

Hitachi Content Platform

v10.0

Installing an HCP with Internal Storage System - Onsite Setup Guide

This book is for customer-site personnel responsible for setting up an HCP system with internal storage (RAIN). It assumes familiarity with computer hardware and a basic understanding of HCP systems.

© 2007, 2025 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., Hitachi Vantara, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

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

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

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

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

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

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

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

AIX, DB2, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, IntelliMagic, IntelliMagic Vision, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z17, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

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

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

The open source content used in Hitachi Vantara products may be found within the Product documentation or you may request a copy of such information (including source code and/or modifications to the extent the license for any open source requires Hitachi make it available) by sending an email to OSS_licensing@hitachivantara.com.

Contents

Preface.....	6
Intended audience.....	6
Product version.....	6
Release notes.....	6
Document conventions.....	6
Related documents.....	8
Accessing product documentation.....	9
Getting help.....	9
Comments.....	10
Chapter 1: HCP with internal storage system overview.....	11
Introduction to Hitachi Content Platform.....	11
HCP with internal storage system hardware.....	12
Final onsite setup activities.....	14
Chapter 2: Site preparation.....	15
Server specifications.....	15
Mechanical details.....	16
Dimensions.....	17
Weight.....	18
Hitachi Universal V3 Rack.....	19
Customer-supplied rack.....	20
Electrical requirements.....	21
Power system.....	21
PDU for the Hitachi Universal V3 Rack.....	22
Power connections.....	22
Electrical specifications.....	24
RoHS compliance.....	25
BNST compliance.....	25
Temperature, humidity, and altitude.....	25
Shock and vibration.....	26
Cooling and airflow.....	27
Required tools and supplies.....	28

Chapter 3: Mounting unracked components.....	29
Components that come with a rackless system.....	29
Hardware assembly procedure.....	30
Considerations for HCP racking and PDU connections.....	30
Considerations for racking an HCP O12 system.....	30
PDUs for the Hitachi Universal V3 Rack.....	31
Considerations for connecting PDUs.....	32
HCP racking and connection diagram.....	32
Considerations for racking nodes.....	42
Power cords.....	43
Rackless assembly recommendation.....	43
Tools and accessories you need.....	43
Prepare the racks.....	43
Install the PDUs.....	43
(Optional) Rack the HCP S32 Nodes.....	43
Rack the HCP S32 Nodes.....	43
Connect the HCP S32 Nodes to the PDUs.....	44
Rack the HCP O12 Nodes.....	44
Separate the inner and outer server rails.....	44
Attach the inner rails to the server.....	46
Install the outer server rails in the rack.....	46
Mount the server in the rack.....	47
Attach the HCP O12 service tag.....	48
Connect the HCP O12 Nodes to the PDUs.....	49
Install front-end connectivity options.....	49
Rack the Ethernet switches.....	49
HCP O12 Node 1G and 10G port diagrams.....	49
(Optional) Install the blanking plates.....	50
Reassemble the racks.....	50
Chapter 4: Connecting the HCP system at your site.....	51
Connecting to the power sources.....	51
Connecting to your corporate network.....	52
Chapter 5: Reconfiguring the HCP system for your site.....	53
Preparing to reconfigure the system.....	53
Connect to the HCP default back-end network.....	54
Log in with the initial user account.....	54
Check the health of the HCP system.....	55
Create a service account.....	55
Log in with the service account.....	56

Verify the serial number.....	56
Changing the network settings.....	57
Changing the front-end network settings.....	58
Changing the back-end network settings.....	59
Changing the back-end IP addresses.....	59
Changing DNS settings.....	59
Changing time settings.....	60
Making the back-end switches known to HCP.....	61
Using SSH to access an HCP node.....	62
Uploading exclusive support access credentials.....	62
BMC administrative credentials.....	63
Configuring the BMC to monitor servers.....	63
Chapter 6: Configuring HCP monitoring with Hitachi Remote Ops.....	64
Enabling SNMP in HCP.....	64
Configuring Hitachi Remote Ops.....	65
Step 1: Log in to Hitachi Remote Ops.....	65
Set the base configuration.....	66
Configure transport agents.....	67
Step 4: Identify the HCP system.....	67
Chapter 7: Configuring DNS for HCP.....	69
DNS advantages.....	70
Zones.....	70
Secondary zones and stub zones.....	71
Configuring an HCP secondary zone or stub zone in Windows.....	72
Configuring an HCP secondary zone in Windows.....	72
Configuring an HCP stub zone in Windows.....	73
Configuring an HCP secondary zone or stub zone in Unix.....	74
Verifying the configuration.....	74
DNS considerations for service by remote systems.....	75

Preface

This guide provides the information needed to deploy an assembled and configured HCP with internal storage (RAIN) system at your site. It includes instructions for assembling components that were ordered without a rack and explains how to configure Hitachi Remote Ops to monitor the nodes in the HCP system.



Note: The information in this book is applicable to the HCP O12 server. For information about the HCP G11 server, see version 9.7 of this book. For information about the HCP G10 server, see version 8.2 of this book.

Intended audience

This book is for customer-site personnel responsible for setting up an HCP system with internal storage (RAIN). It assumes familiarity with computer hardware and a basic understanding of HCP systems.

Product version

This book applies to release 10.0 or later of Hitachi Content Platform.

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 documentation website: <https://docs.hitachivantara.com>.

Document conventions

This document uses the following typographic conventions:

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>
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code>
< > angle brackets	Indicates variables in the following scenarios: <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	Indicates that you have a choice between two or more options or arguments. Examples: [a b] indicates that you can choose a, b, or nothing. { a b } indicates that you must choose either a or b.
-file-spec	Replace with the combination of the directory path and name of a file. This book shows: <i>source-filespec</i> You enter: <code>/opt/arc/build.version</code>
-path	Replace with a directory path with no file or object name This book shows: <i>destination-path</i> You enter: <code>/opt/arc/tools/cluster/temp</code>

This document uses the following icons to draw attention to information:

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

Related documents

The following documents contain additional information about Hitachi Content Platform:

- *HCP System Management Help*

This Help system is a comprehensive guide to administering and using an HCP system. The Help contains complete instructions for configuring, managing, and maintaining HCP system-level and tenant-level features and functionality. The Help also describes the properties of objects stored in HCP namespaces and explains how to access those objects.

- *HCP Tenant Management Help*

This Help system contains complete instructions for configuring, managing, and maintaining HCP namespaces. The Help also describes the properties of objects stored in HCP namespaces and explains how to access those objects.

- *Managing the Default Tenant and Namespace*

This book contains complete information for managing the default tenant and namespace in an HCP system. The book provides instructions for changing tenant and namespace settings, configuring the protocols that allow access to the namespace, and managing search and indexing. The book also explains how to work with retention classes and the privileged delete functionality.

- *Using the Default Namespace*

This book describes the file system HCP uses to present the contents of the default namespace. This book provides instructions for using HCP-supported protocols to store, retrieve, and delete objects, as well as change object metadata such as retention and shred settings.

- *Deploying an HCP VM System on ESXi*

This book contains all the information you need to install and configure an HCP VM system. The book also includes requirements and guidelines for configuring the VMWare® environment in which the system is installed.

- *Installing HCP Evaluation Edition* — This book contains instructions for setting up a virtual HCP system for product evaluation purposes.

- *Installing an HCP SAN-attached Storage System - Onsite Setup Guide* — This book contains instructions for deploying an assembled and configured single-rack HCP with SAN-attached storage (SAIN) system at a customer site. It explains how to make the necessary physical connections and reconfigure the system for the customer computing environment. It also contains instructions for configuring Hitachi Remote Ops to monitor the nodes in an HCP system.

- *Installing an HCP with Internal Storage System - Onsite Setup Guide* — This book contains instructions for deploying an assembled and configured HCP with internal storage (RAIN) system at a customer site. It explains how to make the necessary physical connections and reconfigure the system for the customer computing environment. The book also provides instructions for assembling the components of an HCP with internal storage system that was ordered without a rack and for configuring Hitachi Remote Ops to monitor the nodes in an HCP system.

Accessing product documentation

Product user documentation is available on: <https://docs.hitachivantara.com>. 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](https://support.hitachivantara.com) 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 additional contact methods, go to <https://support.hitachivantara.com/en/contact-support.html>.

[Hitachi Vantara Community](https://community.hitachivantara.com) 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.feedback@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 with internal storage system overview

Hitachi Content Platform (HCP) is the distributed, fixed-content, data storage system from Hitachi Vantara. An HCP system consists of both hardware and software.

An HCP with internal storage system is delivered to a customer site as either a racked appliance or unracked components. In either case, all the components are preconfigured, and the HCP software is already installed. However, once the system is delivered and, for unracked components, assembled, it needs some final onsite setup.

This chapter contains:

- An introduction to HCP
- A description of the hardware architecture of HCP with internal storage systems
- An overview of the final setup activities required to make your HCP with internal storage system operational at your site



Note: In this book, a system that is delivered in a rack is referred to as *preassembled system*. A system that is delivered without a rack is referred to as a *rackless system*, even though, when assembled, it includes a rack.

Introduction to Hitachi Content Platform

HCP is a combination of hardware and software that provides an object-based data storage environment. An HCP repository stores all types of data, from simple text files to medical images to multi-gigabyte database images.

HCP provides easy access to the repository for adding, retrieving, and, when allowed, deleting the stored data. HCP uses write-once, read-many (WORM) storage technology and a variety of policies and internal processes to ensure the integrity of the stored data and the efficient use of storage capacity.

HCP nodes

An HCP system includes multiple servers, called *nodes*, that are networked together. Nodes are the essential part of an HCP system. They manage the data that resides in the system storage.

Each node runs the complete HCP software. HCP runtime operations are distributed among the nodes. If a node fails, the system adapts by redirecting processing to other nodes.

HCP with internal storage and HCP with SAN-attached storage systems

Hitachi Vantara offers three HCP products: HCP with internal storage, HCP with SAN-attached storage, and HCP VM:

- HCP with internal storage systems run on a redundant array of independent nodes and use storage that is internal to those nodes.
- HCP with SAN-attached storage systems run on a SAN-attached array of independent nodes and use storage in Fibre Channel SAN arrays.

To optimize performance for certain usage patterns, nodes in an HCP with SAN-attached storage system can have internal storage in addition to being connected to SAN storage.

- HCP VM systems run on virtual machines in a VMware[®] environment.

HCP with SAN-attached storage systems support larger repositories than HCP with internal storage systems.

HCP System Management Console

HCP includes a web application called the System Management Console. Your HCP system administrator uses this Console to configure, monitor, and manage the system. The Console reports certain hardware problems as they occur, so the system administrator can take appropriate action to initiate repairs.

HCP with internal storage system hardware

HCP with internal storage system hardware consists of:

- Nodes with internal storage (a typical starter system has four nodes). The nodes are numbered from 101 through 104 for a four-node system. The node numbers increase by one for each additional node.

The nodes in an HCP with internal storage system are HCP O12 servers.

- HCP S Series nodes. The possible node models is S32.
- Ethernet switches and cables for networking. The switches in an HCP with internal storage can be for one, 10 and 25 gigabyte back-end network configurations. The possible switch models are:
 - Supported 1 Gbps Ethernet Switch: Cisco Catalyst 1200
 - Supported 25 Gbps switch: Cisco Nexus 93180YC-FX3
 - Additional infrastructure items such as a rack and Power Distribution Units (PDUs).

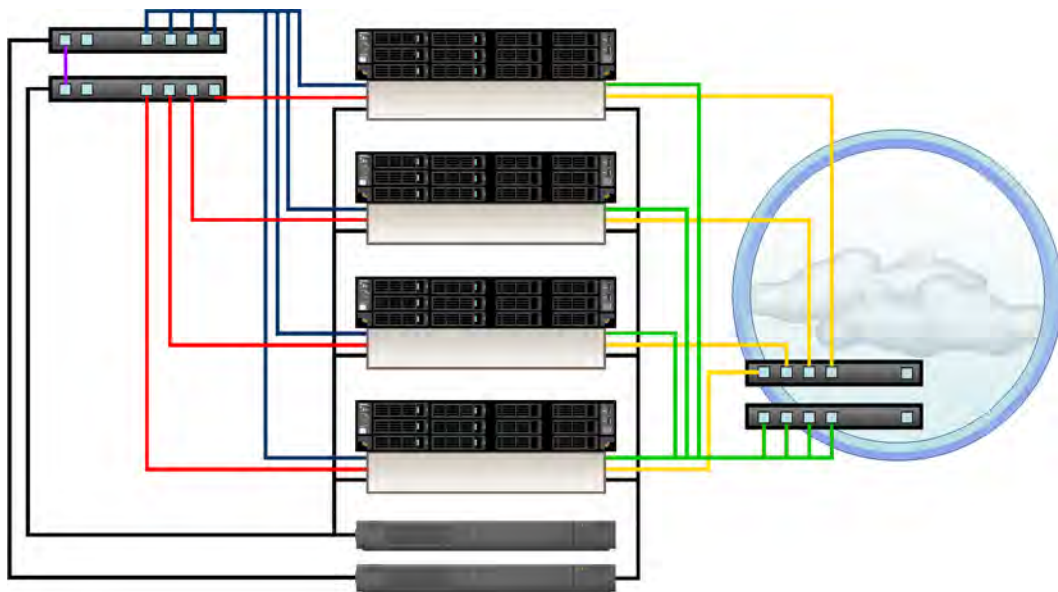
An HCP O12 system uses a back-end network, front-end network, and, in certain configurations, a management network. The isolated back-end network connects the HCP O12 nodes to each other through one or two Ethernet switches, depending on your network configuration and switch model. Each node has a pair of bonded Ethernet ports for connecting to these switches. Node port locations vary, depending on the network configuration the node was constructed for.

Each node is configured with an additional pair of bonded Ethernet ports that allows external applications to access the system. The recommended setup includes either two independent Ethernet switches that connect these ports to the front-end network (that is, your corporate network) or one Ethernet switch with both HCP O12 and the switch configured for active-active bonding.

The front-end network switches and the cables for connecting them to the HCP O12 nodes are not included with the delivered HCP with internal storage system. The cables are customer supplied. You can use any reasonable Ethernet switch model for the front-end network, but you cannot use the back-end switches for the front-end network.

Each node also has an additional management network Ethernet port that allows for the creation of the management network. The management network segregates system and tenant administration, management API, SNMP, syslog, outgoing SMTP, and SSH traffic from the [hcp_system] network.

The following figure shows the standard architecture of an HCP with internal storage system. This system has four nodes, two back-end switches (on the left), and two front-end switches (on the right).



The following table describes the cables in this figure.

Cable	Connects from	Connects to
Red and blue Ethernet	Back-end network interface cards (NICs) in each node	Back-end switches
Green and yellow Ethernet	Front-end NICs in each node	Front-end switches
Purple Ethernet	Back-end switches	Each other
Black power	Each node	Two PDUs
	Each Back-end switch	One PDU

Final onsite setup activities

An HCP with internal storage system arrives with the HCP software already installed and configured with various default settings.

To get the system up and running, you perform the activities outlined in the list below.

1. Verify that your site is ready for the HCP system to be installed.
2. Unpack and assemble.
 - For a preassembled system, remove the racked HCP system from the packing crate and position it in your data center.
 - For a rackless system, assemble the HCP system components in a rack that you supply.
3. Connect the HCP PDUs to your power sources.
4. Reconfigure the HCP system for your environment.
5. Connect the HCP system to your corporate network.



Note: If the preconfigured front-end IP addresses do not work for your environment, perform step 6 below before performing this step.

6. Configure the HCP system as a subdomain in the DNS. Be sure to use your site-specific node IP addresses and not the default IP addresses the system arrives with.

If you don't use DNS at your site, skip this step.

7. (Optional) Configure Hitachi Remote Ops to monitor the HCP nodes.

Chapter 2: Site preparation

Before an HCP with internal storage system can be deployed, you need to ensure that the intended location for the system meets certain environmental requirements. If the location does not already meet these requirements, you should wait to deploy the system until the necessary changes have been made.

You also need to have on hand the additional components that enable you to complete the connections between the HCP system and your environment.

This chapter describes the conditions and components required for the successful installation and operation of an HCP with internal storage system.

Server specifications

An HCP with internal storage node consists of the following components:

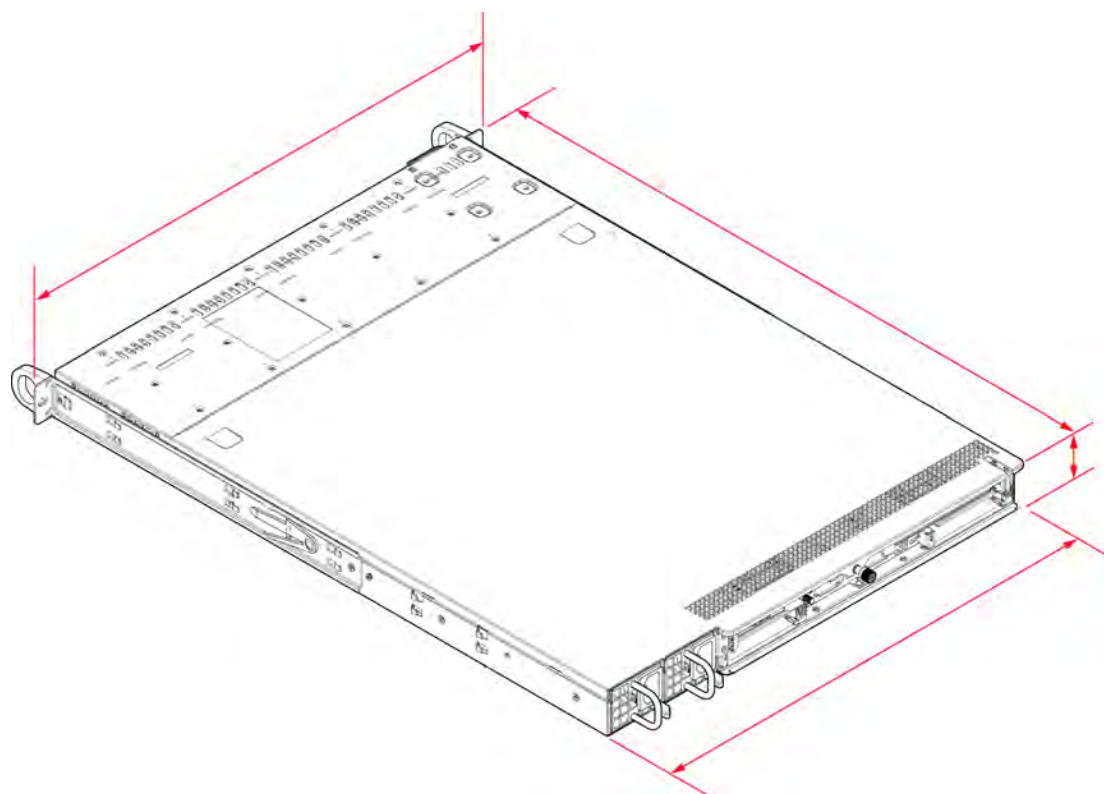
Component	Description
Processor	Genoa 9554P UP 64C/128T 3.1G 256M 360W SP5
Memory	64GB DDR5-4800 2Rx4 LP (16Gb) ECC RDIMM
1.92TB SSD	Samsung PM9A3 1.92TB NVMe PCIe4x4 M.2 22x110mm 1DWPD SED 5YR
SAS controller and RAID card	AOC with SAS3916 controller (U3) and 240PD RAID key(U39)
3.84TB SSD	SamsungPM893 3.84TB SATA 6Gb/s V6 2.5" 7mm 1DWPD 5YR SED
25GbE networking	AIOM dual-port 25GbE SFP28 based on Mellanox CX-4 Lx EN
25GbE networking	AIOM 4x 25GbE SFP28 Intel E810-CAM1, RoHS
TPM	AOM-TPM-9672V- TPM 2.0 with 10 pins SPI,RoHS
CacheVault	Broadcom 05-50039-00 CacheVault with 24-inch remote extender
Battery holder	PCIe plastic battery holder with FH/LP-bracket,RoHS
Cable	Slimline x8 (STR) to slimline x4 (STR),64CM,100 OHM,RoH
Cable	Slimline x8 (LE) to 2x slimline x4 (STR),FFC,76/76CM,10
Heatsink	1U passive CPU VC heatsink for AMD socket SP5 processors
Power	2x 860W redundant (1 + 1) titanium level (96%) power supplies Input: 800W: 100-127Vac/50-60Hz, 860W: 200-240Vac/50-60Hz, 860W: 240Vdc/ 50-60Hz

Mechanical details

The following sections describe the mechanical specifications and requirements for a node.

Dimensions

The arrows in the figure below identify the faces of the node. Use this figure as a reference for the table of physical dimensions that follows the figure.



The table below shows the physical dimensions of the server module.

Parameter	Inches	Millimeters
Server module depth - rack mounting surface to rear connectors surface	23.5	597
Total depth - front surface of handles to rear tab on power supply	26	660.4
Front width	17.2	437
Front width with rack ears	19	482.6
Rear width	17.6	447
Height (1U)	1.7	43

Weight

The table below shows the weights of the various components of an HCP O12 Node and an HCP O12 system.

Item	Quantity	Unit weight lbs (kg)	Extended weight lbs (kg)
HCP O12 Node local storage base unit - includes enclosure, mounting rails, motherboard, drive backplane, two power supplies, six cooling fans, airflow baffle, one CPU, twelve 64GB DIMMs, ten SSDs, RAID controller card with 768 GB of fixed memory, four-port 25GbE network card, two-port 25GbE SFP/10 GbE RJ45 network card, and two power cables.	1	54.01 (24.55)	54.01 (24.55)

Ethernet Switches

Item	Quantity	Unit weight lbs (kg)
Cisco Catalyst 1200	2	11.97 (5.43)
Cisco Nexus 93180YC-FX3	2	121.25 (55)

Fibre Channel Switch

Item	Quantity	Unit weight lbs (kg)
Cisco MDS 9148V	2	21.8 (9.9)

Cables

Item	Quantity	Unit weight lbs (kg)	Extended weight lbs (kg)
Two-meter AC power cable - two required for each switch	2	0.5 (0.227)	1.0 (0.454)
Seven-foot 1Gb Ethernet cable harness	2	3.08 (1.4)	6.16 (2.8)
Twenty-five-foot 1Gb Ethernet cable harness	2	11 (5)	22 (10)
Three-meter 10Gb Ethernet cable (Twinax)	2	0.1 (0.22)	0.2 (0.44)
Five-meter 10Gb Ethernet cable (Twinax)	2	0.18 (0.4)	0.36 (0.8)
Ten-meter 10Gb Ethernet cable (Twinax)	2	0.36 (0.79)	0.72 (1.58)

Hitachi Universal V3 Rack and PDU

See <https://docs.hitachivantara.com/r/en-us/universal-rack/v3/mk-97rk001>.

Hitachi Universal V3 Rack

For the physical dimensions of the Hitachi Universal V3 Rack used when the node is purchased with this rack, see <https://docs.hitachivantara.com/r/en-us/universal-rack/v3/mk-97rk001>.

Customer-supplied rack

You can purchase HCP O12 Nodes without a rack and then install the servers into a rack you supply. If you are supplying the rack(s) for the HCP system, you are responsible for the components shown below:

- A rack that meets these requirements:
 - The rack must be a standard 19-inch rack.
 - The rack must have square holes in the vertical EIA rails.
 - The rack depth must be at least 43.3 inches (1,100mm). The depth of the server, depth of Ethernet switches, and necessary room for cable management necessitates this depth requirement.
 - The server depth shown in the following figure is 23.5 inches (597mm). The power supply tab adds about another inch (25mm). An HCP system requires approximately ten inches (250mm) in the rear of the rack for cable management. Since most racks have a setback from the front of the rack to the vertical EIA rails the total depth required exceeds that of a 39.3 inch rack (1000mm).
 - The width shown in the following figure is 17.2 inches (437mm) and the customer rack must accommodate this dimension. The width shown includes the rail kit required space.



- The distance between the outer surfaces of the front and rear vertical EIA rails should be a minimum of 29 inches (736.6mm). While the server rail kit is able to mount with a shorter depth, some of the Ethernet switch equipment, particularly Cisco Nexus 93180YC-FX3, require this minimum distance.

- PDUs. Power Distribution Units need to provide the appropriate number of IEC 60320 C13 and C19 outlets and appropriate amperage to power the equipment installed in the rack. For proper redundancy, components in the rack should be connected to two PDUs, one for each of the power supplies provided. If a component only has one power supply it should be connected to the first PDU and its redundant counterpart should be connected to the second PDU.

See the following table for the appropriate outlets required for each HCP system component.

Component	# of U	# of Outlets	Outlet Type
HCP O12 Node	1	2	C13
Cisco Catalyst 1200 Ethernet	1	1	C13
Cisco Nexus 93180YC-FX3 Ethernet	1	2	C13
Cisco MDS 9148V Fibre Channel	1	2	C13

- For power requirements of each device, see [Electrical requirements \(on page 21\)](#).
- For storage components, including HCP S32 or Hitachi storage arrays, see the appropriate documentation for those devices to determine the appropriate rack space, outlet quantity, outlet type, and power capacity requirements.
- Velcro straps and/or cable ties for bundling and securing cables.
- Screws and caged nuts for installing equipment into the rack(s).

Electrical requirements

The following sections describe the power requirements and electrical specifications for an HCP O12 Node and other required HCP system components.

Power system

For redundancy, an HCP O12 Node has two power supplies. These power supplies should be connected to two different PDUs, which should be plugged into two separate 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 PDUs should be plugged into different 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.

The power system input can be either single-phase or three-phase with single phase on the outlets.

PDU for the Hitachi Universal V3 Rack

For information about the PDU power system requirements for the Hitachi Universal V3 Rack, see <https://docs.hitachivantara.com/r/en-us/universal-rack/v3/mk-97rk001>.

Power connections

The power connections required by the Hitachi Universal V3 Rack differ by geography and input phase:

Americas

The single-phase, 208V, 30A PDUs have a NEMA L6-30P three-wire plug, as shown below.



The three-phase, 208V, 30A PDUs have a NEMA L15-30 four-wire plug, as shown below.



EMEA/APAC

The single-phase, 230V, 32A PDUs have an IEC 309 three-wire plug, as shown below.



The three-phase, 400V, 32A PDUs have an IEC 320 five-wire power plug, as shown below.



Each HCP system comes with multiple PDUs with IEC 320 C13 and IEC 320 C19 outlets. Each HCP O12 Node has two power supplies with IEC 320 C14 power inlet connectors. Each power supply connects to a PDU using a two-meter IEC 320 C13 to IEC 320 C14 power cable, as shown below. Optional Fibre Channel switches and Ethernet switches use two-meter IEC 320 C13 to IEC 320 C14 power cables.



IEC C14

IEC C13

Optional S10 nodes that come in the same rack as an HCP system plug into the IEC 320 C19 power outlets on the PDUs. Each S10 storage node has two power and cooling modules which should be connected to the PDUs using two-meter IEC 320 C19 to IEC 320 C20 power cables as shown below.



Electrical specifications

In an HCP system, all electrical components are designed to be redundant. For each device in the system, there are either two power supplies or two of the devices so that there is no single point of failure if a power supply or PDU fails. In addition, since all components are redundant, the PDUs on different sides of the rack connect to different power systems, providing power system redundancy.

When an HCP system component with two power supplies is operating normally, each power supply contributes half the power that the device requires. If one power supplies fails, the HCP component continues to run on the single available power supply.

The table below describes the amperages and voltages of the different PDU models.

PDU model	Amperage	Voltage
3P30A-24C13-6C19UL.P	30	208
3P32A-24C13-6C19CE.P	32	400
3P30A-15C13-3C19UL.P	30	208
1P30A-15C13-3C19UL.P	30	208
3P16A-15C13-3C19CE.P	16	400
1P32A-18C13-3C19CE.P	32	230
3P30A-8C13-3C19UL.P	30	208
1P30A-8C13-3C19UL.P	30	208
3P16A-9C13-3C19CE.P	16	400
1P32A-9C13-3C19CE.P	32	230

The table below describes the nominal amperages and wattage of each possible component in an HCP system.

Component	Nominal wattage @ 220V (A)	Nominal wattage @ 220V (W)
HCP O12 Node	N/A	N/A
Cisco Catalyst 1200 - 24 port	110V: 0.24 220V: 0.13	110V: 25.9 220V: 27.5
Cisco Catalyst 1200 - 48 port	110V: 0.41 220V: 0.2	110V: 44.81 220V: 43.93
Cisco Nexus 93180YC-FX3	N/A	N/A
Cisco MDS 9148V	N/A	N/A

RoHS compliance

An HCP O12 Node, including all its components, is compliant with the European Union Restriction of Hazardous Substances (RoHS) Directive (Directive 2002/95/EC), with no exceptions or exemptions.

BNST compliance

Benzenamine, N-phenyl-, reaction products with styrene and 2,4,4-trimethylpentene (BNST) is an antioxidant used as an additive in many industrial lubricants. Its use has been restricted in Canada under the Prohibition of Certain Toxic Substances Regulations, 2012, which went into effect on March 14, 2013. The Regulations include a two-year exemption for BNST used in small-application lubricants in the electrical and electronics engineering industry.

Temperature, humidity, and altitude

The table below shows the acceptable ranges for temperature, humidity, and altitude for the various HCP system components as well as an aggregate for the entire system. Operating and non-operating cases are included in the table below.

Component	Operating temperature *	Operating humidity (non-condensing)	Altitude	Non-operating temperature	Non-operating humidity (non-condensing)
HCP system (not including storage components)	10°C to 35°C (50°F to 95°F)	8%-90%	900m (3,000 feet)	-40°C to 60°C (-40°F to 140°F)	5%-95%
HCP O12 Node	10°C to 35°C	8%-90%	900m (3,000 feet)	-40°C to 60°C	5%-95%

Component	Operating temperature *	Operating humidity (non-condensing)	Altitude	Non-operating temperature	Non-operating humidity (non-condensing)
	(50°F to 95°F)			(-40°F to 140°F)	
Cisco Catalyst 1200	32°C to 122°C (0°F to 50°F)	10%-90%	3,000m (10,000 feet)	-25°C to 70°C (-13°F to 158°F)	10%-90%
Cisco Nexus 93180YC-FX3	0°C to 40°C (32°F to 104°F)	5%-95%	0-4000m (0-13,123 feet)	-40°C to 70°C (-40°F to 158°F)	5%-95%
Cisco MDS 9148V	0°C to 40°C (32°F to 104°F)	10%-90%	-60-2000m (-197-6,500 feet)	-40°C to 70°C (-40°F to 158°F)	10%-95%
* The maximum operating temperature value is specified at sea level and is derated 2.0% per 1,000 feet of increased altitude.					

Shock and vibration

The table below shows the tested limits for shock and vibration for an HCP system and its components where this information is available.

Table 1 HCP server

Vibration (sinusoidal)		Vibration (random)		Shock	
Operating	Non-operating	Operating	Non-operating	Operating	Non-operating
0.25 G at 5 to 200 Hz. Approx. 15 in/axis.	0.5 G at 5 to 200 Hz. Approx. 15 in/axis.	0.40g rms at 5 to 200 Hz. Approx. 60 min/axis.	0.98g rms at 5 to 200 Hz. Approx. 30 min/axis.	2.5 ms duration, 20G, half-sine, one shock on each side.	10 ms duration, 10-20G, square wave, one shock on each side.

Table 2 Cisco switches

Component	Operating shock	Non-operating shock	Operating vibration	Non-operating vibration
Cisco Catalyst 1200	N/A			
Cisco Nexus 93180YC-FX3	N/A			
Cisco MDS 9148V	20G, 11ms, half-sine	44G, 15ms, square wave	0.5G peak, 0.7Grms random, 5 to 500 Hz	2.0G sine, 1.4Grms random, 5 to 500 Hz

Cooling and airflow

The airflow in of all components of an HCP system is designed to go from front to rear and is driven by fans on the various components. Air is pulled through the front of the rack and exhausted out the rear of the rack. Components mounted in the rack, such as Ethernet or Fibre Channel switches, have port side exhaust in keeping with the overall rack airflow. Customers should not reorient the devices in the rack or the airflow may be compromised.

The following table shows the heat dissipation for each of the components, allowing a customer to calculate the heat load and required cooling for their HCP system based on the components installed. It also includes the acoustic noise level of the fans in the units which are providing the airflow, where this information is available.

Component	Heat Dissipation (BTU/h)	Acoustic Noise Level (dB)
HCP O12 Node	N/A	50 DBA
Cisco Catalyst 1200	536.05	0 (Fanless)
Cisco Nexus 93180YC-FX3	2047.285	22
Cisco MDS 9148V	N/A	N/A

When a number of the HCP system components are powered on, the fans run at full speed for a short time to ensure that they are fully operational. After that, under normal conditions, the fans run at lower speeds as required by the device for maintaining appropriate airflow and cooling to the components. The cooling they provide is sufficient to prevent the hard disk drives and other components from exceeding the manufacturer's rated specifications throughout the range of the operating conditions. If overtemperature conditions occur, some of the devices have automatic shutdown capability, but not in all cases.

If a single fan fails in any of the HCP system components, the device continues to operate. However, this fault condition forces the remaining fans to run at higher speed until the condition is corrected.

Required tools and supplies

When assembling, deploying, or maintaining an HCP system, you may need certain tools and supplies. The items you need for any given procedure are listed before the instructions for that procedure.

These are all the tools and supplies that may be required:

Lift

Depending on the type of storage devices used in conjunction with the HCP system, a lift may be required to install or maintain disk storage trays into a rack. The lift must be rated at a minimum of 400 pounds (182kg).

Tools

For installation and maintenance procedures on an HCP system, the following tools may be required:

- #1 Phillips screwdriver
- #2 Phillips screwdriver
- ¼-inch flat-head screwdriver
- Caged nut tool
- Wire cutter

Keyboard and monitor

For the installation of the HCP software, or to perform diagnostics and recover the HCP software, you need a USB keyboard and VGA monitor.

Laptop computer

To upload an HCP software update file, license file, or to use the management console you will need to use a browser on a laptop computer.

1Gb CAT6 Ethernet cable

To connect the laptop computer to the back-end network switch, you need a 1Gb CAT6 Ethernet cable. For 10GB systems, a 1Gb adapter for the switch will be provided.

PDUs with C13/C19 power outlets

To provide power to the HCP system during installation, you need two PDUs with C13 and/or C19 outlets as appropriate for the system being configured. You need these PDUs only if the HCP system will be shipped without a rack.

One 4GB or larger USB flash drives

For the HCP software installation, you need one 4GB or greater USB flash drive. For the best results, use the certified Hitachi Vantara part number DT14GL.P

Chapter 3: Mounting unracked components

The components of an unracked system are delivered configured but not installed in a rack. You need to provide some additional components for installing the system in a rack at your site. This chapter provides instructions for doing this.

Components that come with a rackless system

For a rackless system, the following components are shipped to your site:

- The required numbers of nodes, with the HCP software already installed.



Note: Do not add the same number of nodes, or more nodes, than you have in your cluster; otherwise, it causes a node outage due to metadata rebalancing.

- One or two Ethernet switches for the back-end network. The type and quantity of Ethernet switches you receive depends on your system network configuration. The possible switch types are:

Cisco Catalyst C1200

is a 1 Gbps Ethernet Port switch. You receive four Cisco Catalyst C1200 switches with your system, one for front-end and one for back-end.

Cisco Nexus C93180YC-FX3

is a 25 Gbps SFP28 Ethernet switch. You receive four Cisco Nexus C93180YC-FX3 switches with your system, one for front-end and one for back-end.

- If you use a 1 G network configuration, you are supplied with the required number of Ethernet cables harnesses, half red and half blue. If you use a 10G network configuration, you are supplied the required amount of Ethernet cables to connect your nodes to the back-end network.
- The required amount of power cords for the nodes and back-end switches.
- An Ethernet cable for connecting back-end switches to each other if you are using a network configuration that supports two back-end switches: one purple cable for a 1 G network configuration or one black cable for a 10 G network configuration.
- The required number of perforated blanking plates for covering the back-end switches.

- One service tag per system. This label is on the lower left side of the lowest node.
- The license-key packet. If the HCP software was installed with encryption enabled, this packet also includes the Encryption Key form.



Caution: Store the Encryption Key form in a secure location. The key recorded on this form is not retrievable through the HCP System Management Console or management API. Loss of this key will most likely result in unrecoverable data in the case of catastrophic system failure.

Hardware assembly procedure

To assemble the HCP system:

1. Prepare the rack for installation of the HCP system components.
2. Attach the HCP O12 service tag.
3. Install the PDUs in the rack.
4. (Optional) Rack the HCP O12 Nodes.
5. Rack the HCP O12 enclosure.
6. Rack the Ethernet switches.
7. (Optional) Cover the unused rack units with blanking plates.
8. Reassemble the rack.

Considerations for HCP racking and PDU connections

This section describes the possible HCP system racking configurations and how to connect HCP hardware components to PDUs.

Considerations for racking an HCP O12 system

An HCP O12 system includes a minimum of four HCP O12 Nodes and a maximum of 80 HCP O12 Nodes. The nodes can be racked in a base configuration with Ethernet switches or in an appliance configuration with Ethernet switches and optional S32 Nodes.

In a base configuration, an HCP system can have up to five racks — one base configuration rack and, optionally, one through four expansion racks. A base configuration does not include a VSP Gx00 model or S32 Nodes.

In an appliance configuration, an HCP system can have only one rack but can be expanded with additional storage in secondary racks. An appliance configuration includes one or more VSP Gx00 models arrays or S32 Nodes.

If the HCP system in a base configuration uses expansion racks, those racks must be positioned on the right and left of the base or appliance configuration rack in alternating order so that all HCP O12 Nodes can connect to the back-end Ethernet switches.

The figure below shows how to position the racks.



Tip: For ease of access, remove and set aside the rack side panels and doors before racking and cabling components.

PDUs for the Hitachi Universal V3 Rack

Outlet layout

The PDU for the Hitachi Universal V3 Rack has three color-coded sections: blue, brown, and green. The power inlet cable is attached to the blue end of the PDU.

Each colored-coded section has:

- One or two circuit breakers
- Some number of C19 outlets
- Some number of C13 outlets

In a section with two circuit breakers, the circuit breaker closer to the power inlet cable is number one.

The C19 and C13 outlets are counted separately for each circuit breaker within each section. For each type of outlet, the outlet closest to the applicable circuit breaker is number one.

Each outlet is identified by the following properties, in order:

- The section color: B (blue), R (brown), or G (green)
- The breaker number: 1 or 2
- The outlet type: C19 or C13
- The number of the outlet within its section, preceded by a hyphen (-)

For example, the second C13 outlet for circuit breaker one in the red section is R1C13-2.

PDU part numbers

PDU part numbers describe the PDU model by its hardware characteristics and geographic distribution. Each PDU part number consists of these properties, in order:

- Phase: 1P or 3P
- Amperage: 20A
- Number of C13 outlets: 8C13, 9C13, 10C13, 15C13, or 24C13
- Number of C19 outlets: 2C19, 3C19, or 6C19
- Geographic distribution: UL (Americas) or CE (EMEA/APAC)
- Suffix: .P

For example, a three-phase, EMEA/APAC PDU with an amperage of 30, 15 C13 outlets, and three C19 outlets is 3P30A-15C13-3C19-UL20A.P.

Not all possible part numbers are used. For example, no PDU has the part number 3P10A-10C13-3C19-UL20A.P.

Considerations for connecting PDUs

A rack can have one, two, or three pairs of PDUs. In each pair, one PDU is installed on the left side of the rack. The other PDU is installed on the right side of the rack. For redundancy, the PDUs in each pair should, if possible, be connected to two separate power sources.

If a hardware component has two power supplies. The left power supply connects to the left PDU. The right power supply connects to the right PDU.

To balance the HCP system electrical requirements across the PDU breakers and phases, the system hardware components connect to specific PDU outlets. These outlets are determined by the HCP system racking configuration and the PDU model.

HCP racking and connection diagram

The diagram in this section shows the possible HCP system racking configurations, how to rack the hardware components, and how to connect the hardware components to the PDUs.

Reading the diagram

The racking and connection diagram shows a single rack. The view is from the rear of the rack.

The diagram has:

- Columns that show possible hardware configurations
- Left and right U# columns that show the rack units in which each hardware component is installed
- Left and right PDU outlet columns that show only the outlets used with the hardware configurations in the diagram
- Left and right PDU configuration columns that show the number of PDUs installed on each side of the rack and the orientation of each PDU

Each hardware component connects to the outlets that, in the diagram, are aligned with the bottom or only rack unit occupied by that component.

Diagram legend

In the diagram:

- Hardware components that span columns are used in the configuration shown in the diagram.
- Sections that have no label do not contain any hardware components for the applicable configuration.
- Rack units in italics with a gray background in the U# column show the PDU bracket locations.
- Outlets with darker background colors are C13 outlets. Outlets with lighter background colors are C19 outlets.

- Outlet background colors — blue, brown, and green for the Universal V3 Rack — correspond to the circuits on the PDUs.
- Outlets with black text are always used with the applicable component. Outlets with white text are used only if the applicable component has two power supplies.
- The PWR label on each PDU shows which end of the PDU has the power inlet cable.

The PDUs in the diagram are not drawn to scale.

Hitachi Universal V3 Rack diagram

The Hitachi Universal V3 Rack diagram illustrates the rack-mounting of an HCP O12.

Rack-mounting a RAIN system

The figure below illustrates a maximum rack population.

A rack containing nodes but no storage can have a maximum of 16 nodes. A rack containing S32 Nodes with or without storage can have a maximum of 8 nodes.

Rack-mounting an HCP O12 system in a non-appliance rack (single phase)

	RAIN system	RAIN with S32	RAIN with S32	RAIN with S32
U42	Empty	Empty	Empty	Empty
U41				
U40				
U39				
U38				
U37				
U36				
U35				
U34				
U33				
U32				
U31				
U30				
U29				
U28				
U27				
U26	Ethernet switch #2	Ethernet switch #2	Ethernet switch #2	Ethernet switch #2
U25	Ethernet switch #1	Ethernet switch #1	Ethernet switch #1	Ethernet switch #1
U24	Empty	Empty	Empty	Empty
U23				
U22				
U21				
U20				
U19				
U18				
U17				
U16				
U15				
U14				
U13				
U12				
U11				
U10				
U9				
U8				
U7				
U6				
U5				
U4				
U3				
U2				
U1				

Rack-mounting an HCP O12 system in a non-appliance rack (single phase)

The following figures show the layout for mounting an HCP O12 appliance in a non-appliance rack (that is, a rack Universal V3 Rack containing only server nodes and switches, with no S32 Nodes or other storage).

In this figure, the PDUs used are either:

- Single-phase 1P30A-10C13-2C19-UL20A.P (Americas)
- Single-phase 1P32A-10C13-2C19-CE20A.P (EMEA and APAC)



Note: In the following figures, an asterisk denotes an outlet used only when the Ethernet switch has two power supplies.

		1-Phase US (1P30A-10C13-2C19-UL20A.P)			
Left PDU's	U#	1-Phase EMEA/APAC (1P32A-10C13-2C19-CE20A.P)	U#	Right PDU's	
PDU 3	U42	Empty	U42	PDU 3	
	U41		U41		
	U40		U40		
	U39		U39		
	U38		U38		
	U37		U37		
	U36		U36		
	U35		U35		
	U34		U34		
	U33		U33		
	U32		U32		
	U31		U31		
	U30		U30		
U29	U29				
	B1C13-2 U28	Fiber switch # 2	U28	B1C13-2	
PWR	B1C13-1 U27	Fiber switch # 1	U27	B1C13-1	PWR
PDU 2	R1C13-4* U26	Ethernet switch #2	U26	R1C13-4	
	R1C13-3 U25	Ethernet switch #1	U25	R1C13-3*	
	U24	Empty	U24		
	U23		U23		
	U22		U22		
	U21		U21		
	U20		U20		
	U19		U19		
	U18		U18		
	U17		U17		
	R1C13-2 U16		O12 node #16	U16	R1C13-2
	R1C13-1 U15		O12 node #15	U15	R1C13-1
	B1C13-4 U14		O12 node #14	U14	B1C13-4
B1C13-3 U13	O12 node #13		U13	B1C13-3	
B1C13-2 U12	O12 node #12		U12	B1C13-2	
PWR	B1C13-1 U11	O12 node #11	U11	B1C13-1	PWR
PWR	B1C13-1 U10	O12 node #10	U10	B1C13-1	PWR
PDU 1	B1C13-2 U9	O12 node #9	U9	B1C13-2	PDU 1
	B1C13-3 U8	O12 node #8	U8	B1C13-3	
	B1C13-4 U7	O12 node #7	U7	B1C13-4	
	B1C13-5 U6	O12 node #6	U6	B1C13-5	
	R1C13-1 U5	O12 node #5	U5	R1C13-1	
	R1C13-2 U4	O12 node #4	U4	R1C13-2	
	R1C13-3 U3	O12 node #3	U3	R1C13-3	
	R1C13-4 U2	O12 node #2	U2	R1C13-4	
	R1C13-5 U1	O12 node #1	U1	R1C13-5	

Rack-mounting an HCP O12 system in a non-appliance rack (3-phase)

The following figures show the layout for mounting an HCP O12 appliance in a non-appliance rack (that is, a rack Universal V3 Rack containing only server nodes and switches, with no S32 Nodes or other storage).

In this figure, the PDUs used is 3-phase 3P30A-8C13-3C19-UL20A.P (Americas). There is no EMEA or APAC equivalent,



Note: In the following figures, an asterisk denotes an outlet used only when the Ethernet switch has two power supplies.

Left PDU's		3-Phase US (3P30A-8C13-3C19-UL20A.P)	Right PDU's				
		There is no EMEA/APAC equivalent					
PDU 3	U#	Empty	U#	PDU 3			
	U42		U42				
	U41		U41				
	U40		U40				
	U39		U39				
	U38		U38				
	U37		U37				
	U36		U36				
	U35		U35				
	U34		U34				
	U33		U33				
	U32		U32				
	U31		U31				
	U30		U30				
U29	U29						
R1C13-2	U28	Fiber switch # 2	U28	R1C13-2			
R1C13-1	U27	Fiber switch # 1	U27	R1C13-1			
B1C13-2*	U26	Ethernet switch #2	U26	B1C13-2			
PWR	B1C13-1	U25	Ethernet switch #1	U25	B1C13-1*	PWR	
PDU 2	U#	Empty	U#	PDU 2			
	U24		U24				
	U23		U23				
	U22		U22				
	U21		U21				
	U20		U20				
	U19		U19				
	U18		U18				
	U17		U17				
	Y1C13-2		U16		O12 node #16	U16	Y1C13-2
	Y1C13-1		U15		O12 node #15	U15	Y1C13-1
	R1C13-3		U14		O12 node #14	U14	R1C13-3
	R1C13-2		U13		O12 node #13	U13	R1C13-2
	R1C13-1		U12		O12 node #12	U12	R1C13-1
B1C13-3	U11	O12 node #11	U11	B1C13-3			
B1C13-2	U10	O12 node #10	U10	B1C13-2			
PWR	B1C13-1	U9	O12 node #9	U9	B1C13-1	PWR	
PWR	B1C13-1	U8	O12 node #8	U8	B1C13-1	PWR	
PDU 1	B1C13-2	U7	O12 node #7	U7	B1C13-2		
	B1C13-3	U6	O12 node #6	U6	B1C13-3		
	R1C13-1	U5	O12 node #5	U5	R1C13-1		
	R1C13-2	U4	O12 node #4	U4	R1C13-2		
	R1C13-3	U3	O12 node #3	U3	R1C13-3		
	Y1C13-1	U2	O12 node #2	U2	Y1C13-1		
	Y1C13-2	U1	O12 node #1	U1	Y1C13-2		

		3-Phase EMEA/APAC (3P32A-24C13-6C19-CE20A.P)			
Left PDU's	U#	There is no US equivalent		U#	Right PDU's
	U42			U42	
	U41			U41	
	U40			U40	
	U39			U39	
	U38			U38	
	U37			U37	
	U36			U36	
	U35	Empty		U35	
	U34			U34	
	U33			U33	
	U32			U32	
	U31			U31	
	U30			U30	
	U29			U29	
	Y1C13-8	Fiber switch # 2		U28	Y1C13-8
	Y1C13-7	Fiber switch # 1		U27	Y1C13-7
	Y1C13-6*	Ethernet switch #2		U26	Y1C13-6
	Y1C13-5	Ethernet switch #1		U25	Y1C13-5*
	U24			U24	
	U23			U23	
	U22			U22	
	U21			U21	
	U20	Empty		U20	
	U19			U19	
	U18			U18	
	U17			U17	
	Y1C13-4	O12 node #16		U16	Y1C13-4
	Y1C13-3	O12 node #15		U15	Y1C13-3
	Y1C13-2	O12 node #14		U14	Y1C13-2
	Y1C13-1	O12 node #13		U13	Y1C13-1
	R1C13-8	O12 node #12		U12	R1C13-8
	R1C13-7	O12 node #11		U11	R1C13-7
	R1C13-6	O12 node #10		U10	R1C13-6
	R1C13-5	O12 node #9		U9	R1C13-5
	R1C13-4	O12 node #8		U8	R1C13-4
	R1C13-3	O12 node #7		U7	R1C13-3
	B2C13-8	O12 node #6		U6	B2C13-8
	B2C13-7	O12 node #5		U5	B2C13-7
	B2C13-6	O12 node #4		U4	B2C13-6
	B2C13-5	O12 node #3		U3	B2C13-5
	B1C13-4	O12 node #2		U2	B1C13-4
PWR	B1C13-3	O12 node #1		U1	B1C13-3
					PWR

Rack-mounting an HCP O12 system with HCP S32 Nodes (single or 3-phase)

The following figures show the layout for mounting an HCP O12 appliance in a rack that contains S32 Nodes.

In these figures, the PDUs used are either single phase for Americas and EMEA (top figure) or 3-phase for Americas and EMEA (bottom figure).



Note: In the following figures, an asterisk denotes an outlet used only when the Ethernet switch has two power supplies.

Rack-mounting an HCP O12 system with HCP S32 Nodes (single or 3-phase)

		3x 4U106 units	3x S32 with 1 x 4U106 each	1 x with 2 4U106 & 1 x with 1 4U106				
Left PDU's	U#	Hardware (1-phase US & EMEA)			U#	Right PDU's		
PDU 3	U42	Empty	Empty	Empty	U42	PDU 3		
	U41				U41			
	U40				U40			
	U39				U39			
	U38				U38			
	U37				U37			
	RIC13-4	U36	O12 node #8	O12 node #8	O12 node #8	U36	RIC13-4	
	RIC13-3	U35	O12 node #7	O12 node #7	O12 node #7	U35	RIC13-3	
	RIC13-2	U34	O12 node #6	O12 node #6	O12 node #6	U34	RIC13-2	
	RIC13-1	U33	O12 node #5	O12 node #5	O12 node #5	U33	RIC13-1	
81C13-4	U32	O12 node #4	O12 node #4	O12 node #4	U32	81C13-4		
81C13-3	U31	O12 node #3	O12 node #3	O12 node #3	U31	81C13-3		
81C13-2	U30	O12 node #2	O12 node #2	O12 node #2	U30	81C13-2		
PWR	81C13-1	U29	O12 node #1	O12 node #1	O12 node #1	U29	81C13-1	PWR
PDU 2	RIC13-4	U28	Fiber switch # 2	Fiber switch # 2	Fiber switch # 2	U28	RIC13-4	
	RIC13-3	U27	Fiber switch # 1	Fiber switch # 1	Fiber switch # 1	U27	RIC13-3	
	RIC13-2*	U26	Ethernet switch #2	Ethernet switch #2	Ethernet switch #2	U26	RIC13-2	
	RIC13-1	U25	Ethernet switch #1	Ethernet switch #1	Ethernet switch #1	U25	RIC13-1*	
		U24	Empty	Empty	Empty	U24	PDU 2	
		U23				U23		
		U22				U22		
		U21				U21		
		U20				U20		
		U19				U19		
	U18	4U106 tray #1	Empty	Empty	U18			
	U17				U17			
	U16				U16			
	81C19-1	4U106 tray #2	4U106 tray #1	4U106 tray #1	U15	81C19-1		
	81C13-1				U14	81C13-1		
PWR	81C19-1	U13	4U106 tray #3	S32 Base unit	U13	81C19-1	PWR	
PWR		U12			U12		PWR	
PDU 1		U11	4U106 tray #2	4U106 tray #1	4U106 tray #1	U11	PDU 1	
		U10				U10		
		81C19-1	S32 Base unit	S32 Base unit	S32 Base unit	U9		81C19-1
		U8				U8		
		81C13-2	4U106 tray #1	4U106 tray #1	4U106 tray #1	U7		81C13-2
		U6				U6		
		U5				U5		
		U4	U4					
	RIC19-1	4U106 tray #1	4U106 tray #1	4U106 tray #1	U3	RIC19-1		
	U2				U2			
	RIC13-2	S32 Base unit	S32 Base unit	S32 Base unit	U1	RIC13-2		

Rack-mounting an HCP O12 system with HCP S32 Nodes (single or 3-phase)

		3x 4U106 units	3x S32 with 1 x 4U106 each	1 x with 2 4U106 & 1 x with 1 4U106						
Left PDU's	U#	Hardware (3-phase US & EMEA)			U#	Right PDU's				
PDU 3	U42	Empty	Empty	Empty	U42	PDU 3				
	U41				U41					
	U40				U40					
	U39				U39					
	U38				U38					
	U37				U37					
	Y1C13-2 U36				O12 node #8		O12 node #8	O12 node #8	U36	Y1C13-2
	Y1C13-1 U35				O12 node #7		O12 node #7	O12 node #7	U35	Y1C13-1
	B1C13-3 U34				O12 node #6		O12 node #6	O12 node #6	U34	B1C13-3
	B1C13-2 U33				O12 node #5		O12 node #5	O12 node #5	U33	B1C13-2
B1C13-1 U32	O12 node #4	O12 node #4	O12 node #4	U32	B1C13-1					
R1C13-3 U31	O12 node #3	O12 node #3	O12 node #3	U31	R1C13-3					
R1C13-2 U30	O12 node #2	O12 node #2	O12 node #2	U30	R1C13-2					
PWR R1C13-1 U29	O12 node #1	O12 node #1	O12 node #1	U29	R1C13-1	PWR				
PDU 2	R1C13-3 U28	Fiber switch # 2	Fiber switch # 2	Fiber switch # 2	U28	R1C13-3				
	R1C13-2 U27	Fiber switch # 1	Fiber switch # 1	Fiber switch # 1	U27	R1C13-2				
	R1C13-1* U26	Ethernet switch #2	Ethernet switch #2	Ethernet switch #2	U26	R1C13-1				
	B1C13-2 U25	Ethernet switch #1	Ethernet switch #1	Ethernet switch #1	U25	B1C13-2				
	U24	Empty	Empty	Empty	U24	PDU 2				
	U23				U23					
	U22				U22					
	U21				U21					
	U20				U20					
	U19				U19					
U18	U18									
U17	U17									
U16	4U106 tray #1				U16					
R1C19-1 U15	4U106 tray #2				U15		R1C19-1			
B1C13-1 U14		U14	B1C13-1							
PWR R1C19-1 U13	4U106 tray #3	S32 Base unit	U13	R1C19-1	PWR					
PWR	U12	U12	PWR							
PDU 1	U11	4U106 tray #1	4U106 tray #1	4U106 tray #1	U11	PDU 1				
	U10				U10					
	R1C19-1 U9				U9		R1C19-1			
	U8				U8					
	R1C13-2 U7				S32 Base unit		S32 Base unit	U7	R1C13-2	
	U6				U6					
	U5				U5					
	U4				U4					
	B1C19-1 U3				U3		B1C19-1			
	U2				U2					
Y1C13-2 U1	S32 Base unit	S32 Base unit	S32 Base unit	U1	Y1C13-2					

Rack-mounting an HCP O12 system with HCP S32 Nodes (single or 3-phase)

The following figures show the layout for mounting an HCP O12 appliance in a rack that contains S32 Nodes.

In these figures, the PDUs used are either single phase for Americas and EMEA (top figure) or 3-phase for Americas and EMEA (bottom figure).



Note: In the following figures, an asterisk denotes an outlet used only when the Ethernet switch has two power supplies.

Rack-mounting an HCP O12 system with HCP S32 Nodes (single or 3-phase)

		3x 4U106 units	3x S32 with 1 x 4U106 each	1 x with 2 4U106 & 1 x with 1 4U106				
Left PDU's	U#	Hardware (1-phase US & EMEA)			U#	Right PDU's		
PDU 3	U42	Empty	Empty	Empty	U42	PDU 3		
	U41				U41			
	U40				U40			
	U39				U39			
	U38				U38			
	U37				U37			
	RIC13-4	U36	O12 node #8	O12 node #8	O12 node #8		U36	RIC13-4
	RIC13-3	U35	O12 node #7	O12 node #7	O12 node #7		U35	RIC13-3
	RIC13-2	U34	O12 node #6	O12 node #6	O12 node #6		U34	RIC13-2
	RIC13-1	U33	O12 node #5	O12 node #5	O12 node #5		U33	RIC13-1
81C13-4	U32	O12 node #4	O12 node #4	O12 node #4	U32	81C13-4		
81C13-3	U31	O12 node #3	O12 node #3	O12 node #3	U31	81C13-3		
81C13-2	U30	O12 node #2	O12 node #2	O12 node #2	U30	81C13-2		
PWR	81C13-1	U29	O12 node #1	O12 node #1	O12 node #1	U29	81C13-1	PWR
PDU 2	RIC13-4	U28	Fiber switch # 2	Fiber switch # 2	Fiber switch # 2	U28	RIC13-4	
	RIC13-3	U27	Fiber switch # 1	Fiber switch # 1	Fiber switch # 1	U27	RIC13-3	
	RIC13-2*	U26	Ethernet switch #2	Ethernet switch #2	Ethernet switch #2	U26	RIC13-2	
	RIC13-1	U25	Ethernet switch #1	Ethernet switch #1	Ethernet switch #1	U25	RIC13-1*	
		U24	Empty	Empty	Empty	U24		
		U23				U23		
		U22				U22		
		U21				U21		
		U20				U20		
		U19				U19		
	U18	4U106 tray #1	Empty	Empty	U18			
	U17				U17			
	U16	4U106 tray #2	Empty	Empty	U16			
81C19-1	U15				U15	81C19-1		
81C13-1	U14	4U106 tray #3	S32 Base unit	4U106 tray #2	U14	81C13-1		
PWR	81C19-1		U13	U13	81C19-1	PWR		
PWR		U12			U12	PWR		
PDU 1		4U106 tray #1	4U106 tray #1	4U106 tray #1	U11			
					U10			
	81C19-1	4U106 tray #2	4U106 tray #1	4U106 tray #1	U9	81C19-1		
					U8			
	81C13-2	S32 Base unit	S32 Base unit	S32 Base unit	U7	81C13-2		
					U6			
		4U106 tray #1	4U106 tray #1	4U106 tray #1	U5			
					U4			
	81C19-1	S32 Base unit	S32 Base unit	S32 Base unit	U3	81C19-1		
					U2			
RIC13-2	U1	S32 Base unit	S32 Base unit	S32 Base unit	U1	RIC13-2		

		3x 4U106 units	3x S32 with 1 x 4U106 each	1 x with 2 4U106 & 1 x with 1 4U106						
Left PDU's	U#	Hardware (3-phase US & EMEA)			U#	Right PDU's				
PDU 3	U42	Empty	Empty	Empty	U42	PDU 3				
	U41				U41					
	U40				U40					
	U39				U39					
	U38				U38					
	U37				U37					
	Y1C13-2 U36				O12 node #8		O12 node #8	O12 node #8	U36	Y1C13-2
	Y1C13-1 U35				O12 node #7		O12 node #7	O12 node #7	U35	Y1C13-1
	B1C13-3 U34				O12 node #6		O12 node #6	O12 node #6	U34	B1C13-3
	B1C13-2 U33				O12 node #5		O12 node #5	O12 node #5	U33	B1C13-2
B1C13-1 U32	O12 node #4	O12 node #4	O12 node #4	U32	B1C13-1					
R1C13-3 U31	O12 node #3	O12 node #3	O12 node #3	U31	R1C13-3					
R1C13-2 U30	O12 node #2	O12 node #2	O12 node #2	U30	R1C13-2					
PWR	R1C13-1 U29	O12 node #1	O12 node #1	O12 node #1	U29	R1C13-1	PWR			
PDU 2	R1C13-3 U28	Fiber switch # 2	Fiber switch # 2	Fiber switch # 2	U28	R1C13-3				
	R1C13-2 U27	Fiber switch # 1	Fiber switch # 1	Fiber switch # 1	U27	R1C13-2				
	R1C13-1* U26	Ethernet switch #2	Ethernet switch #2	Ethernet switch #2	U26	R1C13-1				
	B1C13-2 U25	Ethernet switch #1	Ethernet switch #1	Ethernet switch #1	U25	B1C13-2*				
	U24	Empty	Empty	Empty	U24	PDU 2				
	U23				U23					
	U22				U22					
	U21				U21					
	U20				U20					
	U19				U19					
U18	U18									
U17	U17									
U16	4U106 tray #1				4U106 tray #2		U16			
R1C13-1 U15	S32 Base unit						U15	R1C13-1		
B1C13-1 U14		4U106 tray #2	U14	B1C13-1						
PWR	R1C13-1 U13	4U106 tray #3	S32 Base unit	U13	R1C13-1	PWR				
PWR	U12	4U106 tray #3	4U106 tray #1	U12	PWR					
PDU 1	U11	4U106 tray #2		S32 Base unit	S32 Base unit	U11	PDU 1			
	U10					U10				
	R1C13-1 U9					U9		R1C13-1		
	U8					U8				
	R1C13-2 U7					U7		R1C13-2		
	U6					U6				
	U5					U5				
	U4					U4				
	B1C13-1 U3					U3		B1C13-1		
	U2		U2							
Y1C13-2 U1	S32 Base unit	S32 Base unit	S32 Base unit	U1	Y1C13-2					

Considerations for racking nodes

An HCP O12 system can be racked with up to three S32 Nodes in a single rack. If you are racking S32 Nodes, you need to rack the S32 Nodes first at the bottom of the rack.

If the HCP system has more than three S32 Nodes, the extra S32 Nodes need to be racked in separate expansion racks.

Power cords

Each type of Ethernet switch comes with either one or two power cords depending on its needs. The power cords provided with the switches require PDUs with C13 IEC receptacles. HCP O12 servers come with two power cords each that also require PDUs with C13 IEC receptacles.

If your PDUs are not compatible with either of these types of power cords, you need to provide alternative power cords as applicable. The power cords you provide must have a C13 IEC plug at the end that connects to the server or switch.

Rackless assembly recommendation

The following rackless assembly procedure assumes you obey the HCP recommended rack and network setup configurations. If you deviate from the recommended configurations, you are responsible for providing all extra equipment and modifying the HCP system environment to accommodate for your changes. If you do not follow the recommended rack and network setups, it may cause future system expansion complications.

Tools and accessories you need

To assemble an HCP system, you need these tools:

- #2 Phillips screwdriver
- Cage-nut tool
- Wire cutter for trimming any cable ties you use
- Front panel key



Tip: Assembling the server rails is easiest with a magnetic screwdriver.

Prepare the racks

To facilitate the system assembly, remove the doors and sides from your racks.

Install the PDUs

Install the PDUs in the rack.

For instructions on installing PDUs, see [Considerations for HCP racking and PDU connections \(on page 30\)](#).

(Optional) Rack the HCP S32 Nodes

If the HCP system uses HCP S32 Nodes, you need to rack the HCP S32 Nodes. This section describes how to rack the HCP S32 Nodes and connect them to the PDUs.

Rack the HCP S32 Nodes

Rack the HCP S32 Nodes in the rack.

For more information about which rack units to rack the HCP S32 Nodes in, see [Considerations for HCP racking and PDU connections \(on page 30\)](#).

For more information about HCP S32 Node racking, see [Considerations for racking nodes \(on page 42\)](#).



Note: Do not add the same number of nodes, or more nodes, than you have in your cluster; otherwise, it causes a node outage due to metadata rebalancing.

Connect the HCP S32 Nodes to the PDUs

Connect the power cables of the HCP S32 Nodes to the PDUs.

For more information about which PDU outlets to plug the power cables of each HCP S32 Node into, see [Considerations for HCP racking and PDU connections \(on page 30\)](#).

Rack the HCP O12 Nodes

This section describes how to rack the HCP O12 Nodes and connect them to the PDUs.

If you are building an HCP O12 system in a base configuration with optional expansion racks, the HCP O12 Nodes are the first components to be racked. A base configuration supports up to 80 HCP O12 Nodes.

If you are racking an HCP O12 system in an appliance configuration, all of the other storage components need to be installed in the rack before you rack the HCP O12 Nodes. An appliance configuration supports up to six HCP O12 Nodes in the rack.

For more information about which rack units to rack the HCP O12 Nodes, see [Considerations for HCP racking and PDU connections \(on page 30\)](#).



Note: Do not add the same number of nodes, or more nodes, than you have in your cluster; otherwise, it causes a node outage due to metadata rebalancing.

Separate the inner and outer server rails

A server rail kit consists of two sets of inner and outer rails. The rails are universal; that is, each set of rails can be used for either the left or right side of the server.

In a new server rail kit, the inner rails are nested inside the outer rails. You need to separate them so that you can attach the inner rails to the server and the outer rails in the rack.

The following figure shows an inner rail nested inside an outer rail.



The following figure shows the inner and outer rails separated from each other. The outer rail is on top.



The word Front is stamped on the top and bottom lips of each outer rail at the front of the rail. The word BACK is stamped on the top and bottom of each rail at the rear of the rail.



At the rear of each outer rail, the letter L is stamped on one lip and the letter R is stamped on the other lip. With the letter L facing up, the rail goes on the left side of the rack, when viewed from the front of the rack. With the letter R facing up, the rail goes on the right side of the rack.

Procedure

1. Slide the inner rail out of the outer rail toward the front until it locks into place. The inner part of the outer rail slides also slides out.
2. While pulling forward the white tab on the side of the inner rail that faces the outer rail, slide the inner rail forward to release it from the outer rail. Then slide the inner rail all the way out of the outer rail.



3. Slide the inner part of the outer rail back into the outer rail. To do this, while pressing down on the metal tab on the inner part of the outer rail, slide the inner part toward the back to release it. Then slide the inner part all the way back into the outer rail.



Attach the inner rails to the server

The two inner rails in the server rail kit attach to the sides of the server. Each rail can attach to either side of the server.

Procedure

1. Position the rail on the side of the server so that the white tab on the rail faces out and the studs on the server fit into the holes in the rail.



2. While pushing the rail against the server, slide the rail toward the back of the server until the rail locks into place.

Install the outer server rails in the rack

The two outer rails in the server rail kit attach to the sides of the rack. Each rail can attach to either side of the rack.

The outer rails are installed in the lower of the two rack units the server will occupy. For example, if the server will occupy rack units 37 and 38, the outer rails are installed in rack unit 37.

Procedure

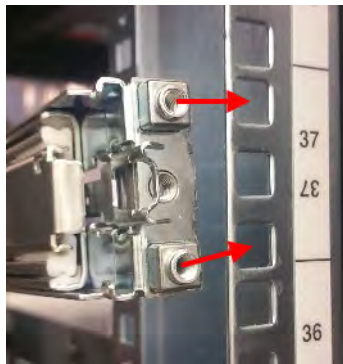
1. At the rear of the rack, with the inside of the outer rail facing into the rack, align the two square studs at the rear of the rail with the back of the top and bottom square holes for the applicable rack unit in the vertical mounting rail.



2. Fit the studs into the holes in the vertical mounting rail and pull the outer rail toward the rear of the rack until the back of the outer rail locks into place.



3. At the front of the rack, align the two square studs at the front of the outer rail with the back of the top and bottom square holes for the applicable rack unit in vertical mounting rail.



4. Fit the studs into the holes in the vertical mounting rail and pull the outer rail toward the front of the rack until the front of the outer rail locks into place.



Mount the server in the rack

Procedure

1. Ensure that the inner part of each outer rail for the server is pushed all the way back into the rack.
2. At the front of the rack, align the rear of the inner rails on the server with the front of the outer rails on the rack.
3. Fit each inner rail into the inside of the inner part of the corresponding outer rail. Then push the server back into the rack as far as the server goes.

4. While pushing back or pulling forward the purple tabs on the outsides of both inner rails on the server, push back on the server to release it. Then slide the server all the way back into the rack.



5. Using the #1 Phillips screwdriver, screw in the black locking screw below the handle on each side of the front of the server.



Attach the HCP O12 service tag

Each HCP O12 system is identified with a system serial number. This serial number is printed on a white rectangular service tag that needs to be affixed to the rear of the appliance or base rack. Service tags are not applied to expansion racks.

Facing the front of the HCP O12 enclosure, the service tag is applied to the bottom left of the front side of appliance or base racks.



Procedure

1. Locate the area where the service tag is to be applied and clean it.
The surface needs to be dry. If you feel it's necessary, use alcohol to clean the surface.
2. Remove the service tag from the backing liner without touching the adhesive side.
3. Attach the service tag by sticking it on the rack and sliding your finger across it from left to right.

Connect the HCP O12 Nodes to the PDUs

Connect the power cables of the HCP O12 Nodes to the PDUs.

For more information about which PDU outlets to plug the power cables of the switches into, see [Considerations for HCP racking and PDU connections \(on page 30\)](#).

Install front-end connectivity options

You can order optional hardware to connect your HCP O12 Nodes to your internal network. Connect the switches to the front-end network based on the hardware you ordered.

Rack the Ethernet switches

Cisco Catalyst C1200 and Cisco Nexus C93180YC-FX3 switches are the only Ethernet switch back-end switches that can be ordered with the HCP O12 system. When you rack the Ethernet switches, they must be installed facing the back of the racks. When mounting a pair of switches, mount the lower one first and the upper one second.

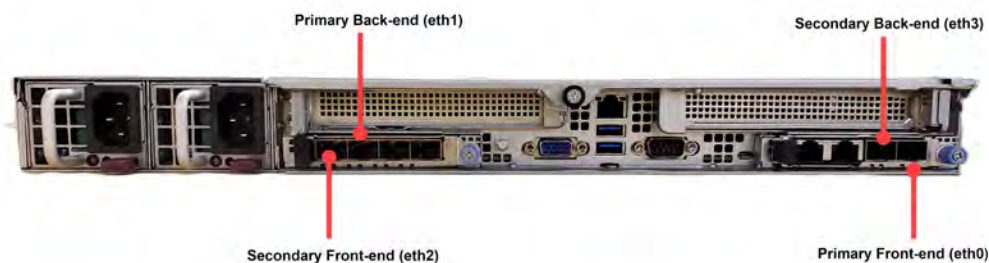


Note: When racking and mounting switches, this manual assumes you are using M5 caged nuts and screws. If you intend to use a different type of caged nut or screw, provide your own variant for the procedure.

HCP O12 Node 1G and 10G port diagrams

For HCP systems with 1G (Cisco Catalyst C1200) or 10G back-end switches (Cisco Nexus C93180YC-FX3), the HCP O12 Node Ethernet ports can be set up for 1Gbe or 10GbE back-end configurations, respectively.

In the following figure, the ports labeled Primary denote the primary port of the back-end network, which should be connected to the Cisco Catalyst C1200 switch in rack position U27, or the Cisco Nexus C93180YC-FX3 switch in rack position U27, or the Cisco Nexus C93180YC-FX3 switch in rack position U37. The ports labeled Secondary denote the secondary port of the back-end network, which should be connected to the Cisco Catalyst C1200 switch in rack position U28, or the Cisco Nexus C93180YC-FX3 switch in rack position U28, or the Cisco Nexus C93180YC-FX3 switch in rack position U39.



(Optional) Install the blanking plates

If there are unused rack units in the rack, you need to cover the empty spaces with blanking plates. The blanking plates are solid plastic pieces that snap onto the front of the rack. Each blanking plate covers one rack unit.



Procedure

1. Hold the plate up to the rack unit.
The blanking plate edges should cover the square holes on the sides of the rack in the rack unit.



2. Gently press on the sides of the blanking plate until it snaps into place.

Reassemble the racks

Using Velcro straps and/or cable ties, bundle any excess length of the cable harnesses and power cords and secure them to the racks. Then replace the doors and sides on the racks.

Chapter 4: Connecting the HCP system at your site

A preassembled HCP with internal storage system arrives with its internal physical connections complete:

- The nodes are connected to the back-end switches.
- The back-end switches are connected to each other.
- All the components are plugged into the PDUs.

For a system ordered without a rack, the instructions in [Mounting unracked components \(on page 29\)](#), tell you how to make all the internal connections.

To get the system up and running in your environment, you need to make the external physical connections. You need to connect:

- The PDUs to the power sources
- The HCP system to your corporate network

This chapter provides instructions for these activities.

Connecting to the power sources

An HCP with internal storage system includes four PDUs. Each PDU has a fixed power cable of the applicable type for the location for which the system was ordered.

A system that includes more than twelve nodes or that has a front-end connection uses all four PDUs.



Note: Depending on the components included in an HCP with internal storage system that you assemble yourself, you may choose to have only two PDUs in the rack.

Each node in an HCP with internal storage system is connected to two PDUs.

You need to connect each PDU to a different power source at your site. If possible, these should be uninterruptible power sources (UPSs).



Important: Before connecting the PDUs to the power sources, ensure that all the power cables connecting the system components to the PDUs are firmly seated at both ends. These can sometimes come loose during shipping.

After you've connected the PDUs to the power sources, you can power on the nodes. The switches power on automatically when the PDUs are connected to the power sources.

Connecting to your corporate network

An HCP with internal storage system should be connected to your corporate network through two front-end switches or through a single front-end switch using active/active bonding. You need to use the Ethernet cables you supply to connect each of these switches to a separate Ethernet switch in your corporate network.

If you configured the HCP system to support a management network, your node management ports should be connected to your front-end switches. The management network segregates system and tenant administration, management API, SNMP, syslog, outgoing SMTP, and SSH traffic from the [hcp_system] network.

There are different types of cables and adapters that can be used to configure a front-end connection. The possible cable types are:

Fiber optic cables

The cables used with optical transceivers.

Twinax cables

The cables used with 10G SFP+ to 1G RJ-45 adapters.

The possible adapter types are:

Optical transceivers

The transceivers should be installed into the front-end ports of each HCP O12 Node.

10G SFP+ to 1G RJ-45 adapters

The adapters connect 10G SFP+ ports to a 1G network. The adapters should be installed into the front-end ports of each HCP O12 Node. These should not be confused with the single adapter provided with all 10G systems that is used by support personnel to perform switch maintenance.

To connect your system to the corporate network you need to cable your front-end switches to the nodes. An HCP O12 Node can have multiple network configurations.



Important: The default front-end IP addresses for the HCP O12 Nodes are 192.168.100.101, 192.168.100.102, and so forth. If these IP addresses don't work for your computing environment, you need to change them before you connect the HCP O12 Nodes to your corporate network. For information about doing this, see [Reconfiguring the HCP system for your site \(on page 53\)](#).



Note: Make sure that you connect to your front-end switches, not your back-end.

Chapter 5: Reconfiguring the HCP system for your site

To reconfigure an HCP system for your computing environment, you need to:

- Verify that the serial number is correct in the system and, if it isn't, rectify it.
- Change the HCP network settings to match your computing environment.
- Change the HCP DNS setting to match your computing environment.
- Change the time setting for the HCP system to match your computing environment.
- Make the back-end switches known to HCP.
- Obtain and install exclusive Support access credentials for SSH if SSH is used in your computing environment.

To perform these activities, you must use the HCP System Management Console. This chapter explains how to:

- Give yourself a System Management Console user account with the service role.
- Perform the reconfiguration activities listed above.



Note: To perform the reconfiguration activities in this chapter before connecting the HCP system to your corporate network, you need to use a computer directly connected to one of the back-end switches.



Important: This chapter describes activities to be performed when you set up the HCP system at your site. Before performing these activities at any other time, consult your authorized HCP provider.

Preparing to reconfigure the system

To reconfigure an HCP system for your computing environment, you must create a user account that has the service role.



Tip: Do not create additional user accounts and roles until you are sure the HCP system is fully operational.

For more information about user accounts and roles, see *Administering HCP*.

Connect to the HCP default back-end network

For using the HCP System Management Console, you need a client computer with connectivity to the default back-end subnet to which the HCP nodes belong. Following is a workflow for connecting a client computer to this subset:

Procedure

1. Ensure that the client computer has a physical connection to one of the back-end switches used by the HCP system.
2. If the client computer is not in the HCP default back-end subnet:
 - a. Make a note of the current IP address and subnet mask for the client computer so you can reset them after you change the network settings for the HCP system.
 - b. On the client computer, set the IP address for the local area network to 10.1.1.100.
 - c. On the client computer, set the subnet mask to 255.255.255.0.

Log in with the initial user account

Procedure

1. Open a browser window, on a computer connected to the HCP back-end network.
2. In the address field, enter:
 - a. `https://10.1.1.101:8000`
The IP address in this URL is the preconfigured back-end IP address of one of the nodes in the HCP system.
3. When prompted, accept the HCP SSL server certificate temporarily for the current session.
The System Management Console login page appears.
4. In the **Username** field, type this case-sensitive username: `security`.
5. In the **Password** field, type this case-sensitive password: `Chang3Me!`
6. Click the **Log In** button.
The Console displays the **Change Password** page.
7. On the **Change Password** page:
 - a. In the **Existing Password** field, type: `Chang3Me!`
 - b. In the **New Password** field, type a new password for the security account.
Passwords must be from six through 64 characters long. They are case sensitive and contain any valid UTF-8 characters, including white space. The minimum password length is six characters.
To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.
 - c. In the **Confirm New Password** field, type the new password again.



Tip: Remember this password. You will need it later to set up additional user accounts. For more information about setting up user accounts, see *Administering HCP*.

8. Click the **Update Password** button.

Check the health of the HCP system

Following is a workflow to ensure that the HCP system is running properly.

Procedure

1. In the top-level menu of the HCP System Management Console, click **Hardware**.
2. On the **Hardware** page, for each node, check that:
 - a. The node status is *Available*
 - b. The status of each logical volume is *Available*



Tip: To see the status of a logical volume, hover over the volume icon.

If all the nodes and logical volumes are available, you can safely continue with the HCP system reconfiguration.

If any nodes have a status other than *Available* or if any logical volumes for available nodes have a status other than *Available*, please contact your authorized HCP service provider for help. Also contact your service provider if the number of logical volume icons for each node does not match your expected number of logical volumes for the node.

Create a service account

Following is a workflow to create a user account to reconfigure the HCP system, in the HCP System Management Console:

Procedure

1. In the top-level menu, select **Security > Users**.
2. On the **Users** page, click **Create User Account**.
3. In the **Create User Account** panel:
 - a. In the **Username** field, type a username for the user account.
Usernames must be from one through 64 characters long and may contain any valid UTF-8 characters. It cannot start with an opening square bracket ([). White space is allowed.
 - b. In the **Full Name** field, type a full name for the user account.
This name must be from one through 64 characters long and may contain any valid UTF-8 characters, including white space.
 - c. In the **Password** field, type a password for the user account.
Passwords must be from six through 64 characters long. They are case sensitive and contain any valid UTF-8 characters, including white space. The minimum password length is six characters. To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.
 - d. In the **Confirm Password** field, type the password again.



Note: Remember this password. You will need it for the reconfiguration activities in this chapter.

- e. In the **Roles** section, select **Service**.
4. Click the **Create Account** button.
5. In the upper right corner of the console, click **Log Out**.
The console returns to the login page.

Log in with the service account

Now that you've created a user account with the service role, you can use that account to log into the HCP System Management console and perform system reconfiguration activities. This time, when you log in, the console displays the Overview page.



Caution: The service role lets you take additional actions that are not described in this book. Some of these actions can have a significant impact on the HCP system. Before taking any other service role actions, be sure you understand their consequences.



Tip: After you complete the last reconfiguration activity, log out of the System Management console and close the browser window to ensure that no one can return to the console on your computer without a fresh login.

Verify the serial number

Following is a workflow designated to verify, and if necessary, change the serial number in the HCP system configuration.

Before you begin

Each HCP system is assigned a unique five-digit serial number. With a preassembled system, this number is on a label that's attached to the side of the system rack at the bottom, just inside the left rear door. With a rackless system, this number is on a label taped to the top of the first node you mount when you assemble the system. When the HCP system software is installed, the serial number is entered as part of the system configuration. You need to verify that the serial number in the system configuration matches the serial number of the label attached to the rack. If the serial numbers don't match, you need to change the serial number in the system configuration.

Procedure

1. Select **Configuration > Miscellaneous** from the top-level menu of the System Management Console.
2. Verify that the serial number in the **Serial Number from Rack Label** field is the same as the serial number on the label delivered with the system.
3. If the serial numbers are not the same:
 - a. In the **Serial Number from Rack Label** field, type the serial number from the label attached to the rack.
 - b. Click **Update Settings**.

Changing the network settings

The HCP system is installed with default network settings. You need to change these settings to match your computing environment.

Before you begin

Following is the workflow you need to know before you begin:

- The IP address to use for the front-end gateway router. Typically, the first three octets in this address are the same as the first three octets in the IP address of the front-end network.
- The subnet mask for the front-end IP addresses.
- If the corporate network is configured to support virtual networking and you want to tag the HCP front-end network, the VLAN ID to use for that network. For information about virtual networking, see *Administering HCP*.
- The front-end IP address to use for each HCP node.



Note: Node numbers don't change when you change IP addresses.

- Whether HCP must hide the IP addresses of the master name servers for the front-end network and allow client access to HCP over the network only through specified downstream DNS servers. A DNS configuration that functions in this way is called hidden master.

A downstream DNS server is a DNS server through which client requests are routed to HCP.

For more information about this and the next two properties, see *Administering HCP*.

- Whether HCP should notify specified downstream HCP servers about changes to the zone definition for the front-end network.
- The rate at which the downstream DNS servers should query HCP for updates to the zone definition for the front-end network domain. The default is three hours.

For the refresh rate for the [hcp_system] network, you can specify any combination of weeks (W), days (D), hours (H), minutes (M), and seconds (S), using this syntax:

```
#W#D#H#M#S
```

- The back-end IP address to use for each HCP node. You can change only the first three octets of the back-end IP addresses. You cannot change the fourth octet.



Important: Change the default back-end IP addresses only if they conflict with existing front-end IP addresses at your site.

After you've made all the necessary changes to the front-end and back-end network settings, you can safely connect the HCP system to your corporate network.

Changing the front-end network settings

Procedure

1. In the top-level menu of the System Management Console, select **Configuration > Networks**.
2. In the list of networks on the **Networks** page, click **[hcp_system]**.
3. In the panel for the **[hcp_system]** network:
 - Type the new IP address, in the **Gateway** field, to change the gateway IP address.
 - Type the new subnet mask, to change the subnet mask, in the **Netmask** field.
 - Select the **Make tagged network** option to make the front-end network tagged. Then, in the **VLAN ID** field, type a unique VLAN ID for the network. Valid values are integers in the range one through 4,095.
 - Click the **Downstream DNS Configuration** to change the DNS settings for the network. Following is the workflow for this process.
 - To enable or disable hidden master, select or deselect, respectively, the **Enable hidden master** option.
 - To enable or disable hidden master, select or deselect, respectively, the **Enable hidden master** option.
 - To enable or disable notify, select or deselect, respectively, the **Enable Notify** option.
 - If you are enabling hidden master or notify, in the **Downstream DNS Servers** field, type a comma-separated list of the IP addresses of one through ten downstream DNS servers. Spaces are not allowed.
 - To change the refresh rate, in the **Refresh Rate** field, type the new refresh rate. For valid values for the refresh rate, see "[Changing the network settings](#)" (on [page 57](#)).
 - To change the node IP addresses, in the **Node IP Addresses** section, type a new front-end IP addresses for the nodes in the HCP system.



Note: Do not change the value in the **MTU** field.

4. Click **Update Settings**.
A warning message appears asking you to confirm the changes you've made.
5. In the field in the message window, type **YES**. This is case sensitive.
6. Click **Update Settings**.
The HCP system restarts with the new settings. This takes a few minutes.
7. If you do not need to change the back-end settings, you can now safely connect the HCP system to your corporate network
8. Log back into the System Management console after the system restarts. Then proceed to the configuration activity.

Changing the back-end network settings

Procedure

1. In the top-level menu of the System Management Console, select **Configuration > Networks**.
2. In the list of networks on the **Networks** page, click **[hcp_backend]**.
3. In the **Node IP Addresses** section in the **[hcp_backend]** panel, type new back-end IP addresses for the nodes in the HCP system.



Important: Do not change the values of the **Multicast Address or Netmask** field.

4. Click the **Update Settings** button.
A warning message appears asking you to confirm the changes you've made.
5. In the field in the message window, type **YES**. This is case sensitive.
6. Click the **Update Settings** button.
The HCP system restarts with the new settings. This takes a few minutes.

Changing the back-end IP addresses

Procedure

1. Change the IP address of the client computer to match the new HCP back-end subnet.
2. Change the IP address of the HCP system switches to match the new HCP back-end subnet.
3. Change the IP address of the HCP system SNMP trap receiver addresses to match the new HCP back-end subnet.
4. Log into the System Management console again after the system restarts. Remember to use one of the new back-end IP addresses in the console URL.

Changing DNS settings

For the HCP system to use DNS services, you need to enable the use of DNS in HCP and specify the IP addresses of all the DNS servers in your environment that are upstream from HCP. An upstream DNS server is a DNS server to which HCP routes the outbound communications it initiates (for example, for sending log messages to syslog servers or for communicating with Active Directory®).

Specifying all the DNS servers ensures that the HCP system can be addressed by hostname as long as at least one of those servers is available. To specify the DNS servers, you need to know their IP addresses.



Note: If you have not yet configured HCP as a subdomain in the DNS, do so now. For information about doing this, see *Administering HCP*.

When changing DNS settings, you can also change the hostname prefix used to name the nodes in the HCP system. You need to do this if you have two HCP systems and:

- You use Active Directory authentication for access to HCP
- The two systems have one or more node numbers in common

If you don't use DNS at your site, you need to disable the use of DNS in HCP.

Procedure

1. In the top-level menu of the System Management Console, select **Configuration > DNS**.
2. On the **DNS Settings** page:
 - If you want to use DNS with HCP, select the Use DNS option.
 - If you don't want to use DNS with HCP, deselect the Use DNS option and skip to step 4.
 - a. Optionally, in the **Hostname Prefix** field, type a new hostname prefix.
The hostname prefix can be from one through 12 characters long and contain only lowercase letters, numbers, and hyphens (-).

Tip: To make node names easier to read, end the hostname prefix with a hyphen (-).

 - b. In the **Upstream DNS Servers** field, type a comma-separated list of the IP addresses of all the upstream DNS servers.
Spaces are not allowed.
3. Click the **Update Settings** button.
A warning message appears asking you to confirm the changes you have made.
4. In the message window field, type `yes`. This is case sensitive.
5. Click the **Update Settings** button.
The System Management Console confirms that you have successfully updated the DNS settings, and HCP restarts. Wait a few minutes for the system to finish restarting. Then proceed to the next reconfiguration activity.

Changing time settings

If you choose to use external time servers, you need to know the IP addresses or hostnames of these servers.



Note: For you to specify an external time server, the HCP system must have connectivity to the time server through the front-end network.

In any case, you need to know the time zone you want HCP to use. It stores all times (such as creation dates and retention settings) in Coordinated Universal Time (UTC) and uses its time zone setting only for presentation purposes.



Note: HCP systems can be configured not to allow changes to time settings through the System Management console. If your system is configured this way, you cannot make the changes described in this section.

To change time-settings for the HCP system:

Procedure

1. In the top-level menu of the System Management Console, select **Configuration > Time**.
2. On the **Time Settings** page:
 - Optionally, in the **Time Servers** field, type a comma-separated list of the IP addresses or hostnames of one or more time servers. Spaces are allowed.
 - Optionally, if the time source is internal, in the **Current Time** field, type the current time. The format for the time is MMDDhhmmYYYY, where MM is the two-digit month, DD is the two-digit day, hh is hours on a 24-hour clock, mm is minutes, and YYYY is the four-digit year. The time you specify cannot be more than one year in the future or 23 hours and 45 minutes in the past. If the time source is internal and you leave this field blank, the current system time doesn't change.
 - Optionally, in the **Time Zone** field, select the new time zone.
3. Click the **Update Settings** button.
A warning message appears asking you to confirm the changes you have made.
4. In the field in the message window, type **YES**. This is case sensitive.
5. Click the **Update Settings** button.
The console confirms that you have successfully updated the time settings, and HCP restarts. Wait a few minutes for the system to finish restarting. Then proceed to the next reconfiguration activity.

Making the back-end switches known to HCP

You can choose to have HCP report the status of the back-end switches in the System Management Console. For HCP to do this, you need to make each switch known to HCP. You do this by telling HCP about the model and IP address of the switch.

By default, the IP addresses of all back-end switches, regardless of manufacturer, are shown in the following table.

Table 3 Default IP addresses for all back-end switches

Switch type	Default IP address for switch A	Default IP address for switch B
Ethernet	10.1.1.252	10.1.1.253
Fibre Channel	10.1.1.250	10.1.1.251

If you changed the back-end IP addresses of the HCP nodes, the switch IP addresses need to change as well. For help with this, contact your authorized HCP service provider.

Procedure

1. In the top-level menu of the System Management Console, select **Configuration > Monitored Components**.
2. On the **Monitored Components** page, for each switch:
 - a. Click **Add**.
A new row appears in the **Components** list. If you inadvertently add an extra row, click the **Delete control** for the row to remove it.
 - b. In the **Model** field in the new row, select the model of the switch that's supplied with the system.
 - c. In the **IP Address** field, type a valid IPv4 address for the switch.
3. Click **Update Settings**.

Using SSH to access an HCP node

When access to an HCP node through the HCP System Management Console or management API is not possible, authorized service providers can use SSH login to access the node.



Note: If SSH is used at the customer site, all SSH keys for a node are updated when Java Virtual Machine starts on the node. The same is true when nodes are swapped.



Important: By default, SSH login is disabled. Disabling SSH enhances security, but also increases the amount of time required for an authorized service provider to diagnose and resolve issues. For information, see [Enabling SSH](#).

Uploading exclusive support access credentials

Obtain the SSH support credentials from the HCP distributor or Hitachi Vantara customer support.

Procedure

1. On the **Security** menu, select **Support Access Credentials**
2. Click **Upload Support Access Credentials**, and then click the **Choose File** button.
3. In the dialog box, go to the location where the exclusive Hitachi Vantara Support Access Credentials key package file is located, and double-click the file.
4. Click the **Next** button. The new SSH keys are uploaded from the key package, validated, and then a review screen asks you to confirm the package to install. (If the package cannot be validated, a message appears and you can try again with a different file.)

5. Review the information on the page.
 - If the information is correct, click **Next**. The procedure validates the package you selected and applies the new set of SSH keys to the system.
 - If the information is incorrect, click **Cancel**. The procedure is cancelled.
6. Verify that the system event is generated in **Monitoring > System Events** to confirm that the key package was applied successfully.

BMC administrative credentials

As part of the HCP onsite setup, the administrative credential associated with each HCP system's baseboard management controller (BMC) must be updated. To perform the update, contact your HCP service provider.

Configuring the BMC to monitor servers

You can configure the HCP system baseboard management controller (BMC) to your corporate network to monitor the health of your servers. If you want to enable this feature, contact your HCP sales representative.

Chapter 6: Configuring HCP monitoring with Hitachi Remote Ops

Hitachi Remote Ops is a Hitachi Vantara LLC product that enables remote monitoring of the nodes in an HCP system. With Hitachi Remote Ops, you can view the status of these components in a web browser. You can also configure Hitachi Remote Ops to notify you by email of error conditions as they occur. Additionally, you can configure Hitachi Remote Ops to report error conditions to Hitachi Remote Ops support personnel. It is recommended to set up Hitachi Remote Ops on all new HCP systems.

Hitachi Remote Ops is for monitoring and error notification purposes only. It does not allow any changes to be made to the system.

Hitachi Remote Ops is installed on a server that is separate from the HCP system. The program uses SNMP to retrieve information from HCP, so SNMP must be enabled in HCP.



Note: HCP supports IPv4 and IPv6 network connections to Hitachi Remote Ops servers. However, Hitachi Remote Ops support for IPv6 network connections varies based on the Hitachi Remote Ops server operating system. For information about requirements for Hitachi Remote Ops servers that support IPv6 networks, see the applicable Hitachi Remote Ops documentation.

This chapter explains how to set up monitoring of HCP nodes with Hitachi Remote Ops .

The chapter assumes that Hitachi Remote Ops is already installed and running according to the documentation that comes with the product.

Enabling SNMP in HCP

To enable Hitachi Remote Ops to work with HCP, you need to enable SNMP in the HCP System Management Console. When you enable SNMP, you can select version 1 or 2c or version 3.

By default, Hitachi Remote Ops is configured to support SNMP version 1 or 2c with the community name public. If you change the community name in HCP or if you select version 3, you need to configure a new SNMP user in Hitachi Remote Ops to match what you specify in HCP. For more information about this, see the Hitachi Remote Ops documentation.

Once SNMP is enabled, the first four nodes in the HCP system monitor for switch SNMP traps. If there are more than four HCP nodes in the system, additional HCP node back-end addresses can be added to the SNMP trap receivers list on the back-end switches. For more information about adding extra nodes back-end address to the SNMP trap receivers list, contact your HCP customer support.

To enable SNMP in HCP for use with Hitachi Remote Ops:

Procedure

1. Log into the HCP System Management Console using the initial user account, which has the security role.
2. In the top-level menu of the System Management Console, select **Monitoring > SNMP**.
3. In the **SNMP Settings** section, on the **SNMP** page:
 - a. Select the **Enable SNMP** at `snmp.hcp-domain-name` option.
 - b. Select either **Use version 1 or 2c** (recommended) or **Use version 3**.
 - c. If you select **Use version 3**, specify a username and password in the **Username**, **Password**, and **Confirm Password** fields.
 - d. Optionally, in the **Community** field, type a different community name.
4. Click the **Update Settings** button.
5. In the entry field in the **Allow** section, type the IP address that you want HCP to use to connect to the server on which Hitachi Remote Ops is installed. Then click the **Add** button.
6. Log out of the System Management Console and close the browser window.

Configuring Hitachi Remote Ops

Procedure

1. Log in to Hitachi Remote Ops.
2. Set the Hitachi Remote Ops base configuration. Include the email addresses where error conditions (if they occur) will be sent.
3. (Optional) Configure transport agents for reporting error conditions to Hitachi Vantara support personnel.
4. Identify the HCP system to be monitored.

Step 1: Log in to Hitachi Remote Ops

To log in to Hitachi Remote Ops:

Procedure

1. Open a web browser window.
2. In the address field, enter the URL for the Hitachi Remote Ops server by using either the hostname or a valid IP address for the server followed by port number 6696. For example:

```
http://hitrack.6696
```

3. In the **Select one of the following UserIds** field, select **Administrator**.

4. In the **Enter the corresponding password field**, type the case-sensitive password for the Administrator user. By default, this password is *hds*.
If Hitachi Remote Ops is already in use at your site for monitoring other devices, this password may have been changed. In this case, see your Hitachi Remote Ops administrator for the current password.
5. Click **Logon**.

Set the base configuration

The Hitachi Remote Ops base configuration specifies information such as the customer site ID, how frequently to scan devices, and whether to report communication errors that occur between Hitachi Remote Ops and monitored services. The Hitachi Remote Ops base configuration specifies information such as the customer site ID, how frequently to scan devices, and whether to report communication errors that occur between Hitachi Remote Ops and monitored devices. The base configuration also specifies the addresses to which Hitachi Remote Ops should send email about error conditions.

If Hitachi Remote Ops is already in use at your site, the base configuration may already be set. In this case, you can leave it as is, or you can make changes to accommodate the addition of HCP to the devices being monitored.

To set the Hitachi Remote Ops base configuration:

Procedure

1. In the row of tabs at the top of the Hitachi Remote Ops interface, click **Configuration**.
The Base page is displayed by default. To return to this page from another configuration page, click **Base** in the row of tabs below Configuration.
2. (Optional) In the **Device Monitoring** section:
 - a. Type your Hitachi Vantara customer ID in the **Site ID** field.
 - b. Specify different values in the other fields to meet the needs of your site. For information about these fields, click the **Help on this table's entries** link above the fields.
3. In the **Notify Users by Email** section:
 - a. In the **eMail Server** field, type the fully qualified hostname or a valid IP address of the email server through which you want Hitachi Remote Ops to send email about error conditions.
 - b. In the **Local Interface** field, select the Ethernet interface that has connectivity to the specified email server. This is the interface on the Hitachi Remote Ops server.
 - c. In the **User List** field, type a comma-separated list of the email addresses to which Hitachi Remote Ops must send email about error conditions.
 - d. In the **Sender's Email Address** field, type a well-formed email address to be used in the From line of each email.

Some email servers require that the value in the From line be an email address that is already recognized by the server.
4. Click the **Submit** button.
5. Optional: Click the **Test Email** button to send a test email to the specified email addresses.

Configure transport agents

A Hitachi Remote Ops transport agent transfers notifications of error conditions to a target location where Hitachi Vantara support personnel can access them. The transfer methods available are HTTPS, FTP, or dial up. For the destinations for each method, contact your authorized HCP service provider.

You can specify multiple transport agents. Hitachi Remote Ops tries them in the order in which they are listed until one is successful.

To configure a transport agent:



Note: This is a conditional task.

Procedure

1. In the row of tabs below **Configuration**, click **Transport Agents**.
2. In the field below **Data Transfer Agents**, select the transfer method for the transfer agent.
3. Click the **Create** button. The new transport agent appears in the list of transport agents. A set of configuration fields appears below the list.
4. In the configuration fields, specify the applicable values for the new transport agent. For information about what to specify, see the Hitachi Remote Ops documentation.
5. Click the **Submit** button. You can change the order of multiple transport agents by moving them individually to the top of the list. To move a transport agent to the top of the list:
 - a. In the **Move to Top?** column, select the transport agent you want to move.
 - b. Click the **Submit** button.

Step 4: Identify the HCP system

To identify the HCP system to be monitored:

Procedure

1. In the row of tabs at the top of the Hitachi Remote Ops interface, click **Summary**.
The Summary page displays up to four tables that categorize the devices known to Hitachi Remote Ops: Device Errors, Communication Errors, Devices Okay, and Not Monitored. To show or hide these tables, click the check boxes below the table names at the top of the page to select or deselect the tables, as applicable. Then click **Refresh**.
While no tables are shown, the page contains an **Add a Device** link.
2. Take one of the following actions:
 - If the **Summary** page doesn't display any tables, click the **Add a device** link.
 - If the **Summary** page displays one or more tables, click the **Item** column heading in any of the tables.
3. In the **Select Device Type** field, select **Hitachi Content Platform (HCP)**. A set of configuration fields appears.

4. Optionally, in the **Name** field, type a name for the HCP system.
The name can be from one through 40 characters long. Special characters and spaces are allowed. Typically, this is the hostname of the system.
5. Optionally, in the **Location** field, type the location of the HCP system.
The location can be from one through 40 characters long. Special characters and spaces are allowed.
6. Optionally, in the **Group** field, type the name of a group associated with the HCP system (for example, "Finance Department").
The group name can be from one through 40 characters long. Special characters and spaces are allowed.
7. In the **Site ID** field, type your Hitachi Vantara customer ID.
If you don't know your customer ID, contact your authorized HCP service provider for help.
8. In the **IP Address or Name (1)** field, type a valid front-end IP address for the lowest-numbered storage node in the HCP system. In the **Local Interface** field, leave the value as **any**.
9. In the **IP Address or Name (2)** field, type a valid front-end IP address for the highest-numbered storage node in the HCP system. In the **Local Interface** field, leave the value as **any**.
10. In the **SNMP Access ID** field, select the SNMP user that corresponds to the SNMP configuration in HCP.
Typically, this is **public**.
11. In the **Comms Error Reporting** field, select one of these options to specify whether Hitachi Remote Ops must report communications errors that occur between Hitachi Remote Ops and the HCP system:
 - **Yes:** Report communication errors
 - **No:** Don't report communication errors
 - **Local:** Report communication errors only to the email addresses specified in the base configuration and not through the specified transport agents.
 - **Default:** Use the setting in the base configuration.
12. Leave **Enabled** selected.
13. Leave **Trace** unselected.
14. Click **Add**.
If the operation is successful, the interface displays a message indicating that the HCP system has been added. Do not click **Add** again: Doing so will add the system a second time.

Chapter 7: Configuring DNS for HCP

Domain name system (DNS) is a network service that translates or resolves domain names (for example, example.com) into IP addresses for client access. The service is provided by one or more servers, called name servers, that share responsibility for resolving client requests.

An HCP system can exist as multiple domains in the DNS — one for each front-end network defined in the system. Each of these domains must be a subdomain of a DNS domain to which you have administrative access, such as your corporate domain. All nodes that have IP addresses defined for a given front-end network belong to the HCP domain defined for that network.



Note: If you enable the management network, you cannot access your front-end network through DNS unless you create secondary zones for the management network.

To enable access to HCP by domain name on any given network, you need to configure the HCP domain for that network in your DNS. You can use either secondary zones or stub zones.

Following is the workflow for this chapter:

- A discussion on the advantages of using DNS
- A description of zones, secondary zones, and stub zones
- The instructions for verifying the HCP domain definitions
- DNS considerations for implementing HCP service by remote systems

For information about domains defined in HCP, see *About Domains*. For information about HCP networks, see *About virtual networking with HCP*.



Note: HCP does not require DNS. For information about using HCP without DNS, see *System Management console URL*. When communicating with a DNS server, HCP may send packets that are larger than 512 bytes. Ensure that these packets can pass through your corporate firewall.

DNS advantages

Using DNS provides several advantages over using IP addresses for access to the HCP system. For example:

- When you use a domain name for namespace access, the HCP DNS manager, which runs on all storage nodes, is responsible for distributing client requests among those nodes. If you use IP addresses, you are responsible for ensuring that the processing load is balanced across the HCP nodes.
- If an application uses a domain name for access to the HCP system and you change the IP addresses of the HCP nodes, you don't need to change the application. If the application uses IP addresses and you change the node IP addresses, you need to update the application to specify the new IP addresses.
- If both IPv4 and IPv6 addresses are defined for a front-end network, applications can use the domain name associated with that network to access the HCP system from client computers that have IPv4 addresses and from client computers that have IPv6 addresses. If an application uses IP addresses to access the HCP system over a front-end network with multiple IP addresses defined for each node, you need to configure the application to access the HCP system using only the IP addresses that are routable from the client computer on which the application is running.
- If you use a domain name to identify the other system when you create a replication link and the IP addresses for that domain are changed on that system, replication continues without interruption. If you use IP addresses to identify the system and the IP addresses for the system change, replication stops until you change the IP addresses in the replication link.
- If you use domain names to identify the systems in a replication topology and you enable DNS failover on those systems, client requests can be automatically redirected to other systems in the topology if the target system fails. If you use IP addresses to identify a system in a replication topology and that system fails, client requests targeting that system cannot be automatically redirected to other systems.

Zones

The domain names resolved by DNS are divided into zones, where each zone is defined by a set of related hostnames. A corporate domain, for example, is associated with a zone.

Each domain you define in HCP is a subdomain of a higher-level domain. In the DNS, you need an HCP domain definition for each combination of network and domain you define in HCP. The IP addresses for each HCP domain in the DNS make up a zone within the zone for the applicable higher-level domain.

For example, suppose that you configure HCP to define two domains, *hcpma.example.com* and *hcp-ca.example.com*. Suppose also that you configure HCP to define three user-defined networks, *net1*, *net2*, and *net3*, and you configure these three networks to associate *net1* and *net2* with domain *hcp-ma.example.com* and associate *net3* with domain *hcpca.example.com*. In this case, you need to add three zones to the DNS, one for each of these domain and network combinations:

```
Domain name: hcp-ma.example.com
Node IP addresses defined for network net1
Domain name: hcp-ma.example.com
Node IP addresses defined for network net2
Domain name: hcp-ca.example.com
Node IP addresses defined for nodes in network net3
```

Secondary zones and stub zones

In the DNS, you configure each HCP domain as a secondary zone or as a stub zone. A DNS server in which a given HCP domain is configured as a secondary zone maintains a full copy of the HCP DNS information for that domain and can, therefore, satisfy requests for resolution of the HCP domain name by itself. You might use secondary zones, for example, if the firewall that HCP sits behind is configured to allow client requests for DNS name resolution to go only to a corporate DNS server.

A DNS server in which a given HCP domain is configured as a stub zone gets only partial DNS information for that domain from HCP. Stub zones minimize zone replication and are less resource intensive for the DNS server.

If you enable hidden primary or notify for a network, the HCP domain for that network must be configured as a secondary zone, not a stub zone, on each DNS server specified in the network configuration.

Secondary zone and stub zone definitions are basically the same. Each definition lists the IP addresses of primary name servers for a domain but does not include individual records for those servers. Those records are stored on the primary name servers themselves. The DNS servers get the individual name server records from the primary name servers listed in the zone definition.

For each network defined in HCP, HCP automatically generates name server records for all storage nodes that have IP addresses in that network. Each of those storage nodes stores a copy of these records, thereby making each storage node eligible to be a primary name server for the applicable domain.

Before HCP can accept client requests that identify the system by a domain name, you need to register some or all of the eligible nodes as primary name servers for the applicable HCP secondary zone or stub zone. You register a node by listing its IP addresses in the secondary zone or stub zone definition.

For any given HCP domain, all storage nodes with IP addresses defined for the applicable network can act as name servers for the HCP DNS manager, regardless of whether they're registered as primary name servers. However, for HCP to be accessible over that network, at least one registered node must be running. Therefore, you need to register a sufficient number of nodes for each network to minimize the risk that all registered nodes for a given network will fail at the same time.



Tip: If HCP has a small number of storage nodes, consider registering them all as primary name servers. The more nodes you register, the more distributed the DNS queries will be.

When defining a secondary zone or stub zone for an HCP domain, you specify a fully qualified domain name for the HCP system. This is the name of the domain associated with the network that is defined in HCP.

Configuring an HCP secondary zone or stub zone in Windows

You can use either the GUI or a command line to configure a secondary zone or stub zone in Windows. The following sections present the GUI configuration procedure for Windows. For information about which Windows servers are supported, check the HCP release notes for the version of HCP that you have installed.

Configuring an HCP secondary zone in Windows

Procedure

1. Open the DNS Manager
 - a. In the Windows Control Panel, double-click **Administrative Tools**.
 - b. In the **Administrative Tools** window, double-click DNS.
The **DNS Manager** window shows the hierarchy of zones currently defined in the DNS.
2. In the **DNS Manager** window, right-click **Forward Lookup Zones** under the higher-level zone within which you want to configure the HCP secondary zone. On the dropdown menu, select **New Zone**.
The **New Zone Wizard** window opens.
3. In the **New Zone Wizard** window, click **Next**.
4. On the Zone Type page, select **Secondary zone**. Then click **Next**.
5. In the **Zone name** field on the **Zone Name** page, type the applicable fully qualified domain name for the HCP system. Then click **Next**.
6. On the Master DNS Servers page, for each HCP storage node you want to register as a master name server, in the list box, type the IPv4 and IPv6 addresses assigned to the node for the applicable network. Then press **Enter**.
When you're finished adding all the node IP addresses, click **Next**

7. Click **Finish**.
The new HCP secondary zone appears in the zone hierarchy in the DNS manager window.


Configuring an HCP stub zone in Windows

How to configure an HCP domain as a stub zone in Windows:

Procedure

1. Open the **DNS Manager**:
 - a. In the **Windows Control Panel**, double-click **Administrative Tools**.
 - b. In the **Administrative Tools** window, double-click **DNS**.

The **DNS Manager** window shows the hierarchy of zones currently defined in the DNS.
2. In the **DNS Manager** window, right-click **Forward Lookup Zones** under higher-level zone within which you want to configure the HCP stub zone. On the dropdown menu, select **New Zone**.
The **New Zone Wizard** window opens.
3. In the **New Zone Wizard** window, click **Next**.
4. On the **Zone Type** page, select **Stub zone**.
5. To configure the stub zone with Windows Active Directory integration, take one of these following actions:
 - a. Select **Store the zone in Active Directory**.
 - b. On the **Active Directory Zone Replication Scope** page, select the option for the way in which you want DNS data to be replicated throughout your network.
 - c. Then click **Next**.

 **Note:** You need to configure the stub zone with Windows Active Directory integration if you plan to enable HCP support for AD. For information about doing that, see *Configuring Active Directory or Windows workgroup support*.

 - d. To configure the stub zone without Windows Active Directory integration, click **Next**.
6. In the **Zone name** field on the **Zone Name** page, type the applicable fully qualified domain name for the HCP system. Then click **Next**.
7. On the **Zone File** page, select **Create a new file with this file name** and leave the default file name in the accompanying field. Then click **Next**.
8. On the **Primary DNS Servers** page, for each HCP storage node you want to register as a primary name server, in the list box, type the IPv4 and IPv6 addresses assigned to the node for the applicable network. Then press **Enter**.
When you're adding all the node IP addresses, click **Next**.
9. Click **Finish**.
The HCP new stub zone appears in the zone hierarchy in the DNS manager window.

Configuring an HCP secondary zone or stub zone in Unix

With BIND in Unix, zones are defined in the `/etc/named.conf` file on the DNS servers. In the definition of a secondary zone or stub zone for an HCP domain, you specify:

- The applicable fully qualified domain name for the HCP system
- The zone type (slave for a secondary zone or stub for a stub zone)
- The name of the file you want the system to use to cache DNS query results for a faster lookup
- A list of the IP addresses of the master name servers for the secondary zone or stub zone (be sure to use all of the node IP addresses assigned to each node for the applicable network)

Here's a sample zone statement that defines a secondary zone for an HCP domain with the domain name `hcp-ma.example.com` and four registered master name servers:

```
zone "hcp-ma.example.com" IN {
    type slave;
    file "/var/named/slave/hcp-ma.example.com";
    masters
    {192.168.210.15;192.168.210.16;192.168.210.17;192.168.210.18;2001:0db8::101;
    2001:0db8::102;2001:0db8::103;2001:0db8::104; };
};
```

Here's a sample zone statement that defines a stub zone for the same domain:

```
zone "hcp-ma.example.com" IN {
    type stub;
    file "/var/named/stub/hcp-ma.example.com";
    masters
    {192.168.210.15;192.168.210.16;192.168.210.17;192.168.210.18;2001:0db8::101;
    2001:0db8::102;2001:0db8::103;2001:0db8::104; };
};
```

Verifying the configuration

You can verify that an HCP secondary zone or stub zone is working properly from either a Windows command-prompt window or a Unix shell. In both cases, you use either the `dig` or `nslookup` command, depending on which is available. The syntax for this is:

```
dig|nslookup (admin|nfs|cifs|www).hcp-domain-name
```

The response to this command should be a list of the IP addresses of all the HCP storage nodes that have IP addresses defined for the network for which the secondary zone or stub zone is defined.

Here's an example of the output from the nslookup command when six out of the ten nodes in the network are registered as primary name servers for the secondary zone or stub zone:

```
#nslookup www.hcp-ma.example.com
Server: adc1850.example.com
Addresses: 192.168.80.45
2001:0db8::201
Name: www.hcp-ma.example.com
Addresses: 192.168.210.11, 2001:0db8::101, 192.168.210.12,
2001:0db8::102,
192.168.210.13, 2001:0db8::103, 192.168.210.14, 2001:0db8::104,
192.168.210.15,
2001:0db8::105, 192.168.210.16, 2001:0db8::106, 192.168.210.17,
2001:0db8::107,
192.168.210.18, 2001:0db8::108, 192.168.210.19, 2001:0db8::109,
192.168.210.20,
2001:0db8::10a
```

If you don't see the expected node list, the secondary zone or stub zone is not defined correctly.

DNS considerations for service by remote systems

When you configure a secondary zone or stub zone for an HCP system, you specify a domain name and the IP addresses of the primary name servers for the applicable HCP domain. This causes client requests that identify the system by that domain name to be forwarded to those primary name servers.

Namespaces can be configured to accept client requests on HCP systems other than the system targeted by the request when that system is unavailable. To enable this redirection to occur automatically for a namespace:

- DNS failover must have been enabled on the target system.
- The applicable replication link must be failed over. The applicable replication link is the link between the target system and the system to which requests must be redirected.



Attention: DNS failover affects all the tenants on an HCP cluster. For DNS failover to succeed, all Active-Active and Active-Passive links must fail over to the target system. If the HCP cluster has tenants that are not part of a replication link, or if the tenant is on a replication link that has not failed over, write requests to the tenant and read requests from the tenant fail if the domain name is used in the request. Requests will succeed if the request includes the IP address of the primary cluster instead of the domain name.

- The applicable secondary zone or stub zone for the target system must include the IP addresses of the applicable primary name servers for the system to which requests must be redirected, where:
 - The applicable secondary zone or stub zone on the target system is the one defined for the data network for the tenant that owns the namespace
 - The applicable primary name servers for the system to which requests should be redirected are the ones included in the secondary zone or stub zone for the network with the same name as the tenant data network on the target system

For examples, you may suppose:

- The data network for a tenant is the network named net1.
- The system targeted by a client request has primary name servers with IPv4 addresses 192.168.210.15, 16, 17, and 18 and with IPv6 addresses 2001:0db8::101, 102, 103, and 104 for net1. The system to which requests must be redirected has primary name servers with IPv4 addresses 192.168.24.72, 73, 74, and 75 and with IPv6 addresses 2001:0db8::201, 202, 203, and 204 for net1.
- The system targeted by a client request has primary name servers with IPv4 addresses 192.168.210.15, 16, 17, and 18 and with IPv6 addresses 2001:0db8::101, 102, 103, and 104 for net1. The system to which requests must be redirected has primary name servers with IPv4 addresses 192.168.24.72, 73, 74, and 75 and with IPv6 addresses 2001:0db8::201, 202, 203, and 204 for net1.

In this case, the secondary zone or stub zone for net1 on the target system have these IP addresses:

```
192.168.210.15
    2001:0db8::101
192.168.210.16
    2001:0db8::102
192.168.210.17
    2001:0db8::103
192.168.210.18
    2001:0db8::104
192.168.24.72
    2001:0db8::201
192.168.24.73
    2001:0db8::202
192.168.24.74
    2001:0db8::203
192.168.24.75
    2001:0db8::204
```

Hitachi Vantara



Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact