above, followed by the identifier (0, 1, or 2) for that temperature sensor.

- The two midplane interconnects, which connect the midplanes to the server modules (base enclosure) or I/O modules (expansion enclosure). In a base enclosure, each midplane interconnect has nine temperature sensors. In an expansion enclosure, each midplane interconnect has three temperature sensors.

The midplane interconnect for server module 1 or I/O module 1 is identified as SBB0. The midplane interconnect for server module 2 or I/O module 2 is identified as SBB1.

The number following each midplane interconnect identifier is the identifier for one of the temperature sensors for the applicable midplane interconnect. For a base enclosure, the temperature sensor identifiers for each midplane interconnect are numbers in the range 0 through 8. For an expansion enclosure, the temperature sensor identifiers for each midplane interconnect are 0, 1, and 2.

Server module details

To see detailed information about a server module, go to Hardware > Overview. Then, to open the SERVER MODULE page, click the server module you want.

In addition to information such as the server module status, hardware model, and boot time, the SERVER MODULE page has a diagram that shows the front view of an individual server module. Colors indicate the status of the ports on the server module.

For an explanation of the colors used in the diagram, click Legend below the diagram.

The SERVER MODULE page also shows log messages for events related to the applicable server module.

To see details and event log messages for an Ethernet port on a server module, click the port in the server module diagram. To see details for a SAS port on a server module (S31 Nodes only), click the port in the server module diagram.

To see detailed information about various server module components, in the SERVER MODULE DETAILS section on the SERVER MODULE page, click the applicable component type. The component types are listed below.

Core Hardware

Shows information about the server module, such as load average, memory usage, CPU hardware, and the time server currently being used by the S Series Node.

File Systems

Shows the information about each file system mounted on the server module.

Network Interfaces

Shows information about the access, management, and server interconnect networks.

SAS Connectors

Shows information about the SAS ports on the server module. Each port is identified by:

- The server module number (1 or 2).
- The port number on the server module. The port numbers, from top to bottom, are 0, 1, 2, and 3.

The SAS Connectors component type is present only for S31 Nodes.

IPMI

Shows temperature sensor and processor sensor values for the server module and other sensor values, if they are available.

Internal Drives

Shows information about the OS SSDs in the server module.

SSD 0 is the SSD closer to the rear of the server module. SSD 1 is the SSD closer to the front of the server module.

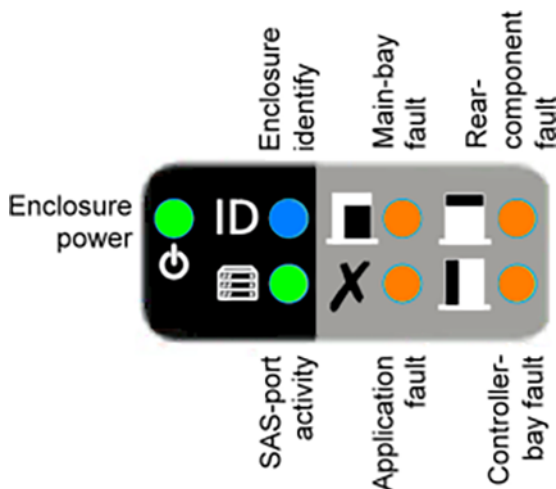
Physical component status indicators

The LEDs on various hardware components of an S11 or S31 Node provide information about the status of the applicable component. Some of these LEDs can also be used for beaoning.

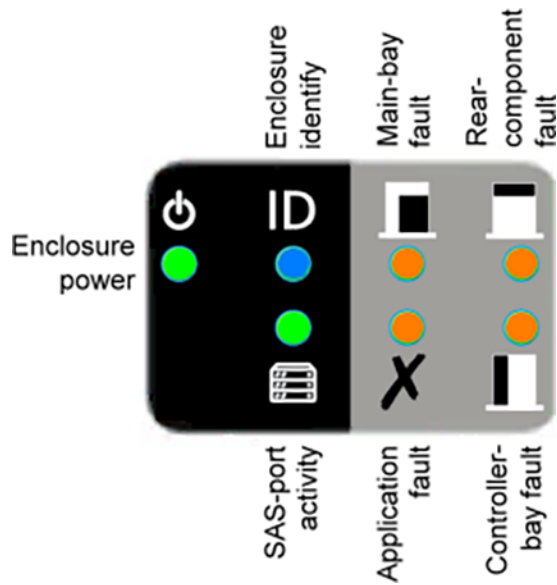
Enclosure front LEDs

Base and expansion enclosures have seven color-coded LEDs that indicate the status of the enclosure. These LEDs are located in the bottom left corner on the front of the enclosure. Each LED is identified by an icon.

The figure below shows the front LEDs and icons on a base enclosure.



The figure below shows the front LEDs and icons on an expansion enclosure.



The table below describes the enclosure front LEDs.

LED	Color	State	Description
Enclosure power	Green	Solid	The enclosure is powered on.
		Blinking	N/A
		Off	The enclosure is powered off.
Enclosure identify	Blue	Solid	N/A
		Blinking	Beaconing is on for the enclosure.
		Off	Beaconing is off for the enclosure.
Main-bay fault	Amber	Solid	One or more data drives, database drives (base enclosure only), or SAS expanders in the enclosure main bay have a critical fault condition, or the main-bay cover is off.
		Blinking	A component in the main bay has a noncritical fault condition.
		Off	All data drives, database drives (base enclosure only), and SAS expanders in the enclosure main bay are operating normally.
Rear-component fault	Amber	Solid	One or more power supplies, rear fans, or rear SAS ports (base enclosure only) in the enclosure have a critical fault condition, or a power supply is missing.
		Blinking	A rear component has a noncritical fault condition, or a rear fan is missing.

LED	Color	State	Description
		Off	All power supplies and rear fans in the enclosure are operating normally.
SAS-port activity	Green	Solid	For a base enclosure, at least one rear SAS port on the enclosure has a healthy connection to a SAS port on an I/O module. For an expansion enclosure, at least one SAS port on the I/O modules in the enclosure has a healthy connection to a rear SAS port on the base enclosure or to a SAS port on another I/O module.
		Blinking	N/A
		Off	For a base enclosure, no rear SAS port on the enclosure has a healthy connection to a SAS port on an I/O module. For an expansion enclosure, no SAS port on the I/O modules in the enclosure has a healthy connection to a rear SAS port on the base enclosure or to a SAS port on another I/O module.
Application fault	Amber	N/A	Unused.
Controller-bay fault	Amber	Solid	One or more of these components in the enclosure controller bay have a critical fault condition, or the controller-bay cover is off: <ul style="list-style-type: none"> ▪ Fans ▪ Personality modules (base enclosure only) ▪ Server modules (base enclosure only) ▪ I/O modules (expansion enclosure only) ▪ Data drives (expansion enclosure only) ▪ Database drives (base enclosure only)
		Blinking	A component in the controller bay has a noncritical fault condition.
		Off	All these components in the enclosure controller bay are operating normally: <ul style="list-style-type: none"> ▪ Fans ▪ Personality modules (base enclosure only) ▪ Server modules (base enclosure only) ▪ I/O modules (expansion enclosure only)

LED	Color	State	Description
			<ul style="list-style-type: none"> Data drives (expansion enclosure only) Database drives (base enclosure only)

Rear SAS port LEDs (base enclosure only)

For each SAS port at the rear of a base enclosure, the enclosure has two color-coded LEDs that indicate the status of the port. These LEDs are located below the ports, as shown in the figure below.

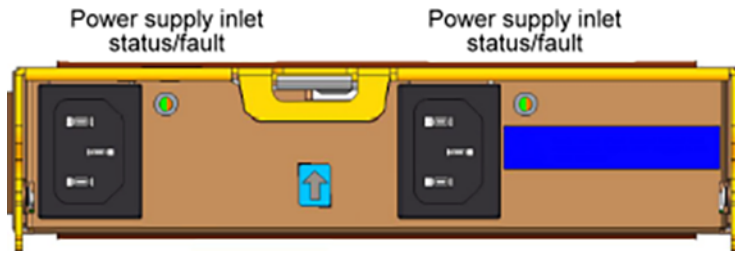


The table below describes these LEDs.

LED	Color	State	Description
SAS port x fault	Amber	Solid	The SAS port has a fault condition.
		Blinking	Beaconing is on for the SAS port.
		Off	The SAS port is operating normally, and beaconing is off for the port.
SAS port x activity	Green	Solid	The SAS port has an active connection.
		Blinking	Activity is occurring on the SAS port.
		Off	The SAS port does not have an active connection.

Power supply LEDs (base enclosure)

For each of the two inlets on each power supply for a base enclosure, the power supply has a single LED that indicates the status of the inlet. Each LED can be green or amber, depending on the inlet status. Each LED is located to the right of the inlet it applies to, as shown in the figure below.

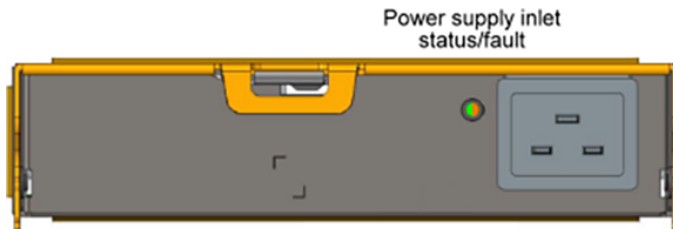


The table below describes these LEDs.

LED	Color	State	Description
Power supply inlet status/fault	Green or amber	Solid green	The power supply inlet is operating normally.
		Blinking green	A power supply firmware upgrade is in progress.
		Solid amber	Either the power supply inlet has a fault condition, or the AC input for the inlet is at the low end of the normal operating range.
		Blinking amber	Beaconing is on for the power supply inlet.
		Off	The power supply inlet is not connected to a power source.

Power supply LED (expansion enclosure)

Each power supply for an expansion enclosure has a single LED that indicates the status of the inlet on that power supply. The LED can be green or amber, depending on the inlet status. The LED is located to the left of the inlet, as shown in the figure below.



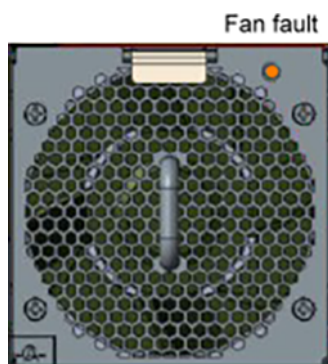
The table below describes this LED.

LED	Color	State	Description
Power supply inlet status/fault	Green or amber	Solid green	The power supply inlet is operating normally.

LED	Color	State	Description
		Blinking green	A power supply firmware upgrade is in progress.
		Solid amber	Either the power supply inlet has a fault condition, or the AC input for the inlet is at the low end of the normal operating range.
		Blinking amber	Beaconing is on for the power supply inlet.
		Off	The power supply inlet is not connected to a power source.

Rear fan LED

Each rear fan on a base or expansion enclosure has a single LED that indicates the status of that fan. The LED is located in the upper right corner of the fan, as shown in the figure below.

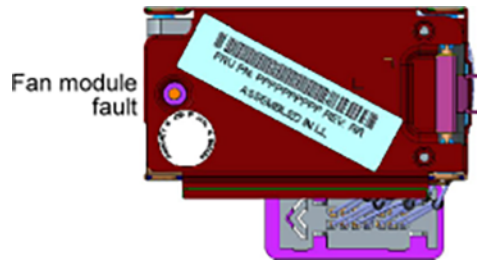


The table below describes this LED.

LED	Color	State	Description
Fan fault	Amber	Solid	The fan has a fault condition.
		Blinking	Beaconing is on for the fan.
		Off	The fan is operating normally, and beaconing is off for the fan.

Controller-bay fan LED (base enclosure)

Each fan in the controller bay of a base enclosure has a single LED that indicates the status of that fan. The LED is located on the left on the top of the fan, as viewed from the front of the enclosure and as shown in the figure below.



The table below describes this LED.

LED	Color	State	Description
Fan module fault	Amber	Solid	The fan has a fault condition.
		Blinking	Beaconing is on for the fan.
		Off	The fan is operating normally, and beaconing is off for the fan.

Controller-bay fan LED (expansion enclosure)

Each fan in the controller bay of an expansion enclosure has a single LED that indicates the status of that fan. The LED is located on the left on the top of the module, as viewed from the front of the enclosure and as shown in the figure below.

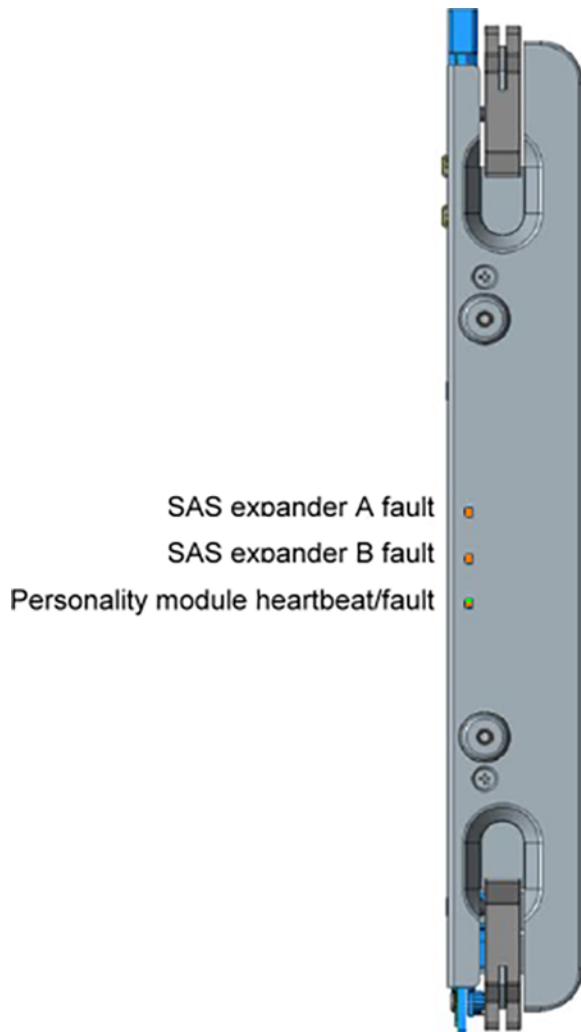


The table below describes this LED.

LED	Color	State	Description
Fan fault	Amber	Solid	The fan has a fault condition.
		Blinking	Beaconing is on for the fan.
		Off	The fan is operating normally, and beaconing is off for the fan.

Personality module LEDs

Each personality module in a base enclosure has three LEDs that indicate the status of the module. These LEDs are located on the left on the top of the module, as shown in the figure below.



The table below describes these LEDs.

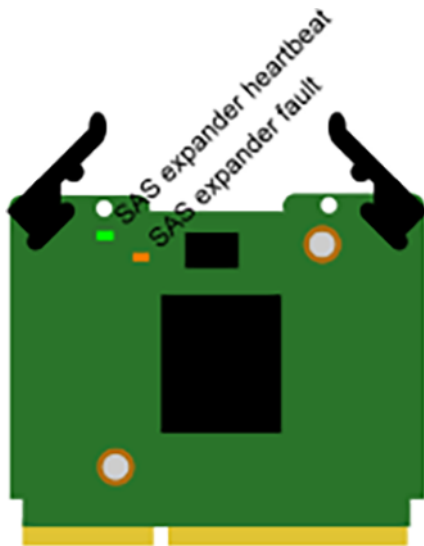
LED	Color	State	Description
SAS expander A fault	Amber	Solid	SAS expander A in the personality module has a fault condition.
		Blinking	N/A
		Off	SAS expander A in the personality module is operating normally.
SAS expander B fault	Amber	Solid	SAS expander B in the personality module has a fault condition.
		Blinking	N/A
		Off	SAS expander B in the personality module is operating normally.

LED	Color	State	Description
Personality module heartbeat/fault	Green or amber	Solid green	N/A
		Blinking green	The personality module is operating normally.
		Solid amber	The personality module has a fault condition.
		Blinking amber	Beaconing is on for the personality module.
		Off	The personality module has no power.

SAS expander LEDs

Each SAS expander in a base or expansion enclosure has two color-coded LEDs that indicate the status of the expander. The LEDs are located on the outer side of the expander and reflect on the inner side of the enclosure side wall. The reflection is visible when you look down on the expander from above.

The figure below shows the locations of the LEDs on a SAS expander.



The table below describes these LEDs.

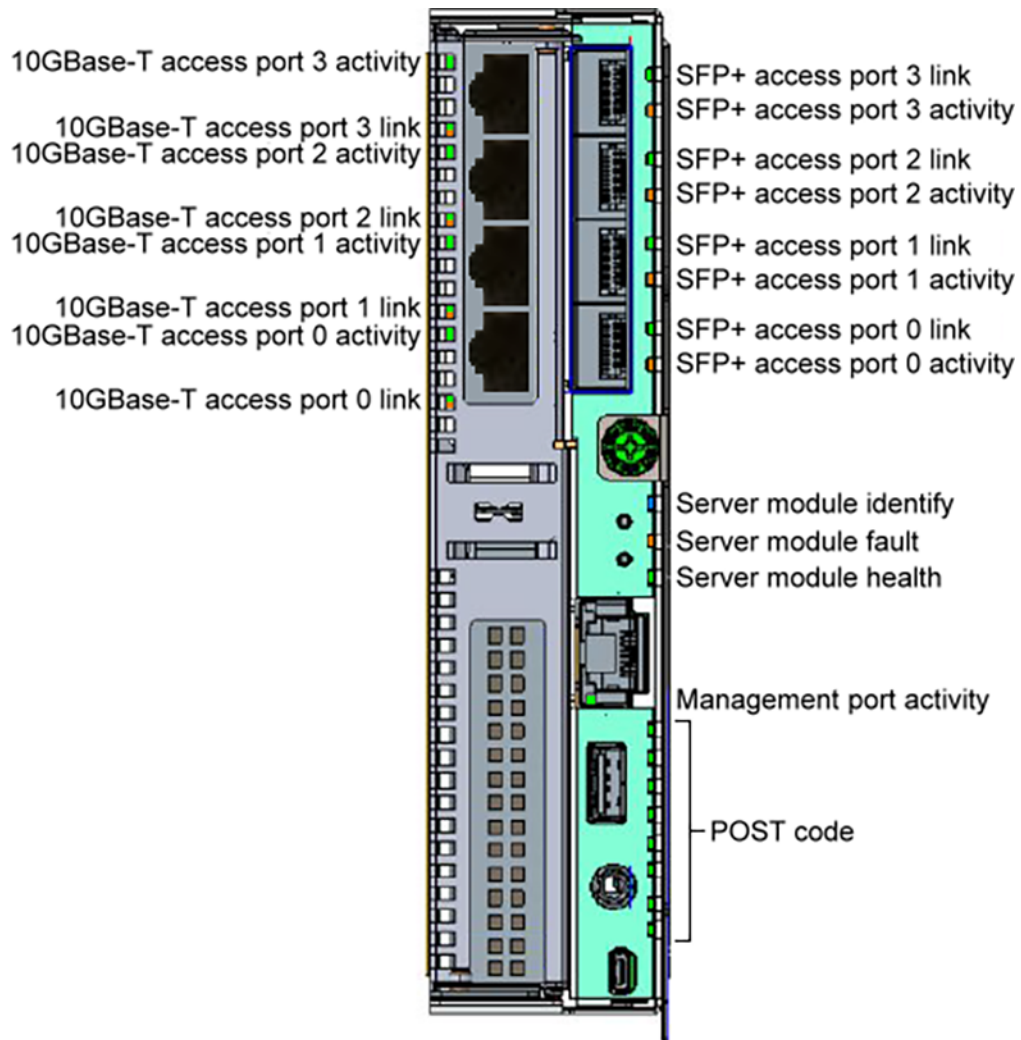
LED	Color	State	Description
SAS expander heartbeat	Green	Solid	N/A
		Blinking	The SAS expander heartbeat is occurring normally.

LED	Color	State	Description
		Off	The SAS expander is not operational.
SAS expander fault	Amber	Solid	The SAS expander has a fault condition.
		Blinking	Beaconing is on for the SAS expander.
		Off	The SAS expander is operating normally, and beaconing is off for the expander.

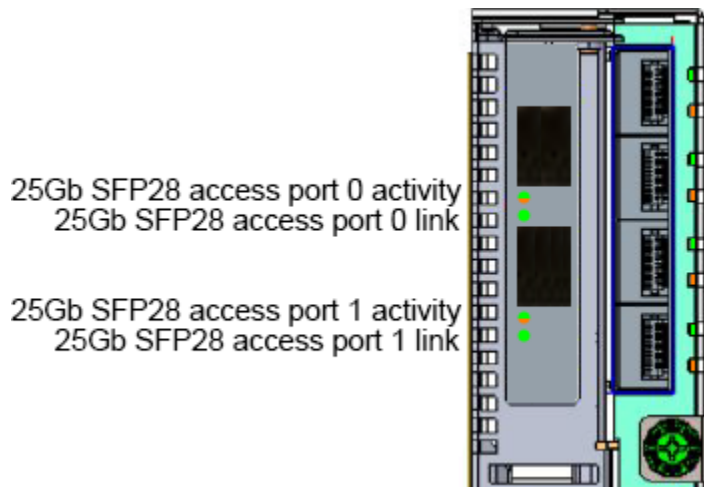
Server module LEDs

Each server module in a base enclosure has multiple color-coded LEDs that indicate the status of the module and the status of the onboard Ethernet ports. These LEDs are located on the right side of the front of the module. If either of the optional Ethernet cards is installed in the server module, the LEDs for the ports on that card are located on the left side of the module.

The figure below shows the onboard LEDs on a server module and the LEDs on the optional four-port 10GBase-T Ethernet card that can be installed in a server module.



The figure below shows the LEDs on the optional two-port 25Gb Ethernet SFP28 card that can be installed in a server module.

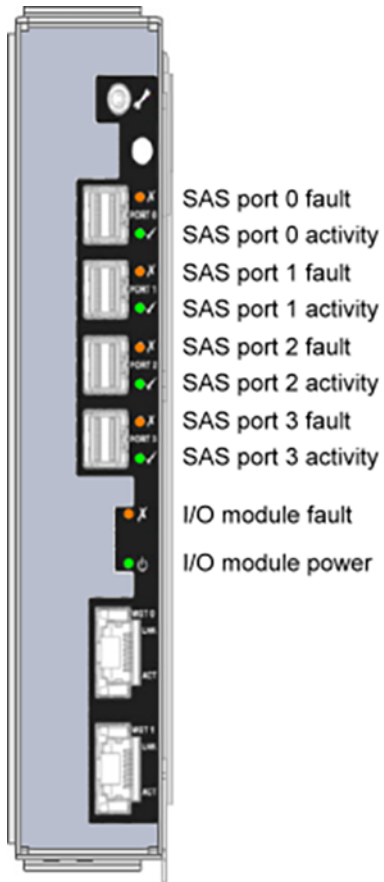


LED	Color	State	Description
SFP+ access port x link	Green	Solid	The port has a link.
		Blinking	N/A
		Off	The port does not have a link.
SFP+ access port x activity	Amber	Solid	The port has a link, but no activity is occurring on the port.
		Blinking	The port has a link, and activity is occurring on the port.
		Off	The port does not have a link.
10GBase-T access port x link	Green or amber	Solid green	The port has a 10Gb link.
		Blinking	N/A
		Off	The port does not have a link.
		Solid amber	The port has a 1Gb link.
10GBase-T access port x activity	Green	Solid	The port has a link, but no activity is occurring on the port.
		Blinking	The port has a link, and activity is occurring on the port.
		Off	The port does not have a link.
25Gb SFP28 access port x link	Green	Solid	The port has a link, but no activity is occurring on the port.
		Off	The port does not have a link.
		Blinking	The port has a link, and activity is occurring on the port.
25Gb SFP28 access port x activity	Green or amber	Solid green	The port has a link that operates at 25Gb per second.
		Solid amber	The port has a link that operates at 10Gb per second.
		Blinking	N/A
		Off	The port does not have a link.
Server module identify	Blue	Solid	N/A
		Blinking	Beaconing is on for the server module.

LED	Color	State	Description
		Off	Beaconing is off for the server module.
Server module fault	Amber	Solid	The server module has a fault condition.
		Blinking	N/A
		Off	The server module is operating normally.
Server module health	Green	Solid	The server module is powered on.
		Blinking	The server module is in the process of booting.
		Off	The server module is powered off.
Management port activity	Green	Solid	N/A
		Blinking	Activity is occurring on the management port.
		Off	The management port is not connected to an active network.
POST code	Green	Solid/off	The eight POST code LEDs go on and off in different combinations while the server module performs self-diagnostics after powering on.

I/O module LEDs

Each I/O module in an expansion enclosure has multiple color-coded LEDs that indicate the status of the module and the status of the ports on the module. These LEDs are located along the right side of the front of the module, as shown in the figure below.



The table below describes these LEDs.

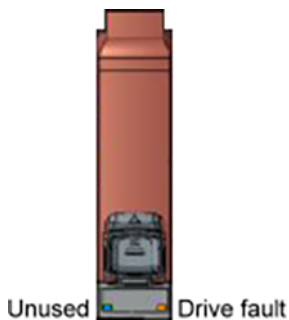
LED	Color	State	Description
SAS port x fault	Amber	Solid	The SAS port has a fault condition.
		Blinking	Beaconing is on for the SAS port.
		Off	The SAS port operating normally, and beaconing is off for the port.
SAS port x activity	Green	Solid	The SAS port has an active connection.
		Blinking	Activity is occurring on the SAS port.
		Off	The SAS port does not have an active connection.
I/O module fault	Amber	Solid	The I/O module has a fault condition.
		Blinking	Beaconing is on for the I/O module.
		Off	The I/O module is operating normally, and beaconing is off for the module.
I/O module power	Green	Solid	The I/O module is powered on.

LED	Color	State	Description
		Blinking	N/A
		Off	The I/O module is powered off.

Drive LEDs

Each data or database drive for an S11 or S31 Node has two color-coded LEDs, one blue and one amber. S11 and S31 Nodes don't use the blue LED.

The LEDs are located on the top of the drive at the end with the tab, as shown in the figure below.



The table below describes the amber LED.

LED	Color	State	Description
Drive fault	Amber	Solid	The drive has a fault condition.
		Blinking	Beaconing is on for the drive.
		Off	The drive is operating normally, and beaconing is off for the drive.

Beaconing

Some HCP S11 and S31 Node components have an LED that can serve as a beacon. When blinking, the beaconing LED lets you easily identify the applicable component in your data center.

In some situations, the S11 or S31 Node turns beaconing on or off automatically to help you identify components.

If you have the administrator or service role, you can use the HCP S Series Management Console or management API to turn beaconing on or off for enclosures, server modules, and I/O modules.

In the Management Console, you use the diagrams on the **ENCLOSURE** and **SERVER MODULE** pages to turn beaconing on or off for the applicable component. While beaconing is on for a component, the applicable LED blinks in the component diagram.

The procedure below uses the Management Console to turn beaconing on or off for a component.

Procedure

1. In the Management Console, go to **Hardware > Overview**.
2. Take one of these actions:
 - To turn beaconing on or off for an enclosure or for an I/O module in an enclosure, click the applicable enclosure.
 - To turn beaconing on or off for a server module, click the applicable server module.
3. Take one of these actions:
 - For an enclosure, in the **Front** diagram on the **ENCLOSURE** page, click any LED in the enclosure diagram or click anywhere on the enclosure background.
 - For a server module, in the **Front** diagram on the **SERVER MODULE** page, click any LED in the server module diagram or click anywhere on the server module background.
 - For an I/O module, in the **I/O Modules** diagram on the **ENCLOSURE** page, click any LED in the I/O module diagram or click anywhere on the I/O module background.
4. In the window that opens:
 - a. Click the slider to set beaconing to **On** or **Off**, as applicable.
 - b. Click **Close**.

Internal logs

HCP S Series Nodes maintain internal logs that record the status and activity of various components of the HCP S Series software. If a problem occurs with the S Series Node, the internal logs can assist support personnel in diagnosing and resolving the problem.



Note: S Series Node time is always expressed in UTC, so the datetime stamps on messages in the internal logs are in UTC.

If you have the administrator, monitor, security, or service role, you can use the HCP S Series Management Console or management API to insert comments into the S Series Node internal logs. You can use this capability, for example, to note unusual events that occur on the S Series Node. Comments can later assist support personnel in understanding the symptoms that indicate a possible problem. Comments can also assist support personnel in determining when a problem started.

To help with troubleshooting, if you have the administrator or service role, you can download the internal logs and send them to your HCP support center. You can use the HCP S Series Management Console or management API to download the logs. For ease of handling, the S Series Node downloads the logs into a single packed file. Neither this file nor the logs themselves are encrypted.

An S Series Node generally keeps internal logs for at least 120 days. However, it keeps the logs for a shorter time period if insufficient space is available for them. You can download the logs for any length of time within the period for which logs exist. When downloading the logs, be sure to include all the days on which you observed issues with the S Series Node.

Inserting comments into the internal logs

The procedure below uses the HCP S Series Management Console to insert a comment into the S Series Node internal logs.

Procedure

1. Log in to the Management Console using a user account with the administrator, monitor, security, or service role.
2. Go to **Monitor > Internal Logs**.
3. On the **INTERNAL LOGS** page, in the field in the **MARK INTERNAL LOGS** section, type the comment text. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
4. Click **Mark**.

Downloading the internal logs

Downloading the S Series Node internal logs is a two-part procedure. In the first part, the S Series Node prepares the logs for download by packing them into a .zip file. In the second part, the S Series Node performs the actual download. The amount of time the S Series Node takes to prepare the logs depends both on the length of time for which you request the logs and on the size of the log files.



Note: Downloading the internal logs puts a heavy load on the S Series Node. Do not take this action unless explicitly told to do so by your authorized service provider.

The procedure below uses the HCP S Series Management Console to download the internal logs.

Procedure

1. Log in to the Management Console using a user account with the administrator or service role.



Tip: To ensure that you consistently see correct status information during a log download operation, use a physical IP address to access the Management Console.

2. Go to **Monitor > Internal Logs**.
3. On the **INTERNAL LOGS** page, in the **DOWNLOAD INTERNAL LOGS** section:

- a. Click in the **Start date** field. Then, in the calendar that opens, select the date of the earliest logs you want to include in the download.

You cannot select a start date that's more than 120 days ago.

Logs are included starting from 12:00 a.m. UTC on the selected date.

- b. Click in the **End date** field. Then, in the calendar that opens, select the date of the most recent logs you want to include in the download.

Logs are included up to 1:00 a.m. UTC, inclusive, on the day following the selected date.

The end date must be later than the start date.

4. Click Prepare.

The S Series Node packs the logs into a .zip file. When the .zip file is ready to be downloaded, the **INTERNAL LOGS** page is automatically updated.

You do not need to stay on the **INTERNAL LOGS** page while the S Series Node is preparing the logs.



Important: While the logs are being prepared for download, do not restart a server module. Doing so causes the logs to remain in the prepare state indefinitely. If the logs do not exit the prepare state, contact your authorized service provider for help.

5. When the status of both server modules is Ready for log download, click Download.

The S Series Node downloads the prepared .zip file, and the **INTERNAL LOGS** page is automatically updated.

By default, the name of the ZIP file is `HCPLogs-yyyyMMdd-hhmm.zip`. Depending on the browser configuration, the browser either saves the file in a default location or prompts for where to save the file.

You do not need to stay on the **INTERNAL LOGS** page while the S Series Node is downloading the logs.

6. When the status of both server modules is Download complete, click Reset.

Chapter 7: Managing server modules

The two server modules in the base enclosure for an HCP S11 or S31 Node are located side by side at the back of the enclosure. Server module 1 is on the right. Server module 2 is on the left.



If you have the administrator or service role, you can use the HCP S Series Management Console or management API to:

- Power on an individual server module. You can do this only if the other server module is currently powered on.
- Reboot one or both server modules.
- Power off one or both server modules. Powering off both server modules effectively shuts down the S11 or S31 Node.

When you reboot or power off the server module that's hosting your connection to the Management Console, the connection is broken. To reconnect to the Management Console while the server module is rebooting or powered off, use the S11 or S31 Node domain name or an IP address for the other server module in the Management Console URL.

To power on the server modules after powering both of them off, disconnect all the power cables from the power supplies in the base enclosure and then reconnect the power cables. As soon as you reconnect the first power cable, the server modules start to power on.



Caution: When powering on an S11 or S31 Node, always power on all the expansion enclosures before you power on the server modules. When shutting down an S11 or S31 Node, always power off both server modules before powering off the expansion enclosures.

Powering off one or more expansion enclosures while one or both server modules are powered on can result in data unavailability and, possibly, even data loss.

The procedure below uses the Management Console to reboot, power off, or power on one or both server modules, as applicable.

Procedure

1. Log in to the Management Console using a user account with the administrator or service role.
2. Go to **Hardware > Overview** or **Hardware > Maintenance**.
3. On the **HARDWARE OVERVIEW** or **HARDWARE MAINTENANCE** page, click **Power Options**.
4. Under **Server Module**, select **Server module 1**, **Server module 2**, or **Server modules 1 and 2**, as applicable.
5. In the **Reason** field, type the reason why you're taking the applicable action. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
6. Click the action you want to take: **Power On**, **Restart** (reboot), or **Shut Down** (power off), as applicable.

Chapter 8: Maintaining HCP S Series Nodes

HCP S Series Node maintenance entails:

- Adding, removing, and replacing hardware components as necessary.

An S Series Node can operate correctly with multiple failed data drives, so failed data drives do not need immediate replacement. The S Series Node issues an alert when the number of failed data drives reaches the threshold at which the drives must be replaced. This threshold depends on the total number of data drives in the S Series Node.

Failed database drives should always be replaced immediately.

- Upgrading the HCP S Series operating system and software when new versions become available.
- Applying hotfixes to resolve specific issues.

To perform any of these activities, you must be an authorized service provider. Customers are not allowed to perform these activities by themselves.

Some maintenance activities are managed from the HCP S Series Management Console or by using the HCP S Series management API. Performing these activities requires a user account with the service role. Only authorized service providers should have user accounts with this role.

While a managed maintenance procedure is in progress, the Management Console displays this message at the top of each page:

```
Maintenance procedure in progress.
```

While an OS and software update is in progress, the Management Console displays this message at the top of each page:

```
Software update in progress.
```

If you have the administrator, monitor, or service role, you can use the Management Console or management API to see a list of the managed maintenance procedures that have been performed on the S Series Node since the HCP S Series software was last installed or reinstalled. If you have the administrator or service role, you can use the Management Console or management API to see a list of the software update procedures that have been performed on the S Series Node, going back to and including the last installation or reinstallation of the HCP S Series software.

To see the hardware maintenance procedure history list in the Management Console, go to Hardware > Maintenance. To see additional information about a procedure, click the gear icon (⚙️) for the procedure.

To see the software update history list in the Management Console, go to System > Update.

Chapter 9: Alerts and event log messages

The HCP S Series Node uses alerts to communicate current conditions. Each alert has a triggering event that is recorded in the S Series Node event log. Not all events trigger alerts, but for those that do, the alert text is the same as the detailed message text for the triggering event.

The table below lists the messages that the S Series Node can write to the event log. For each message, the table shows:

- The message ID
- The detailed message text
- An explanation of the event that caused the message to be logged
- The action, if any, you should take in response to the event
- The severity of the event:
 - N = Notice
 - W = Warning
 - E = Error
- An indication of whether the event triggers an alert

The messages are listed in order by message ID.

ID	Message	Explanation	Action	Sev.	Alert
1002	A test message has been sent to the syslog servers at the following IP addresses: <i>ip-address-list</i>	A user sent a test message to the syslog servers.	No action is required.	N	No
2619	An attempt to restart or shut down a server module failed (originating IP <i>ip-address</i>).	An attempt to restart or shut down a server module failed. The server module may already be down.	No action is required.	N	No
2621	Server module <i>server-module-number</i> failed to apply configuration changes.	An attempt to update the configuration of a server module failed. The internal configuration does not match the reported configuration.	Contact your authorized service provider.	E	No

ID	Message	Explanation	Action	Sev.	Alert
2622	Server module <i>server-module-number</i> failed to apply access configuration changes.	An attempt to update a configuration setting for external access to a server module failed. The internal configuration does not match the reported configuration.	Contact your authorized service provider.	E	No
2625	Server module <i>server-module-number</i> is now synchronized with time server <i>time-server-ip-address</i> .	A server module has been synchronized with an external time server.	No action is required.	N	No
2626	Server module <i>server-module-number</i> lost synchronization with time server <i>time-server-ip-address</i> .	An error occurred in synchronizing the time on a server module with the time on an external time server.	Check network connectivity and that network and time server settings are correct.	E	Yes
2627	Server module <i>server-module-number</i> is not synchronized with a time server.	An error occurred in synchronizing the time on a server module with the time on an external time server.	Check network connectivity and that network and time server settings are correct.	E	Yes
2629	File system <i>file-system-name</i> is <i>percent-full%</i> full on server module <i>server-module-number</i> .	A file system on a server module is reaching capacity.	Contact your authorized service provider.	W	Yes
2630	File system <i>file-system-name</i> is <i>percent-full%</i> full on server module <i>server-module-number</i> . Data access will be disabled if the file system usage reaches capacity.	A file system on a server module is nearly full. Data access will be disabled if the file system usage reaches capacity.	Contact your authorized service provider.	E	Yes
2631	Network interface <i>network-device</i> on server module <i>server-module-number</i> is down.	A network interface went down.	Check network connectivity. If a problem exists, contact your authorized service provider.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2632	Server module <i>server-module-number</i> is unavailable.	A server module is unavailable.	If this event is unexpected and the server module does not restart automatically, contact your authorized service provider. Do not try to restart the server module manually, as that may cause the loss of information needed to diagnose the problem.	E	Yes
2634	Communication from server module <i>server-module-number</i> to DNS servers <i>dns-server-ip-address-list</i> failed.	The HCP S Series Node was unable to establish connectivity to the DNS servers.	Check DNS settings.	E	Yes
2635	Server module <i>server-module-number</i> is available.	The HCP S Series software started on a server module.	No action is required	N	No
2636	Server module <i>server-module-number</i> is unavailable.	A server module is unavailable due to an in-progress upgrade.	If the server module does not restart automatically after the upgrade is complete, contact your authorized service provider.	N	Yes
2637	Server module <i>server-module-number</i> temperature sensor <i>sensor-name</i> has detected a temperature error condition; status: <i>temperature-status</i> .	A server-module temperature sensor is reporting a temperature that is out of the recommended range.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	E	Yes
2638	Server module <i>server-module-number</i> temperature sensor <i>sensor-name</i> has detected a temperature warning condition; status: <i>temperature-status</i> .	A server-module temperature sensor is reporting a temperature that is out of the recommended range.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
2639	Server module <i>server-module-number</i> temperature sensor <i>sensor-name</i> is no longer reporting an abnormal temperature condition.	A server-module temperature sensor is no longer reporting an abnormal temperature condition.	No action is required.	N	No
2640	Fan sensor <i>sensor-name</i> has triggered an alarm on server module <i>server-module-number</i> ; status: <i>fan-status</i> .	A fan sensor is reporting a fan speed that is out of the recommended range.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	E	Yes
2641	Fan sensor <i>sensor-name</i> has triggered a warning on server module <i>server-module-number</i> ; status: <i>fan-status</i> .	A fan sensor is reporting a fan speed that is out of the recommended range.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	W	Yes
2642	Fan sensor <i>sensor-name</i> has removed the alarm on server module <i>server-module-number</i> .	A fan sensor is reporting a return to an acceptable fan speed.	No action is required.	N	No
2643	Server module <i>server-module-number</i> voltage sensor <i>sensor-name</i> has detected a voltage error condition; status: <i>voltage-status</i> .	A server-module voltage sensor is reporting a voltage that is out of the recommended range.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	E	Yes
2644	Server module <i>server-module-number</i> voltage sensor <i>sensor-name</i> has detected a voltage warning condition; status: <i>voltage-status</i> .	A server-module voltage sensor is reporting a voltage that is out of the recommended range.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	W	Yes
2645	Server module <i>server-module-number</i> voltage sensor <i>sensor-name</i> is no longer reporting an abnormal voltage condition.	A server-module voltage sensor is no longer reporting an abnormal voltage condition.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2646	Power supply <i>power-supply-name</i> has triggered an alarm on server module <i>server-module-number</i> ; status: <i>power-supply-status</i> .	A power supply is reporting a problem.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	E	Yes
2647	Power supply <i>power-supply-name</i> has triggered a warning on server module <i>server-module-number</i> ; status: <i>power-supply-status</i> .	A power supply is reporting a problem.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	W	Yes
2648	Power supply <i>power-supply-name</i> has removed an alarm on server module <i>server-module-number</i> .	A power supply is reporting that it has returned to a fully functional state.	No action is required.	N	No
2649	Server module <i>server-module-number</i> processor <i>processor-name</i> has an error condition; status: <i>processor-status</i> .	A server-module processor has an error condition.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	E	Yes
2650	Server module <i>server-module-number</i> processor <i>processor-name</i> has a warning condition; status: <i>processor-status</i> .	A server-module processor has a warning condition.	Check that the server module is functioning properly. If a problem exists, contact your authorized service provider.	W	Yes
2651	Server module <i>server-module-number</i> processor <i>processor-name</i> is no longer in an abnormal condition.	A server-module processor is now functioning properly.	No action is required.	N	No
2652	File system <i>file-system-name</i> is <i>percent-full%</i> full on server module <i>server-module-number</i> . Data access has been disabled.	A file system on a server module is full. Data access has been disabled.	Contact your authorized service provider.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2653	Server module <i>server-module-number</i> swap utilization is too high.	Swap utilization on a server module is too high.	Contact your authorized service provider.	N	No
2654	Server module <i>server-module-number</i> CPU load average is too high.	The CPU load average on a server module is too high.	Contact your authorized service provider.	N	No
2655	Server module <i>server-module-number</i> BMC is no longer accessible.	The baseboard management controller (BMC) in a server module is inaccessible.	Check that the server module is powered on and that the server interconnect network is healthy.	E	Yes
2656	Server module <i>server-module-number</i> BMC is now accessible.	The baseboard management controller (BMC) in a server module is accessible.	No action is required.	N	No
2657	Server module <i>server-module-number</i> is powered off.	A server module is powered off.	Check the server module power and network connectivity.	E	Yes
2658	Server module <i>server-module-number</i> was powered on.	A server module was powered on.	No action is required.	N	No
2659	Network interface <i>network-device</i> is not operating at the correct speed on server module <i>server-module-number</i> .	Either the network interfaces in a bonded network interface are not operating at the same speed, or they are not operating at the requested speed.	Check that the server module is functioning properly and that the network infrastructure is configured correctly. If the problem persists, contact your authorized service provider.	W	Yes
2660	Network interface <i>network-device</i> is now operating at the correct speed on server module <i>server-module-number</i> .	A network interface is now operating at the correct speed.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2661	Network interface <i>network-device</i> is not operating at the correct MTU on server module <i>server-module-number</i> .	A network interface is not operating at the requested MTU.	Check that the server module is functioning properly and that the network infrastructure is configured correctly. If the problem persists, contact your authorized service provider.	W	Yes
2662	Network interface <i>network-device</i> is now operating at the correct MTU on server module <i>server-module-number</i> .	A network interface is now operating at the correct MTU.	No action is required.	N	No
2665	Network interface <i>network-device</i> is not operating in the correct bonding mode on server module <i>server-module-number</i> .	A network interface is not operating in the correct bonding mode.	Check that the server module is functioning properly and that the network infrastructure is configured correctly. If the problem persists, contact your authorized service provider.	W	Yes
2666	Network interface <i>network-device</i> is now operating in the correct bonding mode on server module <i>server-module-number</i> .	A network interface is now operating in the correct bonding mode.	No action is required.	N	No
2667	Server module <i>server-module-number</i> swap utilization is below the error threshold.	Swap utilization on a server module is no longer too high.	No action required.	N	No
2668	Server module <i>server-module-number</i> CPU load average is below the error threshold.	The CPU load average on a server module is no longer too high.	No action required.	N	No
2669	All DNS servers are accepting communications.	The HCP S Series Node can communicate with all the DNS servers.	No action required.	N	No
2670	Network interface <i>network-device</i> on server module <i>server-module-number</i> is up.	A network interface that was down is now up.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2671	Network interface <i>network-device</i> on server module <i>server-module-number</i> is connected to an active network but should not be.	An access network port that is set to OFF is connected to an active network.	Check that the access network port connections match the port settings for the S Series Node.	E	Yes
2672	The connection expectation for network interface <i>network-device</i> on server module <i>server-module-number</i> is now satisfied.	A port connection expectation is now satisfied.	No action is required.	N	No
2673	File system <i>file-system-name</i> is <i>percent-full%</i> full on server module <i>server-module-number</i> .	A file system that was reaching capacity is no longer reaching capacity.	No action is required.	N	No
2674	<i>maintenance-procedure-type</i> maintenance procedure was started.	A maintenance procedure was started.	No action is required.	N	No
2675	<i>maintenance-procedure-type</i> maintenance procedure was completed.	A maintenance procedure was completed.	No action is required.	N	No
2676	<i>maintenance-procedure-type</i> maintenance procedure was canceled.	A maintenance procedure was canceled.	No action is required.	W	No
2678	<i>maintenance-procedure-type</i> maintenance procedure timed out.	A maintenance procedure timed out.	No action is required.	W	No
2679	<i>maintenance-procedure-type</i> maintenance procedure finished with errors.	A maintenance procedure finished with errors.	Use a new maintenance procedure to correct the errors.	E	No

ID	Message	Explanation	Action	Sev.	Alert
2680	Server module <i>server-module-number</i> hardware is unsupported (vendor: <i>server-module-vendor</i> , product: <i>server-module-model</i> , rev: <i>server-module-firmware-revision</i>).	Server module hardware is unsupported.	Contact your authorized service provider.	E	Yes
2681	Server module <i>server-module-number</i> hardware is now supported (vendor: <i>server-module-vendor</i> , product: <i>server-module-model</i> , rev: <i>server-module-firmware-revision</i>).	Server module hardware is now supported.	No action is required.	N	No
2682	An OS SSD in server module <i>server-module-number</i> is unsupported (vendor: <i>ssd-vendor</i> , product: <i>ssd-model</i> , rev: <i>ssd-firmware-revision</i> , wwid: <i>ssd-wwid</i>).	An OS SSD is unsupported.	Contact your authorized service provider.	E	Yes
2683	An OS SSD in server module <i>server-module-number</i> is now supported (vendor: <i>ssd-vendor</i> , product: <i>ssd-model</i> , rev: <i>ssd-firmware-revision</i> , wwid: <i>ssd-wwid</i>).	An OS SSD is now supported.	No action is required.	N	No
2684	A drive error was detected (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive error was detected.	After data has been migrated off of the drive, replace the drive. Data is guaranteed to have been migrated off the drive when the count of bytes under repair shown is zero.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2685	A drive error has been cleared (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , drive-wwid: <i>wwid</i>).	A data drive error was cleared.	No action is required.	N	No
2686	An OS SSD error was detected in server module <i>server-module-number</i> (serial number: <i>ssd-serial-number</i> , wwid: <i>ssd-wwid</i>).	An OS SSD error was detected.	Replace the SSD.	E	Yes
2687	An OS SSD error in server module <i>server-module-number</i> has been cleared (serial number: <i>ssd-serial-number</i> , wwid: <i>ssd-wwid</i>).	An OS SSD error was cleared.	No action is required.	N	No
2688	A drive is not properly configured for internal monitoring (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive is not properly configured for internal monitoring.	Contact your authorized service provider.	W	Yes
2689	A drive is now properly configured for internal monitoring (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive is now properly configured for internal monitoring.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2690	An OS SSD in server module <i>server-module-number</i> is not properly configured for internal monitoring (serial number: <i>ssd-serial-number</i> , wwid: <i>ssd-wwid</i>).	An OS SSD is not properly configured for internal monitoring.	Contact your authorized service provider.	W	Yes
2691	An OS SSD in server module <i>server-module-number</i> is now properly configured for internal monitoring (serial number: <i>ssd-serial-number</i> , wwid: <i>ssd-wwid</i>).	An OS SSD is now properly configured for internal monitoring.	No action is required.	N	No
2692	The HCP S Series Node license expired on <i>license-expiration-date</i> .	The HCP S Series Node license is expired.	Contact your authorized service provider.	E	Yes
2693	The HCP S Series Node license is no longer expired (expiration: <i>license-expiration-date</i>).	The HCP S Series Node license is no longer expired.	No action is required.	N	No
2694	The licensed capacity for the HCP S Series Node is exceeded (capacity: <i>actual-total-capacity</i> , licensed: <i>licensed-capacity</i>).	The physical capacity of the HCP S Series Node exceeds the licensed capacity.	Contact your authorized service provider.	E	Yes
2695	The licensed capacity for the HCP S Series Node is no longer exceeded (capacity: <i>actual-total-capacity</i> , licensed: <i>licensed-capacity</i>).	The physical capacity of the HCP S Series Node no longer exceeds the licensed capacity.	No action is required.	N	No
2696	The HCP S Series Node is not licensed.	The HCP S Series Node is not licensed.	Contact your authorized service provider.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2697	The HCP S Series Node is now licensed (serial number: <i>s-series-node-serial-number</i> , quote number: <i>quote-number</i> , capacity: <i>licensed-capacity</i> , expiration: <i>license-expiration-date</i>).	The HCP S Series Node is now licensed.	No action is required.	N	No
2698	A drive error was detected (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data drive error was detected.	After data has been migrated off of the drive, replace the drive. Data is guaranteed to have been migrated off the drive when the count of bytes under repair is zero.	N	Yes
2699	Server module <i>server-module-number</i> beaoning is on.	Beaoning is on for a server module.	No action is required.	N	Yes
2700	Server module <i>server-module-number</i> beaoning is now off.	Beaoning is now off for a server module.	No action is required.	N	No
2701	A database drive is <i>percent-worn%</i> worn (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A database drive is close to the end of its expected life span.	Replace the drive.	W	Yes
2702	Network interface <i>network-device</i> on server module <i>server-module-number</i> is down.	A network interface went down.	Check network connectivity. If a problem exists, contact your authorized service provider.	N	No
2703	The password for the user account with username <i>username</i> was updated.	A user updated a user account password.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2704	A user with username <i>username</i> successfully logged in to the HCP S Series Management Console from <i>ip-address:port-number</i> .	A user login to the HCP S Series Management Console was successful.	No action is required.	N	No
2705	A user with username <i>username</i> failed to log in to the HCP S Series Management Console from <i>ip-address:port-number</i> .	A user attempt to log in to the HCP S Series Management Console failed.	No action is required.	W	No
2706	An attempt was made to access the HCP S Series Node with the unknown username <i>username</i> from <i>ip-address:port-number</i> .	A user tried to access the HCP S Series Management Console or management API with an unknown username.	Have the user try again with a valid username and password.	W	No
2707	An attempt to access the HCP S Series Node with username <i>username</i> from <i>ip-address:port-number</i> failed because the password is invalid.	A user tried to access the HCP S Series Management Console or management API with an invalid password.	Have the user try again with a valid username and password.	W	No
2708	The user account with ID <i>user-account-id</i> and username <i>username</i> has been automatically disabled because it had <i>failed-attempt-threshold</i> or more failed attempts to access the HCP S Series Node.	A user account was automatically disabled due to too many failed attempts to access the HCP S Series Management Console or management API.	Reenable the user account. Then have the user try again with a valid username and password.	W	No
2709	An attempt to access the HCP S Series Node with user account ID <i>user-account-id</i> and username <i>username</i> failed because the account is disabled.	A user tried to access the HCP S Series Management Console or management API with a disabled user account.	Reenable the user account to allow the user to access the applicable interface.	W	No

ID	Message	Explanation	Action	Sev.	Alert
2710	The user account with ID <i>user-account-id</i> and username <i>username</i> has been automatically disabled because it has been inactive for <i>number-of-days</i> or more consecutive days.	A user account was automatically disabled because it was inactive for too many days.	If the account owner should have access to the HCP S Series Node, re-enable the user account.	W	No
2711	An attempt to log in to the HCP S Series Management Console with user account ID <i>user-account-id</i> and username <i>username</i> failed because the account is disabled.	A user tried to log in to the HCP S Series Management Console with a disabled user account.	Reenable the user account to allow the user to log in.	W	No
2712	An attempt was made to log in to the HCP S Series Management Console with the unknown username <i>username</i> from <i>ip-address:port-number</i> .	A user tried to log in to the HCP S Series Management Console with an unknown username.	Have the user try again with a valid username and password.	W	No
2713	A user with user account ID <i>user-account-id</i> from <i>ip-address:port-number</i> failed to access a requested page in the HCP S Series Management Console.	The user account password or roles may have been modified since the last request to access a page in the HCP S Series Management Console.	Have the user log in to the Console again with a valid username and password.	W	No
2714	The user account with ID <i>user-account-id</i> and username <i>username</i> has been automatically re-enabled after being disabled for <i>number-of-minutes</i> minutes.	A disabled user account was automatically re-enabled.	No action is required.	N	No
2715	Network interface <i>network-device</i> on server module <i>server-module-number</i> is not connected to an active network but should be.	An access network port that is set to ON is not connected to an active network.	Check that the access network port connections match the port settings for the S Series Node.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2716	Beaconing has been requested for a component.	A user requested beaconing for a component.	No action is required.	N	No
2720	A database backup finished successfully.	The HCP S Series Node database was successfully backed up.	No action is required.	N	No
2721	A database backup failed.	An attempt to back up the HCP S Series Node database failed.	Contact your authorized service provider.	E	No
2750	Server module <i>server-module-number</i> operating system partition <i>partition-name</i> is being synchronized (<i>percent-complete</i>).	Operating system partition synchronization is in progress.	No action is required.	N	Yes
2751	Server module <i>server-module-number</i> operating system partition <i>partition-name</i> synchronization is complete.	Operating system partition synchronization is complete.	No action is required.	N	No
2752	Server module <i>server-module-number</i> database partition is being synchronized (<i>percent-complete</i>).	Database partition synchronization is in progress.	No action is required.	N	Yes
2753	Server module <i>server-module-number</i> database partition synchronization is complete.	Database partition is synchronization is complete.	No action is required.	N	No
2754	Server module <i>server-module-number</i> operating system partition <i>partition-name</i> is being recovered (<i>percent-complete</i>).	Operating system partition recovery is in progress.	No action is required.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
2755	Server module <i>server-module-number</i> operating system partition <i>partition-name</i> recovery is complete.	Operating system partition recovery is complete.	No action is required.	N	No
2756	Server module <i>server-module-number</i> database partition is being recovered (<i>percent-complete</i>).	Database partition recovery is in progress.	No action is required.	W	Yes
2757	Server module <i>server-module-number</i> database partition recovery is complete.	Database partition recovery is complete.	No action is required.	N	No
2758	Server module <i>server-module-number</i> operating system partition <i>partition-name</i> is degraded.	An operating system partition is degraded.	Replace the applicable SSD.	E	Yes
2759	Server module <i>server-module-number</i> operating system partition <i>partition-name</i> is no longer degraded.	An operating system partition is no longer degraded.	No action is required.	N	No
2760	A server module <i>server-module-number</i> database partition is degraded.	A database partition is degraded.	No action is required.	E	Yes
2761	A server module <i>server-module-number</i> database partition is no longer degraded.	A database partition is no longer degraded.	No action is required.	N	No
2762	Drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , FRU part number: <i>part-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive failed.	Remove or replace the drive.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2763	Drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , FRU part number: <i>part-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive failed.	A data or database drive has failed but does not yet require replacement. Replace the drive when the HCP S Series Node reports that the threshold for drive replacement has been reached.	N	Yes
2764	An OS SSD error was detected in server module <i>server-module-number</i> (FRU part number: <i>part-number</i> , serial number: <i>ssd-serial-number</i> , wwid: <i>ssd-wwid</i>).	An OS SSD error was detected.	Replace the SSD.	E	Yes
2765	Server module <i>server-module-number</i> operating system partition <i>partition-name</i> is degraded (FRU part number: <i>part-number</i>).	An operating system partition is degraded.	Replace the applicable SSD.	E	Yes
2800	The cover for enclosure <i>enclosure-number</i> has been opened outside of a maintenance procedure.	An enclosure cover is open outside of a maintenance procedure.	Close the enclosure cover.	E	Yes
2801	The cover for enclosure <i>enclosure-number</i> has been opened during a maintenance procedure.	An enclosure cover is open during a maintenance procedure.	No action is required.	N	Yes
2802	The cover for enclosure <i>enclosure-number</i> has been closed.	An enclosure cover was closed.	No action is required.	N	No
2821	Enclosure <i>enclosure-number</i> temperature sensor <i>sensor-name</i> has detected an over-temperature error condition.	An enclosure temperature sensor is reporting an over-temperature error condition.	Check that the enclosure power supplies are functioning properly. If a problem exists, contact your authorized service provider.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2822	Enclosure <i>enclosure-number</i> temperature sensor <i>sensor-name</i> is no longer reporting an over-temperature error condition.	An enclosure temperature sensor is no longer reporting an over-temperature error condition.	No action is required.	N	No
2823	Enclosure <i>enclosure-number</i> temperature sensor <i>sensor-name</i> has detected an over-temperature warning condition.	An enclosure temperature sensor is reporting an over-temperature warning condition.	Check that the enclosure power supplies are functioning properly. If a problem exists, contact your authorized service provider	W	Yes
2824	Enclosure <i>enclosure-number</i> temperature sensor <i>sensor-name</i> is no longer reporting an over-temperature warning condition.	An enclosure temperature sensor is no longer reporting an over-temperature warning condition.	No action is required.	N	No
2825	Enclosure <i>enclosure-number</i> temperature sensor <i>sensor-name</i> has detected an under-temperature error condition.	An enclosure temperature sensor is reporting an under-temperature error condition.	Check that the enclosure power supplies are functioning properly. If a problem exists, contact your authorized service provider.	E	Yes
2826	Enclosure <i>enclosure-number</i> temperature sensor <i>sensor-name</i> is no longer reporting an under-temperature error condition.	An enclosure temperature sensor is no longer reporting an under-temperature error condition.	No action is required.	N	No
2827	Enclosure <i>enclosure-number</i> temperature sensor <i>sensor-name</i> has detected an under-temperature warning condition.	An enclosure temperature sensor is reporting an under-temperature warning condition.	Check that the enclosure power supplies are functioning properly. If a problem exists, contact your authorized service provider.	W	Yes
2828	Enclosure <i>enclosure-number</i> temperature sensor <i>sensor-name</i> is no longer reporting an under-temperature warning condition.	An enclosure temperature sensor is no longer reporting an under-temperature warning condition.	No action is required	N	No

ID	Message	Explanation	Action	Sev.	Alert
2833	Enclosure <i>enclosure-number</i> voltage sensor <i>sensor-name</i> has detected an over-voltage failure condition.	An enclosure voltage sensor has reported an over-voltage failure condition.	Check the power and cooling modules.	E	Yes
2834	Enclosure <i>enclosure-number</i> voltage sensor <i>sensor-name</i> is no longer reporting an over-voltage failure condition.	An enclosure voltage sensor is no longer reporting an over-voltage failure condition.	No action is required.	N	No
2835	Enclosure <i>enclosure-number</i> voltage sensor <i>sensor-name</i> has detected an over-voltage warning condition.	An enclosure voltage sensor has reported an over-voltage warning condition.	Check the power and cooling modules.	W	Yes
2836	Enclosure <i>enclosure-number</i> voltage sensor <i>sensor-name</i> is no longer reporting an over-voltage warning condition.	An enclosure voltage sensor is no longer reporting an over-voltage warning condition.	No action is required.	N	No
2837	Enclosure <i>enclosure-number</i> voltage sensor <i>sensor-name</i> has detected an under-voltage failure condition.	An enclosure voltage sensor has reported an under-voltage failure condition.	Check the power and cooling modules.	E	Yes
2838	Enclosure <i>enclosure-number</i> voltage sensor <i>sensor-name</i> is no longer reporting an under-voltage failure condition.	An enclosure voltage sensor is no longer reporting an under-voltage failure condition.	No action is required.	N	No
2839	Enclosure <i>enclosure-number</i> voltage sensor <i>sensor-name</i> has detected an under-voltage warning condition.	An enclosure voltage sensor has reported an under-voltage warning condition.	Check the power and cooling modules.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
2840	Enclosure <i>enclosure-number</i> voltage sensor <i>sensor-name</i> is no longer reporting an under-voltage warning condition.	An enclosure voltage sensor is no longer reporting an under-voltage warning condition.	No action is required.	N	No
2841	Enclosure <i>enclosure-number</i> current sensor <i>sensor-name</i> has detected an over-current failure condition.	An enclosure current sensor has reported an over-current failure condition.	Check the power and cooling modules.	E	Yes
2842	Enclosure <i>enclosure-number</i> current sensor <i>sensor-name</i> is no longer reporting an over-current failure condition.	An enclosure current sensor is no longer reporting an over-current failure condition.	No action is required.	N	No
2843	Enclosure <i>enclosure-number</i> current sensor <i>sensor-name</i> has detected an over-current warning condition.	An enclosure current sensor has reported an over-current warning condition.	Check the power and cooling modules.	W	Yes
2844	Enclosure <i>enclosure-number</i> current sensor <i>sensor-name</i> is no longer reporting an over-current warning condition.	An enclosure current sensor is no longer reporting an over-current warning condition.	No action is required.	N	No
2845	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) component <i>component-name</i> is reporting a status of <i>component-status</i> .	The status of an enclosure component has changed.	Check that all components are operating normally.	E	Yes
2846	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) component <i>component-name</i> is reporting a status of <i>component-status</i> .	The status of an enclosure component has changed.	Check that all components are operating normally.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
2847	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) component <i>component-name</i> is reporting a status of <i>component-status</i> .	The status of an enclosure component has changed.	No action is required.	N	Yes
2848	Enclosure <i>enclosure-number</i> component <i>component-name</i> beaconing is on.	Beaconing is on for an enclosure component.	No action is required.	N	Yes
2849	Enclosure <i>enclosure-number</i> component <i>component-name</i> beaconing is now off.	Beaconing is now off for an enclosure component.	No action is required.	N	No
2850	Enclosure <i>enclosure-number</i> component <i>component-name</i> is marked failed.	An enclosure component has been marked failed.	Check that the enclosure component is operating properly. If it isn't, replace the component.	E	Yes
2851	Enclosure <i>enclosure-number</i> component <i>component-name</i> failure has been cleared.	An enclosure component is no longer marked failed.	No action is required.	N	No
2852	Enclosure <i>enclosure-number</i> hardware component <i>component-name</i> has been changed.	An enclosure hardware component changed (for example, an I/O module was removed or reinserted).	Verify that this is an expected event.	E	No
2854	The drive in enclosure <i>enclosure-number</i> slot <i>slot-number</i> has been powered off.	A drive was powered off.	If this is an unexpected event, check the health of the drive.	E	Yes
2855	The drive in enclosure <i>enclosure-number</i> slot <i>slot-number</i> has been powered on.	A drive was powered on.	No action is required.	N	No
2856	Enclosure <i>enclosure-number</i> has a warning condition.	An enclosure has a warning condition.	Check that the enclosure is operating normally.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
2857	Enclosure <i>enclosure-number</i> warning has been cleared.	An enclosure no longer has a warning condition.	No action is required.	N	No
2858	Enclosure <i>enclosure-number</i> hardware component <i>component-name</i> has been changed during a maintenance procedure.	An enclosure hardware component has been changed during a maintenance procedure.	Complete the maintenance procedure.	N	No
2859	Enclosure <i>enclosure-number</i> slot <i>slot-number</i> has been marked failed.	An enclosure slot has been marked failed.	Replace the drive in the slot.	E	Yes
2860	Enclosure <i>enclosure-number</i> slot <i>slot-number</i> failure has been cleared.	An enclosure slot is no longer marked failed.	No action is required.	N	No
2861	Enclosure <i>enclosure-number</i> slot <i>slot-number</i> hardware has been changed outside of a maintenance procedure.	Enclosure slot hardware has been marked as changed outside of a maintenance procedure.	If the drive is unavailable, use the remove drives and add drives maintenance procedures to correct the problem.	E	No
2863	Enclosure <i>enclosure-number</i> slot <i>slot-number</i> hardware has been changed during a maintenance procedure.	Enclosure slot hardware has been marked as changed during a maintenance procedure.	Complete the maintenance procedure.	N	No
2866	Server module <i>server-module-number</i> has been marked failed.	A server module has been marked failed.	Check that the server module is operating normally. If it isn't, replace the server module.	E	Yes
2867	Server module <i>server-module-number</i> failure has been cleared.	A server module is no longer marked failed.	No action is required	N	No
2868	Enclosure <i>enclosure-number</i> <i>pcm-fan-name</i> has been marked failed.	A power and cooling module fan has been marked failed.	Check that the power and cooling module is functioning properly. If it isn't, replace the power and cooling module.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2869	Enclosure <i>enclosure-number pcm-fan-name</i> failure has been cleared.	A power and cooling module fan is no longer marked failed.	No action is required.	N	No
2870	Enclosure <i>enclosure-number</i> is in lockdown mode.	An enclosure is in lockdown mode.	Contact your authorized service provider.	E	Yes
2871	Enclosure <i>enclosure-number</i> is no longer in lockdown mode.	An enclosure is no longer in lockdown mode.	No action is required.	N	No
2872	Enclosure <i>enclosure-number</i> hardware is unsupported (vendor: <i>enclosure-vendor</i> , product: <i>enclosure-model</i> , rev: <i>enclosure-firmware-revision</i> , wwid: <i>enclosure-wwid</i>).	Enclosure hardware is unsupported.	Contact your authorized service provider.	E	Yes
2873	Enclosure <i>enclosure-number</i> hardware is now supported (vendor: <i>enclosure-vendor</i> , product: <i>enclosure-model</i> , rev: <i>enclosure-firmware-revision</i> , wwid: <i>enclosure-wwid</i>).	Enclosure hardware is now supported.	No action is required.	N	No
2876	Enclosure <i>enclosure-number</i> slot <i>slot-number</i> drive hardware is unsupported (vendor: <i>drive-vendor</i> , product: <i>drive-model</i> , rev: <i>drive-firmware-revision</i> , wwid: <i>drive-wwid</i>).	Data or database drive hardware is unsupported.	Contact your authorized service provider.	E	Yes
2877	Enclosure <i>enclosure-number</i> slot <i>slot-number</i> drive hardware is now supported (vendor: <i>drive-vendor</i> , product: <i>drive-model</i> , rev: <i>drive-firmware-revision</i> , wwid: <i>drive-wwid</i>).	Data or database drive hardware is now supported.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2878	Enclosure <i>enclosure-number</i> SAS expanders have different firmware versions.	The enclosure SAS expanders have different firmware versions.	Update the enclosure SAS expander firmware.	E	Yes
2879	Enclosure <i>enclosure-number</i> SAS expanders no longer have different firmware versions.	The enclosure SAS expanders now have matching firmware versions.	No action is required.	N	No
2880	Enclosure <i>enclosure-number</i> is not reporting status information.	An enclosure is not reporting status information.	Contact your authorized service provider.	E	Yes
2881	Enclosure <i>enclosure-number</i> is now reporting status information.	An enclosure is now reporting status information.	No action is required.	N	No
2882	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) slot <i>slot-number</i> is reporting a status of <i>slot-status</i> .	The status of an enclosure slot changed.	No action is required.	E	Yes
2883	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) slot <i>slot-number</i> is reporting a status of <i>slot-status</i> .	The status of an enclosure slot changed.	No action is required.	W	Yes
2884	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) slot <i>slot-number</i> is reporting a status of <i>slot-status</i> .	The status of an enclosure slot changed.	No action is required	N	Yes
2885	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) is reporting a status of <i>enclosure-status</i> .	The status of the enclosure has changed.	Check that the enclosure is operating normally.	E	Yes
2886	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) is reporting a status of <i>enclosure-status</i> .	The status of the enclosure has changed.	Check that the enclosure is operating normally.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
2887	Enclosure <i>enclosure-number</i> (serial number <i>serial-number</i>) is reporting a status of <i>enclosure-status</i> .	The status of the enclosure has changed.	No action is required.	N	Yes
2888	A component in enclosure <i>enclosure-number</i> is reporting a failure.	An enclosure component reported a failure.	Check that the enclosure component is operating correctly.	E	Yes
2889	Enclosure <i>enclosure-number</i> failure has been cleared.	An enclosure component is longer reporting a failure.	No action is required.	N	No
2890	Enclosure <i>enclosure-number</i> hardware has been changed.	Enclosure hardware changed	Verify that this is an expected event. If it isn't, contact your authorized service provider.	E	No
2891	Enclosure <i>enclosure-number</i> hardware has been changed during a maintenance procedure.	Enclosure hardware changed during a maintenance procedure	Complete the maintenance procedure.	E	No
2892	Enclosure <i>enclosure-number</i> beaoning is on.	Beaoning is on for an enclosure.	No action is required.	N	Yes
2893	Enclosure <i>enclosure-number</i> beaoning is now off.	Beaoning is now off for an enclosure.	No action is required.	N	No
2894	Enclosure <i>enclosure-number</i> slot <i>slot-number</i> has been marked failed.	An enclosure slot has been marked failed.	Replace the drive in the slot.	N	No
2895	Server module <i>server-module-number</i> beaoning is on.	Beaoning is on for a server module.	No action is required.	N	Yes
2896	Server module <i>server-module-number</i> beaoning is now off.	Beaoning is now off for a server module.	No action is required.	N	No
2897	Server module <i>server-module-number</i> is reporting a status of <i>server-module-status</i> .	The status of a server module has changed.	Check that all server module components are operating normally.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2898	Server module <i>server-module-number</i> is reporting a status of <i>server-module-status</i> .	The status of a server module has changed.	Check that all server module components are operating normally.	W	Yes
2899	Server module <i>server-module-number</i> is reporting a status of <i>server-module-status</i> .	The status of server module has changed.	No action is required.	N	Yes
2900	Server module <i>server-module-number</i> drive initialization is complete (data: <i>total-number-of-data-drives-processed</i> , failed: <i>number-of-failed-drives</i> , unavailable: <i>number-of-unavailable-drives</i> , discovered: <i>number-of-drives-discovered</i> , database: <i>total-number-of-database-drives-processed</i>).	Server module drive initialization is complete.	No action is required.	N	No
2901	Drive is unavailable on server module <i>server-module-number</i> (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive either was removed outside of a maintenance procedure or has become unavailable.	Use the HCP S Series Management Console to check the health of the drive.	E	Yes
2902	Drive is now available on server module <i>server-module-number</i> (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive that was unavailable is now available.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2903	Server module <i>server-module-number</i> detected a new drive (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A new data or database drive was detected.	Complete the active maintenance procedure.	N	No
2904	Server module <i>server-module-number</i> added a data drive (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data drive was added.	No action is required.	N	No
2905	Server module <i>server-module-number</i> formatted a data drive (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data drive was formatted.	No action is required.	N	No
2906	Server module <i>server-module-number</i> removed a drive (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was removed.	No action is required.	N	No
2907	Server module <i>server-module-number</i> detected new drive firmware (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	New data or database drive firmware was detected.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2908	Server module <i>server-module-number</i> marked a drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive has been marked failed.	Remove or replace the drive.	E	No
2909	Server module <i>server-module-number</i> detected a new drive outside of a maintenance procedure and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was added outside of a maintenance procedure and has been marked failed.	Use maintenance procedures to remove and then add the drive.	E	No
2910	Server module <i>server-module-number</i> failed to add a drive and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed because it could not be added.	Replace the drive.	E	No
2911	Server module <i>server-module-number</i> detected a moved drive and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed because it was moved.	Use maintenance procedures to remove and then add the drive.	E	No

ID	Message	Explanation	Action	Sev.	Alert
2912	Server module <i>server-module-number</i> detected an incorrect drive WWID and marked the drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed due to an incorrect WWID.	Replace the drive.	E	No
2913	Server module <i>server-module-number</i> detected an incorrect drive serial number and marked the drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed due to an incorrect serial number.	Replace the drive.	E	No
2914	Server module <i>server-module-number</i> detected an unavailable drive and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed because it is unavailable.	Replace the drive.	E	No
2915	Server module <i>server-module-number</i> failed to format a data drive and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A drive was marked failed because it could not be formatted.	Use maintenance procedures to remove and then add the drive. If that doesn't fix the problem, replace the drive.	E	No

ID	Message	Explanation	Action	Sev.	Alert
2916	Server module <i>server-module-number</i> failed to add a data drive due to an I/O error (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data drive could not be added due to an I/O error.	Use maintenance procedures to remove and then add the drive. If that doesn't fix the problem, replace the drive.	E	No
2917	Server module <i>server-module-number</i> failed to remove a drive (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A drive could not be removed.	Use a maintenance procedure to remove or replace the drive. If that doesn't fix the problem, contact your authorized service provider.	E	No
2918	Server module <i>server-module-number</i> added a database drive (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A server module added a database drive.	No action is required.	N	No
2919	Drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive failed.	Remove or replace the drive.	E	Yes
2920	Drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive failed.	Remove or replace the drive.	N	Yes
2921	Drive unavailable (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive either was removed outside of a maintenance procedure or has become unavailable.	Use the HCP S Series Management Console to check the health of the drive.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2922	Drive unavailable (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive either was removed outside of a maintenance procedure or has become unavailable.	Use the HCP S Series Management Console to check the health of the drive.	N	Yes
2923	Server module <i>server-module-number</i> marked a drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive has been marked failed.	Remove or replace the drive.	N	No
2924	Server module <i>server-module-number</i> detected a new drive outside of a maintenance procedure and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was added outside of a maintenance procedure and has been marked failed.	Use maintenance procedures to remove and then add the drive.	N	No
2925	Server module <i>server-module-number</i> failed to add a drive and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed because it could not be added.	Replace the drive.	N	No
2926	Server module <i>server-module-number</i> detected a moved drive and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed because it was moved.	Use maintenance procedures to remove and then add the drive.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2927	Server module <i>server-module-number</i> detected an incorrect drive WWID and marked the drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed due to an incorrect WWID.	Replace the drive.	N	No
2928	Server module <i>server-module-number</i> detected an incorrect drive serial number and marked the drive failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed due to an incorrect serial number.	Replace the drive.	N	No
2929	Server module <i>server-module-number</i> detected an unavailable drive and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive was marked failed because it is unavailable.	Replace the drive.	N	No
2930	Server module <i>server-module-number</i> failed to format a data drive and marked it failed (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A drive was marked failed because it could not be formatted.	Use maintenance procedures to remove and then add the drive. If that doesn't fix the problem, replace the drive.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2931	Server module <i>server-module-number</i> failed to add a data drive due to an I/O error (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data drive could not be added due to an I/O error.	Use maintenance procedures to remove and then add the drive. If that doesn't fix the problem, replace the drive.	N	No
2932	Server module <i>server-module-number</i> failed to remove a drive (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A drive could not be removed.	Use a maintenance procedure to remove or replace the drive. If that doesn't fix the problem, contact your authorized service provider.	N	No
2933	Drive is unavailable on server module <i>server-module-number</i> (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data or database drive either was removed outside of a maintenance procedure or has become unavailable.	Use the HCP S Series Management Console to check the health of the drive.	N	Yes
2934	Server module <i>server-module-number</i> detected that the data drive in enclosure <i>enclosure-number</i> slot <i>slot-number</i> was moved to enclosure <i>enclosure-number</i> slot <i>slot-number</i> (enclosure: <i>enclosure-number</i> , slot: <i>slot-number</i> , serial number: <i>drive-serial-number</i> , wwid: <i>drive-wwid</i>).	A data drive was moved.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2951	Enclosure <i>enclosure-number</i> is unavailable on server module <i>server-module-number</i> (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure is unavailable.	Contact your authorized service provider.	E	Yes
2952	Enclosure <i>enclosure-number</i> is now available on server module <i>server-module-number</i> (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure that was unavailable is now available.	No action is required.	N	No
2953	Server module <i>server-module-number</i> detected a new enclosure during a maintenance procedure (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	A new enclosure was detected during a maintenance procedure.	Complete the maintenance procedure.	N	No
2954	Server module <i>server-module-number</i> added an enclosure (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was added.	No action is required.	N	No
2955	Server module <i>server-module-number</i> removed an enclosure during a maintenance procedure (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was removed.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2956	Server module <i>server-module-number</i> detected new enclosure firmware (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	New enclosure firmware was detected.	No action is required.	N	No
2957	Server module <i>server-module-number</i> marked an enclosure failed (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was marked failed.	Contact your authorized service provider.	E	No
2958	Server module <i>server-module-number</i> detected a new enclosure outside of a maintenance procedure and marked it as failed (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was added outside of a maintenance procedure and was marked failed.	Contact your authorized service provider.	E	No
2959	Server module <i>server-module-number</i> detected an incorrect enclosure WWID and marked the enclosure failed (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was marked failed due to an incorrect WWID.	Contact your authorized service provider.	E	No

ID	Message	Explanation	Action	Sev.	Alert
2960	Server module <i>server-module-number</i> detected an incorrect enclosure serial number and marked the enclosure failed (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was marked failed due to an incorrect serial number.	Contact your authorized service provider.	E	No
2961	Server module <i>server-module-number</i> detected that an enclosure is unavailable and marked it failed (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was marked failed because it is unavailable.	Contact your authorized service provider.	E	No
2962	Enclosure <i>enclosure-number</i> failed (serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was marked failed.	Contact your authorized service provider.	E	Yes
2963	Enclosure <i>enclosure-number</i> is unavailable (serial number: <i>enclosure-serial number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure is unavailable.	Contact your authorized service provider.	E	Yes
2964	Server module <i>server-module-number</i> enclosure initialization is complete (available: <i>total-number-of-enclosures-processed</i> , failed: <i>number-of-failed-enclosures</i> , unavailable: <i>number-of-unavailable-enclosures</i> , discovered: <i>number-of-enclosures-discovered</i>).	Server module enclosure initialization is complete.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2967	Enclosure <i>enclosure-number</i> is unavailable on server module <i>server-module-number</i> (enclosure: <i>enclosure-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure is unavailable.	Contact your authorized service provider.	N	Yes
2968	Enclosure <i>enclosure-number</i> is unavailable (serial number: <i>enclosure-serial number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure is unavailable.	Contact your authorized service provider.	N	Yes
2969	Enclosure <i>enclosure-number</i> failed (serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was marked failed.	Contact your authorized service provider.	N	Yes
2970	Enclosure <i>enclosure-number</i> failed (FRU part number: <i>part-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was marked failed.	Contact your authorized service provider.	E	Yes
2971	Enclosure <i>enclosure-number</i> failed (FRU part number: <i>part-number</i> , serial number: <i>enclosure-serial-number</i> , wwid: <i>enclosure-wwid</i>).	An enclosure was marked failed.	Contact your authorized service provider.	N	Yes
2980	Server module <i>server-module-number</i> SAS port <i>sas-port-number</i> is connected to enclosure <i>enclosure-number</i> I/O module <i>iom-number</i> port <i>sas-port-number</i> but should be connected to enclosure <i>enclosure-number</i> I/O module <i>iom-number</i> port <i>port-number</i> .	A server module SAS port is connected to an incorrect I/O module port.	Contact your authorized service provider.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2981	Server module <i>server-module-number</i> SAS port <i>sas-port-number</i> is no longer connected to an incorrect enclosure I/O module port.	A server module SAS port is no longer connected to an incorrect enclosure I/O module port.	No action is required.	N	No
2982	Server module <i>server-module-number</i> SAS port <i>sas-port-number</i> should be connected to enclosure <i>enclosure-number</i> I/O module <i>iom-number</i> port <i>sas-port-number</i> but is not.	A server module SAS port is not connected to an enclosure I/O module port but should be.	Contact your authorized service provider.	E	Yes
2983	Server module <i>server-module-number</i> SAS port <i>sas-port-number</i> connection is no longer missing.	A server module SAS port connection is no longer missing.	No action is required.	N	No
2984	Server module <i>server-module-number</i> SAS port <i>sas-port-number</i> is connected to enclosure <i>enclosure-number</i> I/O module <i>iom-number</i> port <i>sas-port-number</i> but should not be.	A server module SAS port is unexpectedly connected to an I/O module port.	Contact your authorized service provider.	E	Yes
2985	Server module <i>server-module-number</i> SAS port <i>sas-port-number</i> no longer has an unexpected connection to an enclosure I/O module port.	A server module SAS port no longer has an unexpected connection to an enclosure I/O module port.	No action is required.	N	No
2986	Enclosure <i>enclosure-numbersas-port-identification</i> is connected to <i>sas-port-identification</i> but should be connected to <i>sas-port-identification</i> .	An enclosure I/O module port is connected to an incorrect enclosure I/O module port.	Contact your authorized service provider.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
2987	Enclosure <i>enclosure-number sas-port-identification</i> is no longer connected to an incorrect SAS port.	An I/O module port is no longer connected to an incorrect SAS port.	No action is required.	N	No
2988	Enclosure <i>enclosure-number sas-port-identification</i> should be connected to <i>sas-port-identification</i> but is not.	An I/O module port is not connected to a SAS port but should be.	Contact your authorized service provider.	E	Yes
2989	Enclosure <i>enclosure-number sas-port-identification</i> connection is no longer missing.	An I/O module port connection is no longer missing.	No action is required.	N	No
2990	Enclosure <i>enclosure-number sas-port-identification</i> is connected to <i>sas-port-identification</i> but should not be.	An I/O module port is unexpectedly connected to a SAS port.	Contact your authorized service provider.	E	Yes
2991	Enclosure <i>enclosure-number sas-port-identification</i> is no longer connected to a SAS port.	An I/O module port is no longer connected to a SAS port.	No action is required.	N	No
2992	Enclosure 1 rear SAS port <i>port-number</i> is connected to enclosure <i>enclosure-number</i> I/O module <i>iom-number</i> port <i>sas-port-number</i> but should be connected to enclosure <i>enclosure-number</i> I/O module <i>iom-number</i> port <i>sas-port-number</i> .	A rear SAS port is connected to an incorrect I/O module port.	Contact your authorized service provider.	E	Yes
2993	Enclosure 1 rear SAS port <i>sas-port-number</i> is no longer connected to an incorrect I/O module port.	A rear SAS port is no longer connected to an incorrect I/O module port.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
2994	Enclosure 1 rear SAS port <i>sas-port-number</i> should be connected to enclosure <i>enclosure-number</i> I/O module <i>iom-number</i> port <i>sas-port-number</i> but is not.	A rear SAS port is not connected to an I/O module port but should be.	Contact your authorized service provider.	E	Yes
2995	Enclosure 1 rear SAS port <i>sas-port-number</i> is now connected to an I/O module port.	A rear SAS port is now connected to an I/O module port.	No action is required.	N	No
2996	Enclosure 1 rear SAS port <i>sas-port-number</i> is connected to enclosure <i>enclosure-number</i> I/O module <i>iom-number</i> port <i>sas-port-number</i> but should not be.	A rear SAS port is unexpectedly connected to an I/O module port.	Contact your authorized service provider.	E	Yes
2997	Enclosure 1 rear SAS port <i>sas-port-number</i> is no longer connected to an I/O module port.	A rear SAS port is no longer connected to an I/O module port.	No action is required.	N	No
3000	The " <i>configuration-setting</i> " value changed from " <i>old-value</i> " to " <i>new-value</i> ".	A user changed a configuration value.	No action is required.	N	No
3001	The " <i>configuration-setting</i> " value changed from " <i>old-value</i> " to " <i>new-value</i> ".	A user changed a configuration value.	No action is required.	N	No
3004	A user account was created with username <i>username</i> , enabled <i>true/false</i> .	A user created a user account.	No action is required.	N	No
3005	The user account with username <i>username</i> and user ID <i>user-account-id</i> was deleted.	A user deleted a user account.	No action is required.	N	No
3006	Bucket <i>bucket-name</i> was created with bucket owner <i>username</i> .	A user created a bucket.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
3007	Bucket <i>bucket-name</i> with bucket owner <i>username</i> was deleted.	A user deleted a bucket.	No action is required.	N	No
3008	The user account with username <i>username</i> was updated: <i>configuration setting</i> changed from " <i>old-value</i> " to " <i>new-value</i> ".	A user updated a user account.	No action is required.	N	No
3009	New access keys were generated for the user account with username {0}.	A user generated new access keys.	No action is required.	N	No
3010	The minimum TLS version has been changed from ' <i>old-tls-setting</i> ' to ' <i>new-tls-setting</i> '.	A user changed the minimum TLS version.	No action is required.	N	No
3015	The exclusive SSH keys in the SSH key package with ID <i>key-package-id</i> have been installed on the HCP S Series Node and are now active.	A user uploaded an SSH key package, and the SSH keys in the package were successfully installed on the HCP S Series Node.	No action is required.	N	No
3017	Exclusive SSH keys have been revoked. The <i>distributor-key</i> default SSH keys are now active.	A user revoked the exclusive SSH keys that were installed on the HCP S Series Node.	No action is required.	W	No
3018	An attempt to install the exclusive SSH keys in the SSH key package with ID <i>key-package-id</i> failed.	An attempt to install exclusive SSH keys failed.	Try uploading the SSH key package again. If the problem persists, contact your authorized service provider.	E	No
3019	An attempt to revoke exclusive SSH keys failed.	An attempt to revoke exclusive SSH keys failed.	Try revoking the exclusive SSH keys again. If the problem persists, contact your authorized service provider.	E	No

ID	Message	Explanation	Action	Sev.	Alert
3131	The HCP S Series Node was shut down; reason: <i>reason</i>	A user shut down the HCP S Series Node.	No action is required.	N	No
3132	The HCP S Series Node was restarted; reason: <i>reason</i>	A user restarted the HCP S Series Node.	No action is required.	N	No
3133	Server module <i>server-module-number</i> was shut down; reason: <i>reason</i>	A user shut down a server module.	No action is required.	N	No
3134	Server module <i>server-module-number</i> was restarted; reason: <i>reason</i>	A user restarted a server module.	No action is required.	N	No
3135	Server module <i>server-module-number</i> was powered on; reason: <i>reason</i>	A user powered on a server module.	No action is required.	N	No
3136	An attempt to power on the server module <i>server-module-number</i> failed (originating IP <i>ip-address</i>).	A user request to power on a server module failed.	No action is required.	E	No
3137	<i>number-of-data-drives</i> data drives have failed or are unavailable.	The data drive failed/unavailable threshold has been exceeded.	Remove or replace the drives.	W	Yes
3138	One or more data drives may be failed or unavailable, but data drive replacement is not required at this time.	The data drive failed/unavailable threshold is no longer exceeded.	No action is required.	N	No
3139	The HCP S Series Node supports a maximum of <i>max-number-of-enclosures</i> enclosures.	The HCP S Series Node has more enclosures than are supported.	Check that the correct server modules are installed in the HCP S Series Node. If the problem persists, contact your HCP support center.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
3140	The HCP S Series Node no longer has more enclosures than the supported maximum of <i>max-number-of-enclosures</i> .	The HCP S Series Node now has a supported number of enclosures.	No action is required.	N	No
3161	Internal logs were marked with search code <i>search-code</i> and message <i>message-text</i> .	A user inserted a message into the HCP S Series Node internal logs.	No action is required.	N	No
3162	A log download started.	A user has requested a download of the HCP S Series Node internal logs.	No action is required.	N	No
3163	A log download with search code <i>search-code</i> failed: <i>failure-reason</i>	A requested download of the HCP S Series Node internal logs failed.	Try to download the logs again. If that fails, contact your authorized service provider.	W	No
3164	Log download preparation with search code <i>search-code</i> started on server module <i>server-module-number</i> .	The HCP S Series Node has started preparing the internal logs for download on an individual server module.	No action is required.	N	No
3165	Log download preparation with search code <i>search-code</i> successfully finished on server module <i>server-module-number</i> .	The HCP S Series Node has finished preparing the internal logs for download on an individual server module.	No action is required.	N	No
3166	Log download preparation with search code <i>search-code</i> failed on server module <i>server-module-number</i> . Continuing with next server module.	The HCP S Series Node failed to prepare the internal logs for download on an individual server module and is continuing with the next server module.	No action is required.	W	No
3167	Log download final preparation has started.	The HCP S Series Node has started the final preparation of the internal logs for download.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
3168	Log download final preparation is complete.	Log download final preparation is complete, and the HCP S Series Node internal logs are ready to be downloaded.	No action is required.	N	No
3169	Log download to client has started.	The HCP S Series Node internal logs have begun streaming to an HTTP client.	No action is required.	N	No
3170	Log download is complete.	The HCP S Series Node internal logs have been downloaded.	No action is required.	N	No
4000	The internal database is not being replicated.	The internal database on one server module cannot connect to the internal database on the other server module.	Check the S Series Node network configuration.	E	Yes
4001	The internal database is being replicated.	The internal database is being replicated from one server module to the other.	No action is required.	N	No
4002	The HCP S Series Node failed to back up the internal database.	The HCP S Series Node failed to back up the internal database.	If this happens repeatedly, contact your authorized service provider.	E	No
5000	Storage is <i>percent-full%</i> full.	Storage is almost full.	Add more capacity or free up space.	W	Yes
5001	Storage is <i>percent-full%</i> full.	Storage is full.	Add more capacity or free up space.	E	Yes
5002	Irreparable objects have been detected.	Too many data drives are unavailable or failed.	Contact your authorized service provider.	E	Yes
5003	Objects may be unavailable due to insufficient recovery sources.	Too many data drives are unavailable or failed.	Check the hardware status and correct any issues. If the problem persists, contact your authorized service provider.	E	No

ID	Message	Explanation	Action	Sev.	Alert
5004	Data cannot be fully protected due to not enough drives or insufficient free space.	Not enough drives or free space is available to perform repairs.	Replace failed drives, add more capacity, or free up space.	E	No
5005	The internal database update is complete.	The internal database update finished.	No action is required.	N	No
5006	The internal database update has encountered an error.	The internal database update process encountered an error.	Contact your authorized service provider.	E	No
5007	Cannot perform metadata operations due to insufficient free space. Data access has been disabled.	Not enough free space is available to perform metadata operations. Data access has been disabled.	Contact your authorized service provider.	E	Yes
5008	Storage is <i>percent-full%</i> full.	Storage is almost full.	Add more capacity or free up space.	W	Yes
5211	The SSL server certificate has been replaced.	A user generated a new SSL server certificate for the HCP S Series Node.	No action is required.	N	No
5212	An attempt to replace the SSL server certificate failed.	A failure occurred during an attempt to replace the SSL server certificate on the HCP S Series Node.	Contact your authorized service provider.	E	No
5213	SSL server certificate <i>distinguished-name</i> expires on <i>expiration-date</i> .	The SSL server certificate for this HCP S Series Node expires soon. If the certificate expires, clients will need to accept the expired certificate in order to use HTTPS for access to the HCP S Series Node.	Install a new SSL server certificate with a later expiration date.	W	Yes
5214	SSL server certificate <i>distinguished-name</i> expired on <i>expiration-date</i> .	The SSL server certificate for this HCP S Series Node has expired. Clients must accept the expired certificate in order to use HTTPS for access to the HCP S Series Node.	Install a new SSL server certificate with a later expiration date.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
5215	A new CSR has been generated.	A user generated a new CSR for the HCP S Series Node.	No action is required.	N	No
5300	The HCP S Series Node is being updated to <i>software-release-number</i> .	A user has started an HCP S Series Node update.	No action is required.	N	No
5301	The HCP S Series Node has been updated to <i>software-release-number</i> .	The HCP S Series Node has been successfully updated.	No action is required.	N	No
5302	An unexpected error occurred during an update of the HCP S Series Node.	An unexpected error occurred during an update of the HCP S Series Node.	Contact your authorized service provider.	E	No
5350	A new license has been applied to the HCP S Series Node.	A user applied a new license to the HCP S Series Node.	No action is required.	N	No
5500	Server module <i>server-module-number</i> has been changed.	A user removed, reinserted, or replaced a server module.	Verify that this is an expected event.	E	No
5501	Enclosure <i>enclosure-number iom-number</i> hardware is unsupported (vendor: <i>iom-vendor</i> , product: <i>iom-model</i> , rev: <i>iom-firmware-revision</i> , wwid: <i>iom-wwid</i>).	I/O module hardware is unsupported.	Contact your authorized service provider.	E	Yes
5502	Enclosure <i>enclosure-number iom-number</i> hardware is now supported (vendor: <i>iom-vendor</i> , product: <i>iom-model</i> , rev: <i>iom-firmware-revision</i> , wwid: <i>iom-wwid</i>).	I/O module hardware is now supported.	No action is required.	N	No
5503	Enclosure <i>enclosure-number</i> is marked failed.	An enclosure has been marked failed.	Check that the enclosure is operating properly. If it isn't, replace the enclosure.	N	No

ID	Message	Explanation	Action	Sev.	Alert
5504	Enclosure <i>enclosure-number</i> SAS expanders have different firmware versions.	The SAS expander firmware is in the process of being upgraded.	No action is required.	N	Yes
5505	Enclosure <i>enclosure-number</i> expander <i>sas-expander-number</i> hardware is unsupported (vendor: <i>vendor-name</i> , FRU part number: <i>part-number</i> , product: <i>product-name</i> , rev: <i>firmware-revision</i> , SAS address: <i>sas-address</i>).	An enclosure contains unsupported SAS expander hardware.	Contact your authorized service provider.	E	Yes
5506	Enclosure <i>enclosure-number</i> expander <i>sas-expander-number</i> hardware is now supported (vendor: <i>vendor-name</i> , FRU part number: <i>part-number</i> , product: <i>product-name</i> , rev: <i>firmware-revision</i> , SAS address: <i>sas-address</i>).	An enclosure now contains supported SAS expander hardware.	No action is required.	N	No
5507	The <i>bay-type</i> cover for enclosure <i>enclosure-number</i> has been opened outside of a maintenance procedure.	An enclosure cover is open outside of a maintenance procedure.	Close the enclosure cover.	E	Yes
5508	The <i>bay-type</i> cover for enclosure <i>enclosure-number</i> has been opened during a maintenance procedure.	An enclosure cover is open during a maintenance procedure.	No action is required.	N	No
5509	The <i>bay-type</i> cover for enclosure <i>enclosure-number</i> has been closed.	An enclosure cover was closed.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
5510	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> hardware is unsupported (vendor: <i>vendor-name</i> , product: <i>product-name</i> , fwRev: <i>firmware-revision</i> , wwid: <i>power-supply-wwid</i>).	An enclosure contains an unsupported power supply.	Contact your authorized service provider.	E	Yes
5511	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> hardware is now supported (vendor: <i>vendor-name</i> , product: <i>product-name</i> , fwRev: <i>firmware-revision</i> , wwid: <i>power-supply-wwid</i>).	An enclosure now contains a supported power supply.	No action is required.	N	No
5512	Enclosure <i>enclosure-number</i> fan <i>fan-number</i> hardware is unsupported (vendor: <i>vendor-name</i> , part number : <i>part-number</i> , wwid: <i>fan-wwid</i>).	An enclosure contains an unsupported fan.	Contact your authorized service provider.	E	Yes
5513	Enclosure <i>enclosure-number</i> fan <i>fan-number</i> hardware is now supported (vendor: <i>vendor-name</i> , part number : <i>part-number</i> , wwid: <i>fan-wwid</i>).	An enclosure now contains a supported fan.	No action is required.	N	No
5514	Enclosure <i>enclosure-number</i> <i>power-supply-number</i> has been marked failed.	A power supply has been marked failed.	Check that the power supply is operating normally. If it isn't, replace the power supply.	E	Yes
5515	Enclosure <i>enclosure-number</i> <i>power-supply-number</i> failure has been cleared.	A power supply is no longer marked failed.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
5516	Enclosure <i>enclosure-number fan-number</i> has been marked failed.	A fan has been marked failed.	Check that the fan is operating normally. If it isn't, replace the fan.	E	Yes
5517	Enclosure <i>enclosure-number fan-number</i> has been cleared.	A fan is no longer marked failed.	No action is required.	N	No
5518	Enclosure <i>enclosure-number power-supply-number</i> has detected a DC over-voltage condition.	A power supply has reported a DC over-voltage condition.	Check the power supply.	E	Yes
5519	Enclosure <i>enclosure-number power-supply-number</i> is no longer reporting a DC over-voltage condition.	A power supply is no longer reporting a DC over-voltage condition.	No action is required.	N	No
5520	Enclosure <i>enclosure-number power-supply-number</i> has detected a DC under-voltage condition.	A power supply has reported a DC under-voltage condition.	Check the power supply.	E	Yes
5521	Enclosure <i>enclosure-number power-supply-number</i> is no longer reporting a DC under-voltage condition.	A power supply is no longer reporting a DC under-voltage condition.	No action is required.	N	No
5522	Enclosure <i>enclosure-number power-supply-number</i> has detected a DC over-current condition.	A power supply has reported a DC over-current condition.	Check the power supply.	E	Yes
5523	Enclosure <i>enclosure-number power-supply-number</i> is no longer reporting a DC over-current condition.	A power supply is no longer reporting a DC over-current condition.	No action is required.	N	No

ID	Message	Explanation	Action	Sev.	Alert
5524	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> has detected an over-temperature failure condition.	A power supply has reported an over-temperature failure condition.	Check the power supply.	E	Yes
5525	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> is no longer reporting an over-temperature failure condition.	A power supply is no longer reporting an over-temperature failure condition.	No action is required.	N	No
5526	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> has detected an over-temperature warning condition.	A power supply has reported an over-temperature warning condition.	Check the power supply.	W	Yes
5527	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> is no longer reporting an over-temperature warning condition.	A power supply is no longer reporting an over-temperature warning condition.	No action is required.	N	No
5528	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> has detected an AC power failure.	A power supply has reported an AC power failure.	Check the power supply.	E	Yes
5529	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> is no longer reporting an AC power failure.	A power supply is no longer reporting an AC power failure.	No action is required.	N	No
5530	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> has detected a DC power failure.	A power supply has reported a DC power failure.	Check the power supply.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
5531	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> is no longer reporting a DC power failure.	A power supply is no longer reporting a DC power failure.	No action is required.	N	No
5532	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> is powered off.	A power supply is powered off.	Check the power supply.	E	Yes
5533	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> was powered on.	A power supply was powered on.	No action is required.	N	No
5534	Enclosure <i>enclosure-number</i> fan- <i>fan-number</i> is off.	A fan is off.	Check the fan.	E	Yes
5535	Enclosure <i>enclosure-number</i> fan- <i>fan-number</i> is on.	A fan that was off is now on.	No action is required.	N	No
5536	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> is not compatible with the other power supply in the enclosure and needs to be replaced.	The power supplies in an enclosure are not compatible with each other.	Contact your authorized server provider.	E	Yes
5537	Enclosure <i>enclosure-number</i> power supply <i>power-supply-number</i> has been replaced.	The power supplies in an enclosure are now compatible with each other.	No action is required.	N	No
5600	An OS SSD in server module <i>server-module-number</i> is <i>percent-worn</i> % worn (serial number: <i>ssd-serial-number</i> , wwid: <i>ssd-wwid</i>).	An OS SSD is close to the end of its expected life span.	Contact your authorized service provider.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
5700	<i>maintenance-procedure-type</i> maintenance procedure is still active and will time out in <i>number-of-minutes</i> minute(s).	A maintenance procedure is still active.	Complete or cancel the active maintenance procedure.	N	No
5800	Internal status files (<i>file-list</i>) on server module <i>server-module-number</i> are not up to date. The oldest update time is <i>date-time</i> .	One or more internal status files are out of date.	Contact your authorized service provider.	E	Yes
5801	Internal status files (<i>file-list</i>) on server module <i>server-module-number</i> are not up to date. The oldest update time is <i>date-time</i> .	One or more internal status files are out of date.	No action is required.	W	No
5900	Server module <i>server-module-number</i> network interface <i>device-name</i> card is unsupported (vendor: <i>vendor-name</i> , product: <i>product-name</i>).	A server module network interface card is unsupported.	Contact your authorized service provider.	E	Yes
5901	Server module <i>server-module-number</i> network interface <i>device-name</i> card is now supported (vendor: <i>vendor-name</i> , product: <i>product-name</i>).	A server module network interface card is now supported.	No action is required.	N	No
5902	Server module <i>server-module-number</i> SAS card <i>sas-card-number</i> is unsupported (vendor: <i>vendor-name</i> , product: <i>product-name</i> , rev: <i>revision</i>).	A server module SAS card is unsupported.	Contact your authorized service provider.	E	Yes

ID	Message	Explanation	Action	Sev.	Alert
5903	Server module <i>server-module-number</i> SAS card <i>sas-card-number</i> is now supported (vendor: <i>vendor-name</i> , product: <i>product-name</i> , rev: <i>revision</i>).	A server module SAS card is now supported.	No action is required.	N	No
5904	Server module <i>server-module-number</i> is missing a virtual IP address.	A server module is missing a virtual IP address. A virtual IP address must be specified for each physical IP address for a server module.	Specify the missing virtual IP address for the server module.	W	Yes
5905	Server module <i>server-module-number</i> is no longer missing a virtual IP address.	A server module is no longer missing a virtual IP address.	No action is required	N	No
5906	Server module <i>server-module-number</i> memory card <i>memory-card-id</i> has detected an error condition.	A server-module memory card is reporting an error.	Contact your authorized service provider.	E	Yes
5907	Server module <i>server-module-number</i> memory card <i>memory-card-id</i> is no longer reporting an error condition.	A server-module memory card is no longer reporting an error condition.	No action is required.	N	No
5908	Server module {0} access network interface card (vendor: <i>network-interface-card-vendor</i> , product: <i>network-interface-card-model</i>) does not match the corresponding card on server module <i>server-module-number</i> (vendor: <i>server-module-vendor</i> , product: <i>server-module-model</i>).	The server module access network interface cards do not match.	Replace the access network interface card in one of the server modules.	W	Yes

ID	Message	Explanation	Action	Sev.	Alert
5909	Server module {0} access network interface card (vendor: <i>network-interface-card-vendor</i> , product: <i>network-interface-card-model</i>) matches the corresponding card on server module <i>server-module-number</i> .	The server module access network interface cards match.	No action is required.	N	No
10043	The HCP S Series Node update to <i>software-release-number</i> has been restarted.	A user restarted an update of the HCP S Series Node.	No action is required.	N	No
10044	<i>precheck-failure</i>	The HCP S Series Node could not be updated due to a precheck failure.	Contact your authorized service provider.	E	No
99999	An unknown event occurred: <i>event-id</i>	The HCP S Series Node could not find an event message.	Wait for the update to finish. Then check the event log for the specified message ID. If the event message indicates a persistent error condition, contact your HCP support center.	W	No

Chapter 10: Supported limits

HCP S Series Nodes support the maximum values listed in the table below.

Item	Limit
Maximum number of objects per S Series Node	Limited only by available capacity and object size
Maximum object size	10 TB
Maximum file size per PUT request (larger file sizes require multipart write)	10 GB
Maximum parts per multipart write	10,000
Maximum number of users	10,000
Maximum number of buckets	10,000
Maximum number of buckets per owner	100
Maximum number of concurrent connections to the HCP S Series Management Console	25 per server module
Maximum number of concurrent connections through the management API	50 per server module
Maximum number of concurrent connections through the Hitachi API for Amazon S3 (the S3 compatible API)	500 per server module

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA



HitachiVantara.com/contact