HITACHI
Inspire the Next

Hitachi Content Platform

Installing an HCP SAIN System — Final On-site Setup

Hitachi Data Systems

MK-98ARC020-16

Contents

Preface

This book is the final on-site setup guide for single-rack **Hitachi Content Platform (HCP)** systems that run on a SAN-attached array of independent nodes (**SAIN**). It provides all the information you need to deploy an assembled and configured HCP SAIN system at your site. Additionally, it explains how to configure Hi-Track® to monitor the nodes in the HCP system.

Intended audience

This book is intended for the people at a customer site who are responsible for the on-site setup of an HCP SAIN system. It assumes you have experience working with computer hardware, as well as a basic understanding of HCP systems.

Product version

This book applies to release 7.1 of HCP.

Related documents

The following documents contain additional information about Hitachi Content Platform:

- *Administering HCP* — This book explains how to use an HCP system to monitor and manage a digital object repository. It discusses the capabilities of the system, as well as its hardware and software components. The book presents both the concepts and instructions you need to configure the system, including creating the tenants that administer access to the repository. It also covers the processes that maintain the integrity and security of the repository contents.

- *Managing a Tenant and Its Namespaces* — This book contains complete information for managing the HCP tenants and namespaces created in an HCP system. It provides instructions for creating namespaces, setting up user accounts, configuring the protocols that allow access to namespaces, managing search and indexing, and downloading installation files for HCP Data Migrator. It also explains how to work with retention classes and the privileged delete functionality.

- *Managing the Default Tenant and Namespace* — This book contains complete information for managing the default tenant and namespace in an HCP system. It provides instructions for changing tenant and namespace settings, configuring the protocols that allow access to the namespace, managing search and indexing, and downloading installation files for HCP Data Migrator. It also explains how to work with retention classes and the privileged delete functionality.

- *Replicating Tenants and Namespaces* — This book covers all aspects of tenant and namespace replication. Replication is the process of keeping selected tenants and namespaces in two or more HCP systems in sync with each other to ensure data availability and enable disaster recovery. The book describes how replication works, contains instructions for working with replication links, and explains how to manage and monitor the replication process.

- *HCP Management API Reference* — This book contains the information you need to use the HCP management API. This RESTful HTTP API enables you to create and manage tenants and namespaces programmatically. The book explains how to use the API to access an HCP system, specify resources, and update and retrieve resource properties.

- *Using a Namespace* — This book describes the properties of objects in HCP namespaces. It provides instructions for accessing namespaces by using the HTTP, WebDAV, CIFS, and NFS protocols for the purpose of storing, retrieving, and deleting objects, as well as changing object metadata such as retention and shred settings. It also explains how to manage namespace content and view namespace information in the Namespace Browser.

- *Using the HCP HS3 API* — This book contains the information you need to use the HCP HS3 API. This S3™-compatible, RESTful, HTTP-based API enables you to work with buckets and objects in HCP. The book introduces the HCP concepts you need to understand in order to use HS3 effectively and contains instructions and examples for each of the bucket and object operations you can perform with HS3.

- *Using the HCP OpenStack Swift API* — This book contains the information you need to use the HCP OpenStack Swift API. This S3™-compatible, RESTful, HTTP-based API enables you to work with containers and objects in HCP. The book introduces the HCP concepts you need to understand in order to use HSwift effectively and contains instructions and examples for each of the container and object operations you can perform with HSwift.

- *Using the Default Namespace* — This book describes the file system HCP uses to present the contents of the default namespace. It provides instructions for accessing the namespace by using the HCP-supported protocols for the purpose of storing, retrieving, and deleting objects, as well as changing object metadata such as retention and shred settings.

- *HCP Metadata Query API Reference* — This book describes the HCP metadata query API. This RESTful HTTP API enables you to query namespaces for objects that satisfy criteria you specify. The book explains how to construct and perform queries and describes query results. It also contains several examples, which you can use as models for your own queries.

- *Searching Namespaces* — This book describes the HCP Search Console (also called the Metadata Query Engine Console). It explains how to use the Console to search namespaces for objects that satisfy criteria you specify. It also explains how to manage and manipulate queries and search results. The book contains many examples, which you can use as models for your own searches.

- *Using HCP Data Migrator* — This book contains the information you need to install and use HCP Data Migrator (HCP-DM), a utility that works with HCP. This utility enables you to copy data between local file systems, namespaces in HCP, and earlier HCAP archives. It also supports bulk delete operations and bulk operations to change object metadata. Additionally, it supports associating custom metadata and ACLs with individual objects. The book describes both the interactive window-based interface and the set of command-line tools included in HCP-DM.

- *Installing an HCP System* — This book provides the information you need to install the software for a new HCP system. It explains what you need to know to successfully configure the system and contains step-by-step instructions for the installation procedure.

- *Deploying an HCP-VM System* — 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.

- *Third-Party Licenses and Copyrights* — This book contains copyright and license information for third-party software distributed with or embedded in HCP.

- *HCP-DM Third-Party Licenses and Copyrights* — This book contains copyright and license information for third-party software distributed with or embedded in HCP Data Migrator.

- *Installing an HCP RAIN System — Final On-site Setup* — This book contains instructions for deploying an assembled and configured HCP 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 RAIN system that was ordered without a rack and for configuring Hi-Track Monitor to monitor the nodes in an HCP system.

Getting help

The Hitachi Data Systems® customer support staff is available 24 hours a day, seven days a week. If you need technical support, call:

- United States: (800) 446-0744

- Outside the United States: (858) 547-4526

Note: If you purchased HCP from a third party, please contact your authorized service provider.

Comments

Please send us your comments on this document:

HCPDocumentationFeedback@hds.com

Include the document title, number, and revision, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Data Systems.

Thank you!

Comments

1

HCP SAIN system overview

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

The hardware for an HCP SAIN System can be housed in a single rack or in multiple racks. This book addresses only single-rack HCP SAIN systems. These systems are delivered as racked, assembled, and preconfigured appliances with the HCP software already installed. However, once the system is delivered, it needs some final on-site setup.

This chapter contains:

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

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 multigigabyte 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 RAIN and SAIN systems

HDS offers three HCP products: HCP 300, HCP 500, and HCP-VM:

- HCP 300 systems run on a redundant array of independent nodes (RAIN) and use storage that's internal to those nodes.

- HCP 500 systems run on a SAN-attached array of independent nodes (SAIN) and use storage in fibre channel SAN arrays. SAN stands for storage area network.

  To optimize performance for certain usage patterns, nodes in an HCP 500 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 SAIN systems support larger repositories than HCP RAIN 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 SAIN system hardware

HCP SAIN system hardware consists of:

- Nodes (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 SAIN system are either Hitachi Compute Rack 210H (CR 210H) servers or blades in Hitachi Compute Blade 320 (CB 320) servers.

- One or more SAN-attached storage arrays (a typical starter system has one array). Each storage array has one controller tray and one or more expansion trays.

  Storage can be running storage or spindown storage. Running storage is storage on continuously spinning disks. Spindown storage is storage on disks that can be spun down and spun up as needed. All systems have running storage. Only some systems have spindown storage.

- Ethernet switches and cables for networking. The switches in a single-rack HCP SAIN system are Dell PowerConnect 2824 switches.

- Fibre channel cables that connect the nodes to the storage arrays. (Some systems include fibre channel switches between the nodes and the storage arrays.)

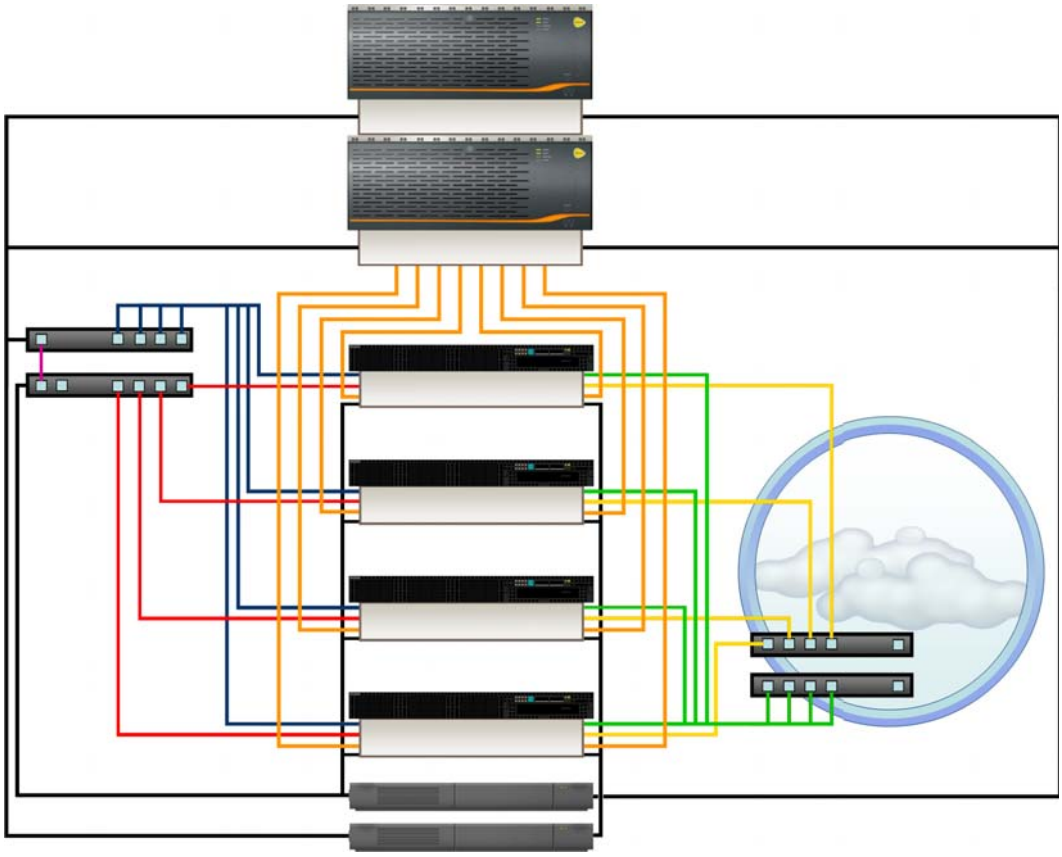
- Additional infrastructure items such as a rack and power distribution units (PDUs).

An HCP system uses both back-end and front-end networks. The isolated back-end network connects the HCP nodes to each other through two redundant Ethernet switches. Each node has a pair of bonded Ethernet ports for connecting to these switches.

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 and the switch configured for active-active bonding.

The front-end network switches and the cables for connecting them to the HCP nodes are not included with the delivered HCP SAIN system. You need to supply them yourself. For information on these switches and cables, see "Additional components" on page 9.

The figure below shows the architecture of an HCP SAIN system. This system has four nodes, a fibre channel SAN array that consists of one controller tray and one expansion tray, two back-end switches (on the left), and two front-end switches (on the right). The nodes shown are CR 210H servers.



The table below 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
Orange fibre channel	Each node	SAN array

(Continued)

Cable	Connects from	Connects to
Black power	Each node	Two PDUs
	Each back-end switch	One PDU
	Tray in the SAN-attached storage array	Two PDUs

Final on-site setup activities

An HCP SAIN system arrives racked and assembled. The HCP software is already installed and is configured with various default settings.

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

Step	Activity	More information
1	Verify that your site is ready for the HCP system to be installed.	Chapter 2, "Site preparation," on page 7
2	Remove the racked HCP system from the packing crate and position it in your data center.	N/A
3	Connect the HCP PDUs to your power sources.	"Connecting to the power sources" on page 12
4	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.	"Connecting to your corporate network" on page 13
5	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.	*Administering HCP*
6	Reconfigure the HCP system for your environment.	Chapter 4, "Reconfiguring the HCP system for your site," on page 15
7	For HCP systems with spindown storage, reconfigure the storage arrays that have spindown storage so HCP can communicate with them at your site.	Chapter 5, "Reconfiguring storage arrays with spindown storage," on page 29
8	Optionally, configure Hi-Track Monitor to monitor the HCP nodes.	Chapter 6, "Configuring HCP monitoring with Hi-Track Monitor," on page 33

2

Site preparation

Before an HCP SAIN 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 SAIN system.

Environmental requirements

An HCP SAIN system comes in a standard 42U equipment rack. The table below shows the size and weight of the servers, switches, and infrastructure components in an HCP SAIN system.

Property		Value
External dimensions of the racked system		Height: 78.8" (2001.45 mm) Width: 23.7" (601.4 mm) Depth: 41.2" (1047.08 mm)
Weight	Rack, PDUs, and wiring harnesses	Approximately 450.8 lbs (204.5 kg)
	Each CR 210H server with internal storage	Approximately 35.6 lbs (16.15 kg)
	Each CR 210H server without internal storage	Approximately 32.4 lbs (14.68 kg)
	Each CR 220S server	Approximately 49.4 lbs (22.4 kg)
	Each Ethernet switch (two total)	Approximately 9.9 lbs (4.5 kg)

Your data center must be able to compensate for the server and switch characteristics shown in the table below.

Component	Max. power draw in watts	Max. total current draw in amps	Max. cooling in BTUs/hour
Each CR 210H server with internal storage	368.8	2.3	1,290.4
Each CR 210H server without internal storage	328.6	2.1	1,149.7
Each CR 220S	474.1	2.8	1,662.7
Each Ethernet switch	110	0.5	375.3

All measurements in the table above are at 200V.

HCP supports the full line of Hitachi Data Systems storage arrays. To determine the site requirements for the storage configuration used by your HCP system, you can use the HDS Weight and Power Calculator, which is available here: http://www.hds.com/go/weight-and-power-calculator

For power, an HCP SAIN system requires four 220V, 30-amp circuits. Each circuit must present the applicable receptacle for the location for which the system was ordered, as indicated in the table below.

Location	Receptacle
United States	NEMA L6-30
EMEA/APAC	IEC 309
Australia	AS 3112

Additional components

To connect an HCP SAIN system to your corporate network, you need to provide:

- One or two switches in your corporate network, each with a port speed of at least one Gb/s. If you're using a single switch, the switch must have at least twice as many open ports as the number of nodes in the system and must be configured for active/active bonding. If you're using two switches, each switch must have at least as many open ports as the number of nodes in the system.

- For each node, two Cat 6 Ethernet cables. If possible, half these cables should be one color and half another color. Also, if possible, the cables should be colors other than red and blue.

3

Connecting the HCP system at your site

An HCP SAIN 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.
- The nodes are connected to the storage array
- The trays in the storage array are connected to each other.
- All the components are plugged into the PDUs.

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 SAIN system includes four PDUs. Each PDU has a fixed power cable of the applicable type for the location for which the system was ordered.

Each node is connected to two PDUs. The back-end switches are each connected to one PDU.

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.

Once you've connected the PDUs to the power sources, you can power on the system:

1. Power on the controller tray (that is, the bottommost tray) in each storage array. This causes the other trays in the array to power on automatically.

2. Wait for the arrays to be online and ready to serve requests from the HCP nodes.

3. Power on the nodes.

The back-end switches power on automatically when the PDUs are connected to the power sources.

Connecting to your corporate network

An HCP SAIN system should be connected to your corporate network through two front-end switches or through a single front-end switch using active/active bonding. This section provides instructions for using two switches. If you're using a single switch, follow the same instructions, connecting each node to a pair of bonded ports in that switch instead of to the two switches.

Important: The default front-end IP addresses for the HCP nodes go from 192.168.100.101 through 192.168.100.104 (or higher for a system with more that four nodes). If these IP addresses don't work for your computing environment, you need to change them *before* you connect the HCP nodes to your corporate network. For information on doing this, see Chapter 4, "Reconfiguring the HCP system for your site," on page 15.

With two front-end switches, each node in the system should be connected to both switches. Use cables of one color to connect the nodes to one of the switches and cables of another color to connect the nodes to the other switch.

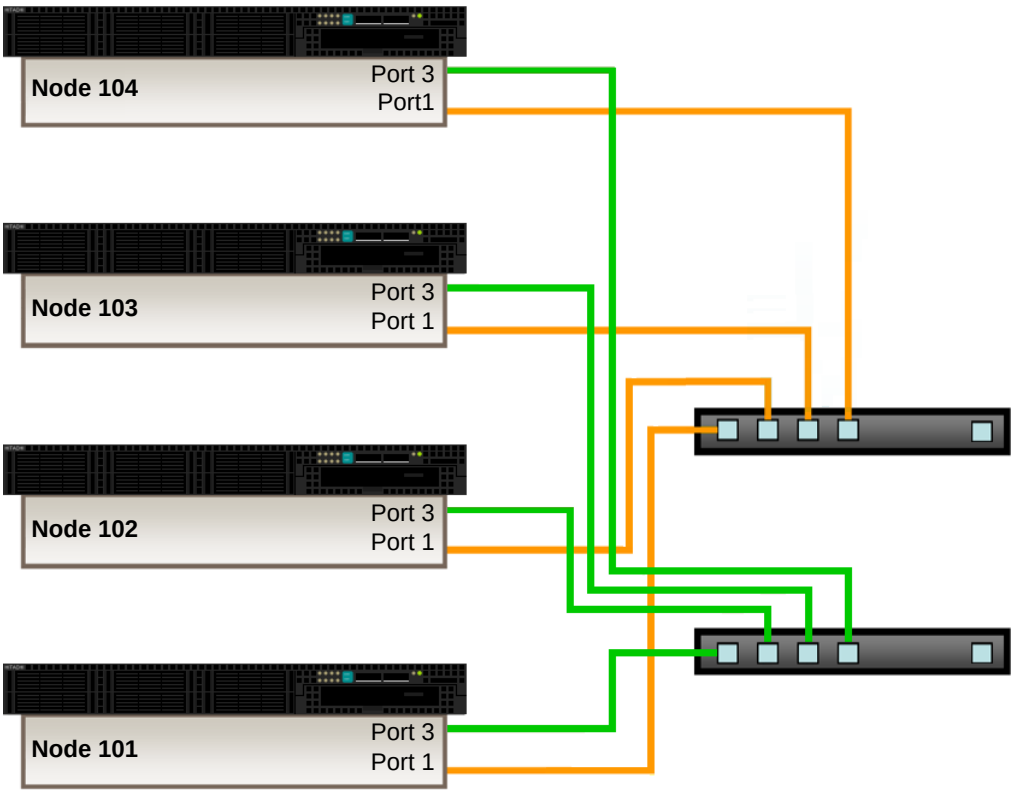
Note: Do *not* put the switches you provide in the rack holding the HCP system.

To connect the HCP system to the your corporate network:

1. Label each cable at both ends. Then connect the cables to the nodes and front-end switches:
   - For nodes that are CR 210H servers:
     - Connect all the cables for one switch to Ethernet port 3 on each node. This becomes the primary switch.
     - Connect all the cables for the other switch to Ethernet port 1 (one) port on each node. This becomes the secondary switch.
   - For nodes that are blades in CB 320 servers:
     - Connect all the cables for one switch to Ethernet port 1 (one) on each blade. This becomes the primary switch.
     - Connect all the cables for the other switch to Ethernet port 3 on each blade. This becomes the secondary switch.

Connect the cables to the switches in sequential order by node number. That is, connect node 101 to first port in each switch, node 102 to the second port, and so on.

The figure below shows these connections for the CR 210H servers.



2. Bundle the cables separately for each switch and use cable ties to secure them to the rack that holds the HCP system. The cables should be secure but not strained or pinched.

4

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, correct it
- Change the HCP network settings to match your computing environment
- Change the HCP DNS settings to match your computing environment
- Change the time settings for the HCP system to match your computing environment
- Make the back-end switches known to HCP

To perform these activities, you use the HCP System Management Console. You can do them in any order.

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 first set up the HCP system at your site. Before performing these activities at any other time, be sure to consult your authorized HCP service provider.

Preparing to reconfigure the system

To reconfigure an HCP system for your computing environment, you first need to create a user account that has the service role. To do this, follow the steps outlined in the table below.

Step	Activity	More information
1	Connect a client computer to the HCP default back-end network.	"Step 1: Connect to the HCP default back-end network" below
2	Log into the System Management Console with the initial user account.	"Step 2: Log in with the initial user account" on page 17
3	Check the health of the HCP system.	"Step 3: Check the health of the HCP system" on page 18
4	Create a new user account with the service role.	"Step 4: Create a service account" on page 18
5	Log into the System Management Console with the new user account.	"Step 5: Log in with the service account" on page 20

Tip: Do not create additional user accounts until you're sure the HCP system is fully operational.

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

Step 1: Connect to the HCP default back-end network

For you to use the HCP System Management Console, you need a client computer with connectivity to the default back-end subnet to which the HCP nodes belong. To connect a client computer to this subnet:

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. Set the subnet mask to 255.255.255.0.

Step 2: Log in with the initial user account

To log into the HCP System Management Console for the first time:

1. On a computer connected to the HCP back-end network, open a browser window.

2. In the address field, enter:

   https://10.1.1.101:8000

   The IP address in this URL is the preconfigured back-end 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 on the **Log In** button.

   The Console displays the **Change Password** page.

7. On the **Change Password** page:

   – In the **Existing Password** field, type: *Chang3Me!*

   – In the **New Password** field, type a new password for the *security* account.

     Passwords must be from six through 64 characters long, are case sensitive, and can 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.

– 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 on setting up user accounts, see *Administering HCP*.

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

Step 3: Check the health of the HCP system

At this point, you need to ensure that the HCP system is running properly. To do this:

1. In the top-level menu in the HCP System Management Console, click on **Hardware**.

2. On the **Hardware** page, for each node, check that:

   – The node status is **Available**

   – The status of each logical volume is **Available** or, for spindown volumes (if the system has any), either **Available** or **Spun down**

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

If all the nodes and logical volumes are available (or, for spindown volumes, spun down), 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** or **Spun down**, 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 the expected number of logical volumes for the node.

Step 4: Create a service account

To create a user account that you can use to reconfigure the HCP system, in the System Management Console:

1. In the top-level menu, mouse over **Security** to display a secondary menu.

2. In the secondary menu, click on **Users**.

3. On the **Users** page, click on **Create User Account**.

4. In the **Create User Account** panel:

   – In the **Username** field, type a username for the user account. Usernames must be from one through 64 characters long and can contain any valid UTF-8 characters, but cannot start with an opening square bracket ([). White space is allowed.

   – In the **Full Name** field, type a full name for the user account. This name must be from one through 64 characters long and can contain any valid UTF-8 characters, including white space.

   – In the **Password** field, type a password for the user account. Passwords must be from six through 64 characters long, are case sensitive, and can 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.

   – In the **Confirm Password** field, type the password again.

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

   – In the **Roles** section, select **Service**.

5. Click on the **Create User Account** button.

6. In the upper right corner of the Console, click on **Log Out**.

   The Console returns to the login page.

Step 5: 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 the 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.

Verifying the serial number

Each HCP system is assigned a unique five-digit serial number. 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.

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.

To verify and, if necessary, change the serial number in the HCP system configuration:

1. In the top-level menu in the System Management Console, mouse over **Configuration** to display a secondary menu.

2. In the secondary menu, click on **Miscellaneous**.

3. 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.

4. 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 on the **Update Settings** button.

Changing network settings

The HCP system is installed with default network settings. You need to change these settings to match your computing environment. Before you can do this, you need to know:

- 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 on 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 should 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 on this and the next two properties, see *Administering HCP*.

- Whether HCP should notify specified downstream DNS 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
```

These considerations apply to specifying the refresh rate:

– In each case, # must be an integer greater than or equal to one.

– If an integer is specified without a time unit, the time unit is assumed to be seconds.

– Time units can be specified in any order.

– Any given time unit can be specified only once.

– Time units are not case sensitive.

– The total time specified must be in the range one through 2,147,483,647 seconds.

- 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

To change the HCP front-end network settings:

1. In the top-level menu in the System Management Console, mouse over **Configuration** to display a secondary menu.

2. In the secondary menu, click on **Networks** to display the **Networks** page.

3. In the list of networks, click on [hcp_system].

4. In the panel for the [hcp_system] network:

   – To change the gateway IP address, in the **Gateway** field, type the new IP address.

   – To change the subnet mask, in the **Netmask** field, type the new subnet mask.

   – To make the front-end network tagged, select the **Make tagged network** option. 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.

   – To change the DNS settings for the network, click on the **Downstream DNS Configuration** link. Then:

     • 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 network settings" above.

   – To change the node IP addresses, in the **Node IP Addresses** section, type new front-end IP addresses for the nodes in the HCP system.

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

5. Click on the **Update Settings** button.

   A warning message appears asking you to confirm the changes you've made.

6. In the field in the message window, type *YES*. This is case sensitive.

7. Click on the **Update Settings** button.

The HCP system restarts with the new settings. This takes a few minutes.

8. If you do not need to change the back-end settings, you can now safely connect the HCP system to your corporate network.

9. Log back into the System Management Console after the system restarts. Then proceed to the next configuration activity.

Changing the back-end settings

To change the HCP back-end network node IP address settings:

1. In the top-level menu in the System Management Console, mouse over **Configuration** to display a secondary menu.

2. In the secondary menu, click on **Networks** to display the **Networks** page.

3. In the list of networks, click on [hcp_backend].

4. In the **Node IP Addresses** section in the [hcp_backend] panel, type new backend IP addresses for the nodes in the HCP system.

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

5. Click on the **Update Settings** button.

   A warning message appears asking you to confirm the changes you've made.

6. In the field in the message window, type *YES*. This is case sensitive.

7. Click on the **Update Settings** button.

The HCP system restarts with the new settings. This takes a few minutes.

Note: If you changed the back-end IP addresses of the HCP nodes:

1. Change the IP address of the client computer to match the new HCP back-end subnet.

2. 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 on 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.

To change the HCP system DNS settings:

1. In the top-level menu, mouse over **Configuration** to display a secondary menu.

2. In the secondary menu, click on **DNS**.

3. On the **DNS Settings** page:

   – Do either of these:

     • 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.

   – Optionally, in the **Hostname Prefix** field, type a new hostname prefix. The hostname prefix can be from one through 12 characters long and can contain only lowercase letters, numbers, and hyphens (-).

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

   – 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.

4. Click on 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 on the **Update Settings** button.

   The 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

The internal time of the delivered HCP system may not exactly match the time in your computing environment. You can choose to leave the HCP time as is, reset it to match your environment and still have the system use its own internal time, or use one or more external time servers.

If you choose to use external time servers, you need to know the IP addresses or hostnames of those servers. Additionally, you need to know the time zone you want HCP to use.

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. HCP 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 the time settings for the HCP system:

1. In the top-level menu, mouse over **Configuration** to display the secondary menu.

2. In the secondary menu, click on **Time**.

3. 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.

   – 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.

4. Click on 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 on 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, if any.

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 the back-end switches are 10.1.1.252 and 10.1.1.253. 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.

To make the back-end switches known to HCP:

1. In the top-level menu in the System Management Console, mouse over **Configuration** to display a secondary menu.

2. In the secondary menu, click on **Monitored Components**.

3. On the **Monitored Components** page, for each switch:

   a. Click on **Add**.

      A new row appears in the **Components** list. The row is highlighted in green.

      If you inadvertently add an extra row, click on 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.

4. Click on the **Update Settings** button.

5

Reconfiguring storage arrays with spindown storage

In an HCP SAIN system with spindown storage, HCP needs to know the controller IP addresses for the storage arrays that have spindown storage in order to request that logical volumes be spun up or spun down as needed. This chapter explains how to configure the storage arrays at your site so that HCP can use the spindown storage on them.

Connecting the arrays to your storage-monitoring network

If your HCP system includes spindown storage, the storage arrays with spindown storage come connected to the HCP back-end switches by Ethernet cables. Disconnect the cables from the back-end switches and connect them to switches in the network you use to monitor storage at your site.

Changing the controller IP addresses on the arrays

The storage arrays with spindown storage are installed with default IP addresses for their controllers. For the first or only storage array, these addresses are:

- For controller 0: 10.1.1.10
- For controller 1: 10.1.1.11

For additional arrays, the fourth octet of the IP address increments by one. So, for example, the IP addresses for controller 0 and controller 1 in the second array would be 10.1.1.12 and 10.1.1.13, respectively.

Typically, you need to change these IP addresses to addresses in the network you use to monitor storage at your site. Whether you change them or not, the controller IP addresses must also be accessible from the HCP front-end network.

To change the controller IP addresses on each storage array with spindown storage, you use Storage Navigator. Storage Navigator is an HDS tool used to configure HDS storage arrays. For instructions on using Storage Navigator, see the applicable HDS documentation for the type of arrays you have.

Changing the controller IP addresses in HCP

After you've changed the controller IP addresses on the storage arrays with spindown storage, you need to make the new addresses known to HCP.

In HCP, storage arrays are identified by their serial numbers. Before changing the controller IP addresses for an array in HCP, be sure you have the serial number for the array and know which IP address goes with which controller in the array.

Changing the controller IP addresses for a storage array in HCP causes all spindown volumes in the array to spin up. These volumes eventually spin back down if they're not actively being used.

To change storage array controller IP addresses in HCP:

1. Log into the HCP System Management Console using the user account with the service role that you created in "Step 4: Create a service account" on page 18.

2. In the top-level menu, mouse over **Configuration** to display a secondary menu.

3. In the secondary menu, click on **Arrays**.

4. On the **Arrays** page, type the new IP addresses in the applicable fields.

5. Click on the **Update Settings** button.

   A warning message appears asking you to confirm the changes you've made.

6. In the field in the message window, type *YES*. This is case sensitive.

7. Click on the **Update Settings** button.

6

Configuring HCP monitoring with Hi-Track Monitor

Hi-Track Monitor is an HDS product that enables remote monitoring of the nodes and storage in an HCP SAIN system. With Hi-Track Monitor, you can view the status of these components in a web browser. You can also configure Hi-Track Monitor to notify you by email of error conditions as they occur. Additionally, you can configure Hi-Track Monitor to report error conditions to HDS support personnel.

Hi-Track Monitor is for monitoring and error notification purposes only. It does not allow any changes to be made to the system.

Hi-Track Monitor 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 Hi-Track servers. However, Hi-Track support for IPv6 network connections varies based on the Hi-Track server operating system. For information on requirements for Hi-Track servers that support IPv6 networks, see the applicable Hi-Track documentation.

This chapter explains how to set up monitoring of HCP nodes with Hi-Track Monitor. For information on setting up storage monitoring, see the Hi-Track Monitor documentation.

This chapter assumes that Hi-Track Monitor is already installed and running according to the documentation that comes with the product.

Enabling SNMP in HCP

To enable Hi-Track Monitor 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, Hi-Track Monitor 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 Hi-Track Monitor to match what you specify in HCP. For more information on this, see the Hi-Track Monitor documentation.

To enable SNMP in HCP for use with Hi-Track Monitor:

1. Log into the HCP System Management Console using the initial user account, which has the security role.

2. In the top-level menu in the System Management Console, mouse over **Monitoring** to display a secondary menu.

3. In the secondary menu, click on **SNMP**.

4. In the **SNMP Settings** section on the **SNMP** page:

   – Select the **Enable SNMP at snmp.*hcp-domain-name*** option.

   – Select either **Use version 1 or 2c** (recommended) or **Use version 3**.

     If you select **Use version 3**, specify a username and password in the **Username**, **Password**, and **Confirm Password** fields.

   – Optionally, in the **Community** field, type a different community name.

5. Click on the **Update Settings** button.

6. 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 Hi-Track Monitor is installed. Then click on the **Add** button.

7. Log out of the System Management Console and close the browser window.

Configuring Hi-Track Monitor

To configure Hi-Track Monitor to monitor the nodes in the HCP system, follow the steps outlined in the table below.

Step	Activity	More information
1	Log into Hi-Track Monitor.	"Step 1: Log into Hi-Track Monitor" below
2	Set the Hi-Track Monitor base configuration, including the email addresses to which email about error conditions should be sent.	"Step 2: Set the base configuration" below
3	Optionally, configure transport agents for reporting error conditions to HDS support personnel.	"Step 3 (optional): Configure transport agents" on page 37
4	Identify the HCP system to be monitored.	"Step 4: Identify the HCP system" on page 38

Step 1: Log into Hi-Track Monitor

To log into Hi-Track Monitor:

1. Open a web browser window.
2. In the address field, enter the URL for the Hi-Track Monitor server (using either the hostname or a valid IP address for the server) followed by the 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 Hi-Track Monitor is already in use at your site for monitoring other devices, this password may have been changed. In this case, see your Hi-Track Monitor administrator for the current password.

5. Click on the **Logon** button.

Step 2: Set the base configuration

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

If Hi-Track Monitor 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 Hi-Track Monitor base configuration:

1. In the row of tabs at the top of the Hi-Track Monitor interface, click on **Configuration**.

   The **Base** page is displayed by default. To return to this page from another configuration page, click on **Base** in the row of tabs below **Configuration**.

2. In the **Device Monitoring** section:

   – In the **Site ID** field, type your HDS customer ID. If you don't know your customer ID, contact your authorized HCP service provider for help.

   – Optionally, specify different values in the other fields to meet the needs of your site. For information on these fields, click on the **Help on this table's entries** link above the fields.

3. In the **Notify Users by Email** section:

   – In the **eMail Server** field, type the fully qualified hostname or a valid IP address of the email server through which you want Hi-Track Monitor to send email about error conditions.

   – In the **Local Interface** field, select the Ethernet interface that has connectivity to the specified email server. (This is the interface on the Hi-Track Monitor server.)

   – In the **User List** field, type a comma-separated list of the email addresses to which Hi-Track Monitor should send email about error conditions.

– 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 known to the server.

4. Click on the **Submit** button.

5. Optionally, to send a test email to the specified email addresses, click on the **Test Email** button.

Step 3 (optional): Configure transport agents

A Hi-Track Monitor transport agent transfers notifications of error conditions to a target location where HDS 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. Hi-Track tries them in the order in which they are listed until one is successful.

To configure a transport agent:

1. In the row of tabs below **Configuration**, click on **Transport Agents**.

2. In the field below **Data Transfer Agents**, select the transfer method for the new transport agent.

3. Click on 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 on what to specify, see the Hi-Track Monitor documentation.

5. Click on 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:

1. In the **Move to Top?** column, select the transport agent you want to move.

2. Click on the **Submit** button.

Step 4: Identify the HCP system

To identify the HCP system to be monitored:

1. In the row of tabs at the top of the Hi-Track Monitor interface, click on **Summary**.

   The **Summary** page displays up to four tables that categorize the devices known to Hi-Track Monitor — Device Errors, Communication Errors, Devices Okay, and Not Monitored. To show or hide these tables, click in the checkboxes below the table names at the top of the page to select or deselect the tables, as applicable. Then click on the **Refresh** button.

   While no tables are shown, the page contains an **Add a device** link.

2. Take one of these actions:

   – If the **Summary** page doesn't display any tables, click on the **Add a device** link.

   – If the **Summary** page displays one or more tables, click on 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 HDS 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**.

    For information on configuring SNMP in HCP, see "Enabling SNMP in HCP" on page 34.

11. In the **Comms Error Reporting?** field, select one of these options to specify whether Hi-Track should report communication errors that occur between Hi-Track Monitor 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 on the **Add** button.

    If the operation is successful, the interface displays a message indicating that the HCP system has been added. Do not click on the **Add** button again. Doing so will add the system a second time.

Index

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2627
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-98ARC020-16