HITACHI
Inspire the Next

# Hitachi Content Platform

## Installing an HCP System

Hitachi Data Systems

MK-99ARC026-15
23 December 2016

# Contents

# Preface

This book is the software installation guide for the Hitachi Content Platform (HCP). It contains the concepts and instructions you need to install both the Appliance Operating System and the HCP software on the nodes in an HCP system.

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

## Intended audience

This book is intended for people who are responsible for installing HCP system software at a customer site. It assumes you have experience working with computer systems and installing software applications.

## Product version

This book applies to release 7.3 of the Hitachi Content Platform.

# Syntax notation

The table below describes the conventions used for the syntax of commands, expressions, URLS, and object names in this book.

| Notation | Meaning | Example |
|---|---|---|
| **boldface** | Type exactly as it appears in the syntax (if the context is case insensitive, you can vary the case of the letters you type) | This book shows:<br><br>**https://admin.***hcp-name.domain-name***:8000**<br><br>You enter: https://admin.hcp-ma.example.com:8000 |
| *italics* | Replace with a value of the indicated type | |

# 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 HSwift API. This OpenStack Swift, 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 or move 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.

- *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 SAIN System - Final On-site Setup* - This book contains instructions for deploying an assembled and configured single-rack HCP 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 Hi-Track® Monitor to monitor the nodes in an HCP system.

- *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.

## Accessing product documentation

Product documentation is available on Hitachi Data Systems Support Connect: https://knowledge.hds.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

## Getting help

Hitachi Data Systems Support Portal is the destination for technical support of products and solutions sold by Hitachi Data Systems. To contact technical support, log on to Hitachi Data Systems Support Connect for contact information: http://portal.hds.com

Hitachi Data Systems Community is a global online community for HDS 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 http://community.hds.com, register, and complete your profile.

**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 and number, including the revision (for example, -01), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Data Systems.

**Thank you!**

# 1

# HCP overview

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

Once the HCP hardware is set up, the software must be installed. You can install the software yourself, or you can have your authorized HCP service provider do the installation for you.

This chapter reviews some basic HCP concepts and describes the HCP hardware architecture. The chapter also contains an overview of HCP installation activities

## Introduction to Hitachi Content Platform

Hitachi Content Platform is a distributed storage system designed to support large, growing repositories of fixed-content data. HCP provides a cost-effective, scalable, easy-to-use repository that can accommodate all types of data, from simple text files to medical images to multigigabyte database images.

A **fixed-content storage system** is one in which the data cannot be modified. HCP uses write-once, read-many (WORM) storage technology and a variety of policies and services to ensure the integrity of the stored data and the efficient use of storage capacity.

HCP can run on either a SAN-attached array of independent nodes (**SAIN**), SAN stands for storage area network, or a networked redundant array of independent nodes (**RAIN**).

SAIN systems include both internal storage in each node and Fibre-Channel SAN arrays. RAIN has only internal storage in each node.

HCP-VM systems (called VM systems) run on virtual machines in a VMware® environment. In this environment, HCP functions mostly as a RAIN system, with the virtual storage emulating internal storage.

What follows is a brief overview of HCP basics. For a more in-depth introduction to HCP, see *Administering HCP*.

**Object-based storage**
HCP stores **objects** in a repository. Each object permanently associates data HCP receives with information about that data; that is, each object encapsulates both object data and metadata.

HCP distributes objects across its storage space but still presents them as files in a standard directory structure.

**Namespaces**
An HCP repository is partitioned into namespaces. A **namespace** is a logical grouping of objects such that the objects in one namespace are not visible in any other namespace. Namespaces are not associated with any preallocated storage.

An HCP system can have a maximum of 10,000 locally defined namespaces, including one special namespace called the **default namespace**. Applications are typically written against namespaces other than the default; these namespaces are called HCP namespaces. The default namespace is most often used with applications that existed before release 3.0 of HCP

**Note:** Replication can cause an HCP system to have more than 10,000 namespaces. For information on replication, see *Replicating Tenants and Namespaces*.

**Tenants**
Namespaces are owned and managed by administrative entities called **tenants**. A tenant typically corresponds to an organization such as a company or a division or department within a company. A tenant can also correspond to an individual person.

An HCP system can have a maximum of 1,000 tenants. Each tenant, except one, can own multiple namespaces. The exception, called the **default tenant**, owns the default namespace and only that namespace.

**Namespace access protocols**
HCP supports access to namespaces through a variety of industry-standard protocols. For actions such as adding objects to a namespace, viewing and retrieving objects, changing object metadata, and deleting objects, HCP supports:

- For HCP namespaces only:
  - A RESTful HTTP API (simply referred to as HTTP in the HCP documentation).
  - HS3, which is a RESTful, HTTP-based API that's compatible with Amazon® S3. With HS3, namespaces are called **buckets**.
  - HSwift, which is a RESTful, HTTP-based API that's compatible with OpenStack Swift. With HSwift, namespaces are called **containers.**
- For the default namespace only, a non-RESTful implementation of HTTP
- For all namespaces:
  - WebDAV
  - CIFS
  - NFS

HCP allows special-purpose access to namespaces through two additional protocols: SMTP (for storing email) and, for the default namespace only, NDMP (for backing up and restoring data).

**Data access authentication**
The HTTP, HS3, HSwift, WebDAV, and CIFS protocols can be configured to require authentication for access to HCP namespaces. If these are the only protocols enabled for a namespace, users and applications must present valid credentials for access to the namespace content.

HCP supports both local and remote authentication methods. For remote authentication, HCP supports Windows® Active Directory® and RADIUS.

### HCP Search Console

HCP includes a web application called the **Search Console** that lets users search for objects based on specified criteria. This Console works with either of these two search facilities:

- The **HCP metadata query engine** — This facility is integrated with HCP and works internally to perform searches and return results to the Search Console. The metadata query engine is also used by the metadata query API.

  When working with the metadata query engine, the Search Console is called the **Metadata Query Engine Console**.

- The **Hitachi Data Discovery Suite (HDDS) search facility** — This facility interacts with HDDS, which performs searches and returns results to the HCP Search Console. To use the HDDS search facility, you need to first install and configure HDDS, which is a separate product from HCP.

The Search Console can use only one search facility at any given time. The search facility is selected at the HCP system level. If no facility is selected, the HCP system does not support the use of the Search Console to search namespaces.

Each search facility maintains its own index of objects in each search-enabled namespace and uses this index for fast retrieval of search results. The search facilities automatically update their indexes to account for all new and deleted objects and changes to object metadata.

For more information on the two search facilities, see *Administering HCP*. For information on using the HCP Search Console, see *Searching Namespaces*.

### HCP services

HCP **services** are background processes that each perform a specific function that contributes to the continuous tuning of the HCP system. In particular, services are responsible for optimizing the use of system resources and maintaining the integrity and availability of the stored data.

### Replication

**Replication** is the process of keeping two or more HCP systems in sync with each other. The replication service on any given system automatically

copies selected HCP tenants and namespaces and default-namespace directories to one or more other systems. Both configuration information and namespace content are copied.

Replication is configured by the creation of links, each of which establishes a secure trust relationship between two systems. The link determines what is replicated between the two systems and how data is transmitted between the systems.

For more information on replication, see *Replicating Tenants and Namespaces*

**Note:** Replication is an add-on feature to HCP, with a separate purchase price.

# HCP hardware

HCP hardware consists of:

- Servers
- Internal and/or SAN storage
- Networking components such as cables and switches
- Additional infrastructure items such as racks and power distribution units (PDUs)

**Note:** For VM systems, this hardware configuration applies to the physical environment in which HCP-VM runs.

## Nodes and storage

An HCP system includes multiple **nodes** that are networked together, where each node is either an individual server, a blade in a Hitachi Compute Blade 320 (CB 320), or a virtual machine. Each physical node can have multiple internal drives and/or can connect to SAN storage. Each virtual node emulates a server that has only internal drives.

By default, HCP stores all objects on **primary running storage**, which is the physical storage that's managed by the nodes in the HCP system and consists of continuously spinning disks. However, HCP can be configured to use HCP S Series Nodes, known as **economy storage**, as an alternative to primary running storage or for tiering purposes.

HCP can also use additional storage for tiering. These devices, like Amazon S3 or Microsoft Azure, are called **extended storage**, and are managed outside of the HCP system.

An HCP SAIN system can also be configured to use additional storage that's managed by the nodes in the HCP system and consists of disks that can be spun up or spun down as needed. HCP uses this additional storage, called **primary spindown storage**, for tiering purposes.

The physical storage managed by a node maps to **logical volumes**. Logical volumes on storage managed by HCP are **local storage volumes**. Logical volumes can also be **NFS volumes** (also called **external volumes**). These are volumes that are stored on extended storage and are accessed using NFS mount points.

## Storage nodes

Storage nodes are the core components of an HCP system. These nodes manage the objects that reside in the system storage. To ensure data integrity and continuous availability in case of a hardware or software failure, HCP uses RAID technology for its storage and can also be configured to store the data and metadata for each object in multiple locations.

Each storage node runs all the HCP software. The nodes work together to serve both as a repository manager and as a gateway that enables access to the data in the repository.

All runtime operations are distributed among the storage nodes, thereby ensuring reliability and performance as capacity grows. If a node fails, the HCP system adapts by redirecting processing to other nodes, so the stored data remains available to users

## Logical volumes

Each node in an HCP system manages its own set of logical volumes. On each node, local storage and NFS (external) volumes have numeric IDs in the range 0 (zero) through 127.

Logical volume 0 (zero) on each node is reserved for the operating system. The IDs for the other volumes depend on the volume type:

**Data volume** — Primary running storage that stores object data and does not store the metadata query engine index. **Primary running storage** is storage that's managed by HCP and consists of continuously spinning disks.

Data volumes on SAN storage have numeric IDs in the range 1 (one) through 63. Data volumes on internal storage have IDs 92 and 93 if your HCP nodes have six drives. If your nodes have 12 drives (local storage systems only), you also have data volumes with IDs 94 and 95.

- **Index volume** (SAIN systems only) — Primary running storage that stores only the metadata query engine index. All storage nodes should have the same number of index volumes.

  Index volumes have numeric IDs in the range 64 through 91.

- **Shared volume** — Primary running storage that stores both object data and the metadata query engine index. All storage nodes have one shared volume.

  The shared volume for each node has a numeric ID in the same range as data volumes.

- **Spindown volume** (SAIN systems only) — Primary spindown storage that stores object data and does not store the metadata query index. **Primary spindown storage** is storage that's managed by HCP and consists of disks that can be spun down and spun up as needed. All storage nodes should have the same number of spindown volumes.

  Spindown volumes have numeric IDs in the range 96 through 127. The volume numbering starts from 96 and goes up.

- **NFS volume** or **external volume** — Extended storage that's accessed using an NFS mount point. NFS volumes store only object data.

  NFS volumes have numeric IDs in the range 96 through 127. The volume numbering starts from 127 and goes down.

For information on the metadata query engine index, primary spindown storage, and NFS storage (external storage), see *Administering HCP*.

## Networking

HCP has both back-end and front-end networks. The isolated back-end network connects the HCP nodes to each other through two redundant back-end Ethernet switches. Each node has a pair of bonded Ethernet ports that are used to connect the node to these switches.

**Caution:** The back-end network must remain separate from the front-end network. Interfering with the operation of the back-end network or back-end switches can cause the HCP system to become inoperable and can result in data loss.

Each storage node is configured with an additional pair of bonded Ethernet ports that allow external applications to access the system. The recommended configuration options are:

- Two independent Ethernet switches that connect these ports to the front-end network
- One Ethernet switch, with both HCP and the switch configured for active-active bonding

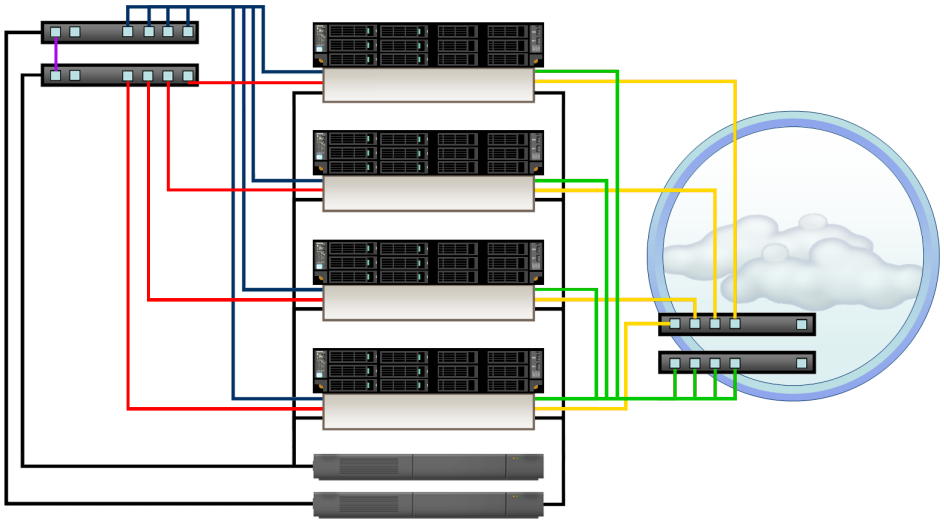
HCP supports virtual networking for the front-end network. This enables the segregation of network traffic between clients and different HCP tenants, between management and data access functions, and between system-level and tenant-level traffic. For information on virtual networking with HCP, see *Administering HCP*.

## System architecture

The following figures show the architecture of HCP RAIN, SAIN, and VM systems and the relationship between two systems involved in replication.

**RAIN system architecture**

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

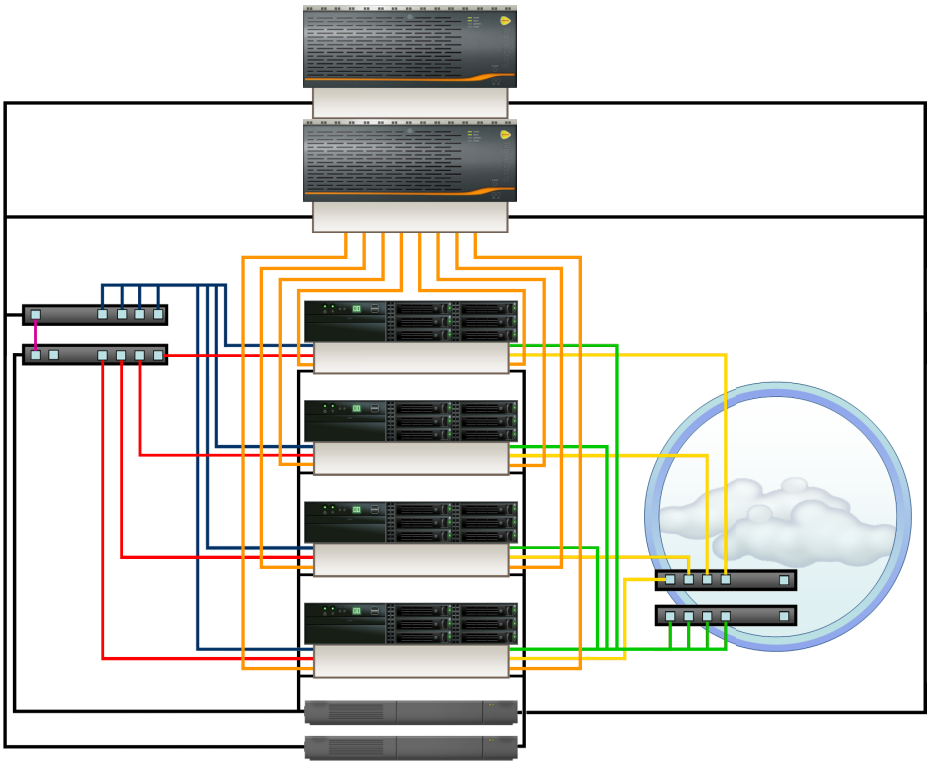


The table below describes the cables in this figure.

| 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 |
| Black power | Each node | Two PDUs |
| | Each back-end switch | One PDU |

### SAIN system architecture

The figure below shows the architecture of an HCP system that uses a Fibre Channel SAN array. This system has four storage nodes, two modular storage trays, two back-end switches (on the left), and two front-end switches (on the right). Each node has multipathed access to the shared SAN storage.



The table below describes the cables in this figure.

| Cable | Connects from | Connects to |
|---|---|---|
| Red and blue Ethernet | Back-end 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 |
| Black power | Each node | Two PDUs |
| | Each back-end switch | One PDU |
| | Each storage tray | Two PDUs |

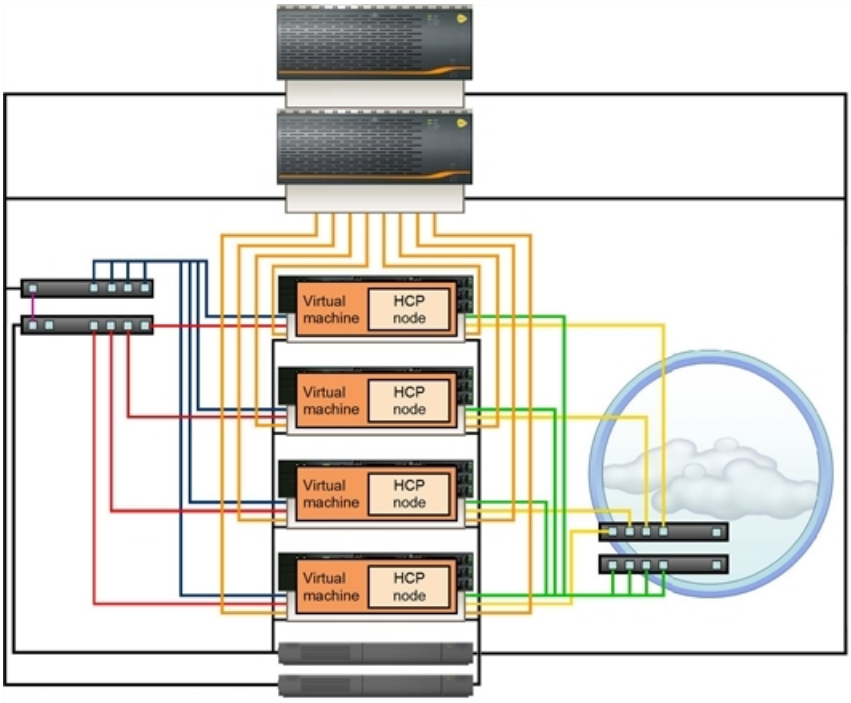
**Note:**

- Nodes in HCP SAIN systems are either individual servers or individual blades in blade servers. The figure above shows individual servers.
- Some HCP SAIN systems include Fibre Channel switches between the nodes and the SAN arrays.

### VM system architecture

The physical environment for an HCP VM system has the same architecture as an HCP SAIN system. That is, the servers that host the VMs on which HCP runs have multipathed access to shared SAN storage. The physical switch and port configurations are the same as for SAIN systems.

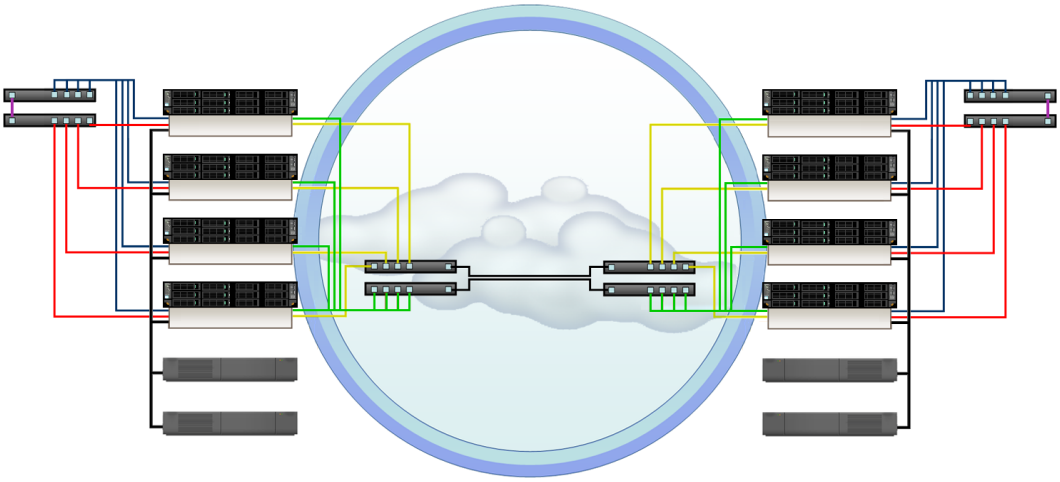
Depending on the number of physical servers and the capabilities of those servers, a VM system can have one or more HCP nodes running in each server. The figure below shows the physical environment for a VM system with four HCP nodes, each running in its own physical server. For information about the hardware configuration in this figure, see SAIN system architecture above.




### Network connections for HCP with replication

Replication occurs between pairs of HCP systems. The two systems in a replication pair are connected through the front-end network infrastructure, as shown in the figure below. Replication traffic from each system must be

routable to the network selected for replication on the other system.



For more information on replication, see *Replicating Tenants and Namespaces*.

# HCP software

HCP system software consists of an operating system (the **Appliance operating system**) and HCP software. For maximum reliability, each storage node in an HCP system runs all the HCP software. This software includes components that:

- Handle object data and metadata
- Ensure that services run as expected
- Enable you to configure, monitor, and manage the HCP system and the tenants and namespaces defined in the system
- Provide a human-readable interface to HCP system configuration, activity, and status
- Enable access to namespaces using the supported namespace access protocols
- Support data transfer to and from the HCP system through the HCP Data Migrator utility
- Support searching namespaces through the metadata query API and the HCP Search Console

## HCP System Management Console

The System Management Console is a secure web application that provides interactive access to the HCP system. To use the System Management Console, you need a user account. This account determines what you have permission to do in the Console.

A **role** is a named collection of permissions that can be associated with a user account. Some of the activities in this book require you to have a user account with a specific role. This is noted with the applicable procedures.

HCP is installed with one predefined user account. The username and default password for this account are:

Username: **security**
Password: **Chang3Me!**

This account includes only the security role. When you first install HCP, you need to either create a new user account with the administrator role or modify the *security* account to include the administrator role so you can change the system configuration as needed.

**Note:** The password for the *security* account must be changed the first time someone logs in as *security*.

For more information on the System Management Console, user accounts, and roles, see *Administering HCP*.

**Note:** When administering a tenant, you use a different web application, called the Tenant Management Console. For information on this Console, see *Managing a Tenants and Its Namespaces* or *Managing the Default Tenant and Namespace*.

# HCP installation procedure

To successfully install and configure an HCP system, follow the steps outlined in the procedure below:

1. Gather the information you need to perform the installation (see Chapter 2: "Gathering installation information" on page 15)
2. Install the Appliance operating system (see )

3. Learn about the HCP software installation program (see "HCP Setup program" on page 41)

4. Install the HCP software (see "Performing the HCP software installation" on page 46)

5. Verify the HCP system installation (see "Verifying the HCP installation" on page 59)

6. Perform additional system configuration procedures, as needed (see "Performing additional system configuration procedures" on page 61)

# 2

# Gathering installation information

The software for an HCP system consists of an operating system (the Appliance operating system) and the HCP software.

Before you can install the Appliance OS and the HCP software, you need to know certain information about the system you're creating. For example, you need to know the IP addresses of the HCP nodes, the serial number for the system, and which features you want to enable.

Some of the information you need comes from the HCP distributor. The rest depends on decisions you make yourself or in conjunction with your authorized HCP service provider. Often, you make these decisions before the hardware arrives on site.

Once the HCP system is up and running, you may want to do some post-installation setup. For example, you may want to enable syslog logging or disable the ability to ping the HCP nodes.

This chapter describes the information you need for installing both the Appliance OS and the HCP software. It also outlines the information required for any post-installation setup you want to do.

The descriptions in this chapter are intended to help you prepare for an HCP system installation. You can use the forms in Appendix A: "Forms" on page 63, to record the information you collect. You can then keep the completed forms available to facilitate the installation procedure.

## Information for an OS installation

To install the Appliance OS for a new HCP system, you need to know about the nodes and the front-end and back-end networks to be configured for the system.

**Tip:** You can use the "Appliance OS Installation Information" on page 63 to record this information.

**HCP nodes**
For a fresh installation of the OS, you need to know which servers at your site are supposed to be nodes in the HCP system. For each server, you need to know:

- The physical location.
- The back-end IP address (see Back-end IP addresses below). The back-end network information that you specify during the OS installation is for the [hcp_backend] network.
- The front-end network IP mode (IPv4, IPv6, or Dual). The front-end network IP mode that you specify during the OS installation is used to set both the system-level IP mode and the [hcp_system] network IP mode. The front-end network IP mode must be the same on all nodes.

  The system-level IP mode setting determines whether HCP supports the use of only IPv4 addresses, only IPv6 addresses, or both types of IP addresses for *all* front-end networks defined on the HCP system, including the [hcp_system] network and any user-defined networks.

  The [hcp_system] network IP mode setting determines whether during the installation, the [hcp_system] network is configured to use IPv4 addresses, IPv6 addresses or both types of IP addresses.

**Note:** A user-defined network can be configured to use a specific type of IP address *only* if the [hcp_system] network is also configured to use that type of IP address.

  For more information on the effects of the system-level IP mode setting and the [hcp_system] network IP mode setting, see *Administering HCP*.

- The front-end network IP configuration settings. The front-end network IP configuration information that you specify during the OS installation is for the [hcp_system] network:
  - If the front-end network IP mode is IPv4 or Dual:
    - The front-end network IPv4 gateway IP address and subnet mask. These settings must be the same for all nodes.

  - The IPv4 address to assign to the node for the front-end network. This address must be on the same subnet as the IPv4 gateway.

- If the front-end network IP mode is IPv6 or Dual:

  - The primary IPv6 gateway IP address and prefix length for the front-end network. These settings must be the same for all nodes.

  - The primary IPv6 address to assign to the node for the front-end network. This address must be on the same subnet as the primary IPv6 gateway.

  - If a secondary IPv6 gateway is defined for the [hcp_system] network:

    - The secondary IPv6 gateway IP address and prefix length for the front-end network. These settings must be the same for all nodes.

**Note:** The primary and secondary IPv6 gateways must be on separate, non-overlapping subnets.

    - The secondary IPv6 address to assign to the node for the front-end network. This address must be on the same subnet as the secondary IPv6 gateway.

- The bonding mode for the front-end network. With two front-end switches, HCP supports a bonding mode of active-backup. With a single front-end switch, HCP supports a bonding mode of active-active (802.3ad) for link aggregation or active-backup. The front-end network bonding mode must be the same on all nodes.

- The interface type for the front-end network. The interface type can either be 10BaseT or SFP+ and must be the same on all nodes.

- Whether to make the [hcp_system] network a tagged network by providing a VLAN ID for it and, if so, what VLAN ID to use. The customer may choose to do this if the networking infrastructure is VLAN capable. If specified, the VLAN ID must be the same on all nodes.

For information on the [hcp_system] and [hcp_backend] networks and VLAN IDs, see *Administering HCP*.

**Back-end IP addresses**
All the nodes in an HCP system must be on the same system-specific private back-end subnet. This subnet is used only for internode communication. It must not be connected to your corporate network, which is used for other types of data communication .

For the back-end subnet, use the installation default of 10.1.1.x (with the required subnet mask of 255.255.255.0) unless it's already in use in your corporate network. If 10.1.1.x is unavailable, choose another private IP subnet.

For the fourth octet of the back-end IP addresses, use sequential numbers such as 101, 102, 103, and so on. These octets can differ from the fourth octets in the front-end IP addresses.

**Note:** The HCP software installation procedure in this book refers to the highest-numbered storage node. The number assigned to a node is the fourth octet of its back-end IP address.

**Caution:** Once HCP is installed, interfering with the operation of the back-end network or back-end switches can cause the system to become inoperable and/or can result in data loss.

# Information for an HCP software installation

The HCP software installation program prompts for a variety of configuration information. This information is described in the following sections.

**Tip:** You can use the "HCP Software Installation Information" on page 65 to record this information.

## HCP nodes

For an HCP software installation, you need to know the back-end IP address of each HCP node.

During the installation, you can specify node IP addresses individually or as a range.

## Distributor key

For an HCP software installation, you need to know the name of the distributor key. This key enables access to the HCP nodes for troubleshooting purposes.

For the name of the distributor key, contact your HCP distributor.

## Networking

When installing the HCP software, you need this networking information:

- If the front-end network IP mode is set to IPv4 or Dual, the IPv4 gateway IP address used to route requests from the HCP system to the front-end network. This is the same as the front-end network IPv4 gateway IP address that you specified during the OS installation.
- If the front-end network IP mode is set to IPv6 or Dual:
  - The primary IPv6 gateway IP address used to route requests from the HCP system to the front-end network. This is the same as the primary IPv6 gateway IP address that you specified for the front-end network during the OS installation.
  - Optionally, the secondary IPv6 gateway IP address used to route requests from the HCP system to the front-end network. If you specified a secondary IPv6 gateway IP address for the front-end network during the OS installation, specify that IP address during the HCP software installation. If you did not specify a secondary IPv6 gateway IP address during the OS installation, do not specify one during the HCP software installation.
- The system-specific IP address that the HCP nodes use to multicast messages to the other nodes in the system over the back-end network. This address must begin with 238.

  Normally, you accept the default multicast address proposed by the installation program. This default is 238.177.1.1.

## Domain name system

If DNS is in use at your site, HCP can be configured to use DNS services. To set this up, you need to specify a domain name for the HCP system in the DNS. The recommended procedure is to do this before the HCP software is

installed.

When HCP is configured to use DNS, clients can direct requests to the HCP system by using the system domain name, and HCP can distribute those requests among the nodes in the system. Without DNS, clients must direct requests to specific nodes by using the node IP addresses, which can create an imbalance in node activity.

The domain name for the HCP system should consist of a name for the system together with the name of the corporate domain (for example, hcp-ma.example.com, where hcp-ma is the system name and example.com is the corporate domain name). That is, HCP should be configured as a subdomain of the corporate domain.

The system domain name can contain only lowercase letters, numbers, and hyphens (-). It must consist of at least three segments, separated by periods (.). Each segment must be one through 63 characters long. The entire domain name, including the periods between segments, must be less than 128 characters long.

When installing the software for an HCP system, you need to specify the domain name for the HCP system. The installation program creates a domain with this name in HCP and associates that domain with the [hcp_system] network.

If you don't use DNS, you still need to provide a domain name for the HCP system. Client requests can use this dummy domain name for access to the system if the node IP addresses are mapped to the dummy domain name in a `hosts` file. For more information on using a `hosts` file for this purpose, see *Administering HCP*.

For the HCP software installation, in addition to the domain name for the HCP system, you also need to know whether you want to use DNS with HCP and, if so, you need to know *all* of the IPv4 and IPv6 addresses that HCP needs to use to forward DNS requests to *each* of the upstream DNS servers. An **upstream DNS server** is a DNS server to which HCP routes the outbound communications that it initiates (for example, for sending log messages to syslog servers or for replication purposes).

**Note:**

- To enable HCP to communicate with DNS, each DNS server must have at least one IPv4 or IPv6 address that is routable from the [hcp_system] network.
- You cannot use the domain name to access an HCP system until the HCP domain is configured in the DNS.
- HCP can use Windows Active Directory for user authentication *only* if the list of DNS server IP addresses includes the IPv4 and IPv6 addresses that HCP uses to communicate with at least one DNS server that can resolve the Active Directory domain name.
- A **downstream DNS server** is a DNS server through which client requests are routed to HCP. The downstream and upstream DNS servers can be the same servers.

Once the HCP system is running, you can use the System Management Console to create additional domains. For information on this and on configuring the HCP domain in the DNS, see *Administering HCP*.

## Time synchronization

you need to decide whether the HCP system should use itself as a time source or should use one or more external time servers. When the time source is internal, the nodes synchronize time among themselves. Because HCP is a closed system, making the time source internal ensures compliance with the applicable regulatory requirements.

On the other hand, using internal time can result in clock drift, thereby causing HCP system time to differ from the time settings of other applications in the corporate environment. Resetting the HCP system time to compensate for this drift can affect object retention, thereby violating compliance.

External time servers can be corporate or Internet time servers. Using a corporate time server keeps the HCP system time synchronized with other applications in the corporate environment. However, if the corporate time server is not completely secure, compliance is not guaranteed. The same concern about compliance applies to Internet time servers. Using multiple external time servers helps ensure the integrity of the time source.

**Note:**

- HCP does not support using a Windows as an external time server.
- To ensure proper system time synchronization, HCP requires each external time server to have a minimum stratum of 10. For best results, it is recommended that you use external time servers that have a minimum stratum of 5 or less.
- When HCP is using an external time server, if either of the following happens, the HCP system automatically restarts itself:
  - The time on the time server is changed by more than 1,000 seconds.
  - The HCP system switches to a different time server whose time differs from the original time server by more than 1,000 seconds.
- For HCP to use Windows Active Directory for user authentication, the HCP system time must be the within five minutes of the Active Directory time. The recommended configuration is for HCP and Active Directory to use the same external time server.

To set the time source during a software installation, you specify either *internal* or the IP addresses or hostnames of the external time servers that you want to use. If you specify *internal*, you also need to supply the initial time to which the nodes should synchronize.

**Note:**

- You can specify an external time server during HCP installation only if the HCP system already has connectivity to the time server through the [hcp_system] network.
- HCP creates a comma-delimited list of the external time server IP addresses and hostnames that you specify during the HCP software installation. The comma-delimited list of external time servers can be at most 143 characters long (including the commas).
- If the front-end network IP mode is set to Dual, you can specify both IPv4 and IPv6 addresses for one or more external time servers.

If you start the HCP software installation within the same installation program session in which you specify the initial system time, the installation program adjusts the specified time to account for the time that elapses between when you specify the initial system time and when the program actually installs the software.

Regardless of the time source, you also need to specify a time zone for the HCP system. Normally, this is the time zone in which the system is located.

The installation program can present a list of time zones in which you can find the exact text for the one you want to use. You can also find lists of time zones on the Internet.

The System Management Console includes a page for changing the time settings for the HCP system. This page is intended for use only by authorized HCP service providers.

Changing time settings after the system is installed has certain implications and may cause the system to no longer be in compliance with some government regulations. Because of this, you can configure the HCP system not to allow changes to time settings through the Console. In this case, the system is said to be in **time compliance mode**. Before you install the HCP software, you needs to decide whether the system should be in this mode.

## Internal Configuration Settings

For a software installation, you need to know what values you want to use for several internal configuration settings.

### Storage configuration

During the installation of the HCP software, you need to specify the type of storage the system uses. The options are internal and external.

For RAIN systems, you need to specify that it's internal. For SAIN systems, including those that use internal storage in addition to the SAN storage, you need to specify that the storage is external.

Additionally, for SAIN systems, you need to know:

- Whether any of the storage arrays used by the HCP system are shared with other applications or systems
- Whether the HCP nodes are blades in one or more Hitachi CB 320 servers and, if so, the IP address of the management module (also called the chassis IP address) for each server

**Note:** If the HCP system is using CB 320 servers, for each CB 320 server, you need to add the lowest-numbered storage node in the HCP system to the list of SNMP managers in the server configuration. For the community name, use *public*. To identify the node, use its front-end network IP address. If the node has multiple front-end network IP addresses, you need to create a separate SNMP manager list entry for each front-end network IP address.

If the lowest-numbered node changes at any time (for example, due to prolonged node unavailability or the addition of a node with a lower number), you need to update the configuration of each CB 320 server accordingly.

For information on configuring CB 320 servers, see the applicable Hitachi documentation.

- From your SAN administrator :
  - Whether any nodes in the HCP system have index-only volumes (that is, logical volumes with numbers in the range 64 through 91) and, if so, the intended configuration of those volumes.
  - Whether any nodes in the HCP system have spindown volumes (that is, volumes with numbers in the range 96 through 127) and, if so, the intended configuration of those volumes.
  - If any nodes have spindown volumes, the controller 0 (zero) and controller 1 (one) IP addresses for each array on which those volumes reside. To verify that you've entered these addresses correctly during the HCP installation setup, you should also know the serial number of each array.

**Note:** To enable HCP to use spindown volumes, all controller IP addresses must be routable from the [hcp_system] network.

## Serial number

When you install HCP, you need to specify the unique five-digit serial number for the system. This number is on a label on the rack that houses the HCP nodes. This label is attached to the side of the rack at the bottom, just inside the left rear door.

## Replication

If you purchased the HCP replication feature, you need to enable the feature when you install the HCP software. Enabling replication allows the feature to be available; it does not create a replication link or start replication activity.

**Important:** Do not enable replication if you have not purchased this feature. Doing so makes the system violate your license agreement.

If you enable replication, you also need to know whether the installation is a reinstallation of HCP on one system in a replication pair after a failover to the other system in the pair with DNS failover enabled. DNS failover is the process by which one system in a replication pair is able to service requests targeted to the other system when the first system is unavailable.

If this is such a reinstallation, two different scenarios are possible upon completion:

- Requests that target this system continue to be redirected to the other system until data recovery is complete. To enable this scenario, when you configure the HCP system during the installation procedure, you need to specify that this is a reinstallation.
- This system immediately restarts servicing requests that target it. To enable this scenario, when you configure the HCP system during the installation procedure, you need to specify that this is not a reinstallation.

For more information on replication, see *Replicating Tenants and Namespaces*.

## Customer support contact information

When installing the HCP software, you have the option of specifying HCP customer support contact information. You specify this information as a text string.

After installation, you can use the syscontact field in the HCP MIB file (HCP-MIB.txt) to retrieve the contact information through SNMP.

# Post-installation configuration information

Once the HCP system is running, some additional configuration may be required. You perform this configuration through the HCP System Management Console. For some configuration procedures, you need a user account with the administrator role. For others, you need a user account with the security role.

**Configuration that requires the administrator role**
For post-installation configuration procedures that require the administrator role, you need to know:

- Whether to allow HCP nodes to respond to ping requests. Disabling this option provides extra security for the HCP system.
- Whether to disable the ability for HCP service providers and support personnel to use SSH to log into the HCP nodes.

**Important:** While disabling SSH provides extra security for the HCP system, it also severely limits the ability of service providers and support personnel to provide support for the HCP system.

- Whether to allow HCP nodes to respond to node status commands that check the health of the nodes.
- Whether to create additional networks and domains. In this case, you need to ensure that your networking infrastructure supports the networks you create.
- Creating networks requires that virtual network management be enabled for the system. To have this feature enabled, contact your authorized HCP service provider.
- Whether to install a new SSL server certificate for the domain created during installation. In this case, you need to either have an SSL server certificate to install or have the information needed to generate a certificate signing request.
- Whether to keep deletion records in the transaction log after objects are deleted, and if so, how long to keep them.
- Whether to change the storage tiering threshold.

- Whether to create any new service schedules and, if so, the criteria for scheduling services in them.
- Whether to modify the default service plan that is created during installation. For example, you can modify the default service plan to change the default ingest tier data protection level (DPL) and metadata protection level (MPL) settings or to create a new default storage tiering strategy.
- Whether to create any service plans and, if so, the name and configuration of each one.
- Whether to configure the HDDS search facility.
- Which search facility, if any, to select for use with the HCP Search Console.
- Whether to enable integration with Hitachi Device Manager. If you enable this option, you need to know the Device Manager URL, username, and password.

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

- Whether to create a replication link (only if you've purchased the replication feature) and, if so, the link properties.

**Configuration that requires the security role**

For post-installation configuration procedures that require the security role, you need to know:

- Whether to restrict access to the HCP System Management Console to a limited number of clients and, if so, the IPv4 and IPv6 addresses of those clients
- Whether to restrict access to the HCP Search Console to a limited number of clients and, if so, the IPv4 and IPv6 addresses of those clients
- Whether to enable the HCP management API

- Whether to create additional user accounts and, if so, the properties for each account
- Whether to enable HCP support for Active Directory
- If support for Active Directory is enabled, whether to create HCP group accounts and, if so, which Active Directory groups to create them from

**Configuration that requires either the administrator or security role**
For post-installation configuration procedures that require either the administrator or security role, you need to know:

- Whether to enable monitoring and/or modification of the HCP system through SNMP and, if so, the IP addresses that HCP needs to use to communicate with the clients that can perform these functions.
- Whether to enable syslog logging and, if so, the IP addresses that HCP needs to use to communicate with the syslog servers.
- Whether to enable SNMP logging and, if so, the IP addresses that HCP needs to use to communicate with the SNMP managers.
- Whether to configure a connection to an email server to enable email notification about HCP log messages. If you want to configure a connection to an email server, you need to know:
    - The IP address that HCP needs to use to communicate with the email server that you want to use to send email notification messages
    - Whether to change the email message template or configure recipients for email notification messages

**Note:** To enable communication between HCP and any given SNMP client, SNMP manager, syslog server, or email server, that client or server must have at least one IPv4 or IPv6 address that's routable from the [hcp_ system] network.

**Getting more information**
For more information on all of the above procedures except creating a replication link, see *Administering HCP*. For information on creating a replication link, see *Replicating Tenants and Namespaces*.

3

# Installing the Appliance Operating System

Once the hardware for an HCP system is configured and healthy, you can install the Appliance operating system (OS) on each node. This chapter provides instructions on performing an Appliance OS installation on an HCP system.

**Important:** This chapter assumes that the HCP system hardware is already assembled, installed, configured, and working properly. From this point forward you cannot install more hardware until you finish installing HCP software.

**Caution:** Installing the Appliance OS destroys all data on the system volume and all primary storage volumes. Before installing, be very sure that the server on which you're installing is supposed to be an HCP node.

## Resources you need for an OS installation

To install the Appliance OS, you need:

- From the HCP distributor, the Appliance OS installation USB.

**Tip:** For the quickest installation, have one USB for each node in the HCP system. That way, you can install the OS on multiple nodes at the same time.

- A USB keyboard and VGA monitor.

# Before you install the OS

Before you install the Appliance OS:

- Complete the "Appliance OS Installation Information" on page 63 so the information you need for the OS installation is readily available.
- Check the HCP release notes for any last minute installation information.
- Ensure that the BIOS date in the node is correct. The OS installation fails if the BIOS date is one or more years in the past.
- For SAIN systems, verify that:
  - The formatting of all LUNs used by HCP is 100 percent complete. (When a LUN is completely formatted, its state is Normal.)
  - Each node has full connectivity to the storage arrays. If it doesn't, please contact your authorized HCP service provider
  - For each node, LUN 0 (zero) is configured for the OS, and sufficient storage is allocated for the data, index, shared, and spindown volumes, as applicable. If these conditions aren't true, submit a request to your SAN administrator to reconfigure the storage.

**Note:** For HCP to use storage in an array in the AMS 2000 or HUS family, Task Management Isolation Mode must be enabled on the array.

- Optionally, for SAIN systems, submit a request to your SAN administrator to review the storage configuration (see "Optionally reviewing the storage configuration" on the facing page).
- For SAIN systems with spindown storage, submit a request to your SAN administrator to spin up all spindown volumes that are allocated to the HCP system.
- If the console you're using is not already connected to the node, connect it.

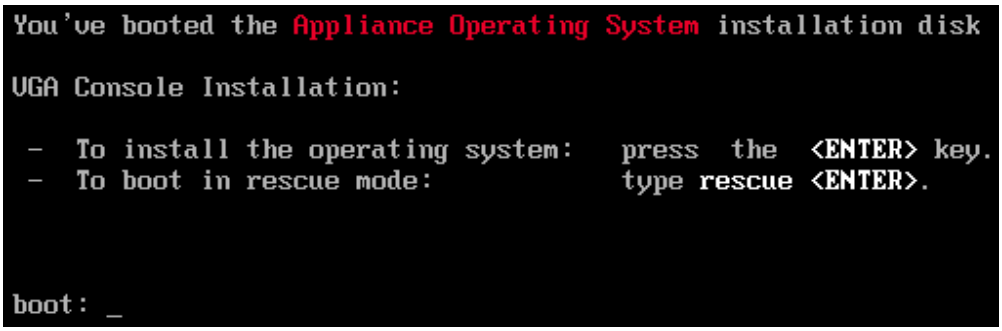
**Tip:** You need the console only for the first part of the OS installation. As soon as you've completed that part of the installation, you can disconnect the console. This enables you to share the console among nodes when installing the OS on multiple nodes at the same time.

# Optionally reviewing the storage configuration

Before installing the OS for a SAIN system, you may want to submit a request to your SAN administrator to review the storage configuration for one or more nodes. To review the storage configuration for a node:

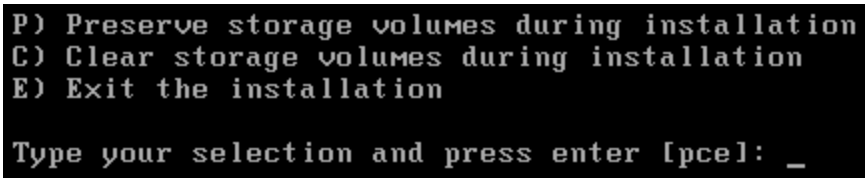
1. Connect the keyboard and monitor to the node.
2. If you are using a DVD, connect the external DVD drive to a USB port on the node.
3. Insert the Appliance OS installation USB into a USB port on the node or the DVD into the external DVD drive.
4. Power on or reboot the node.

   The installation program prompts for the installation mode.




5. Either press Enter, or let the program default to the installation option after 75 seconds.

   The installation program prompts for the procedure you want to perform.




6. Enter *e*.

   The installation program exits.

7. At the command prompt, enter:

   ```
   fchbainfo | more
   ```

   The console displays the first screenful of storage configuration information for the node:

   - To page through the rest of the information, use the space bar.
   - To stop the display before you've viewed all the configuration information, press the Q key.

## Performing the OS installation

To install the Appliance OS on a node:

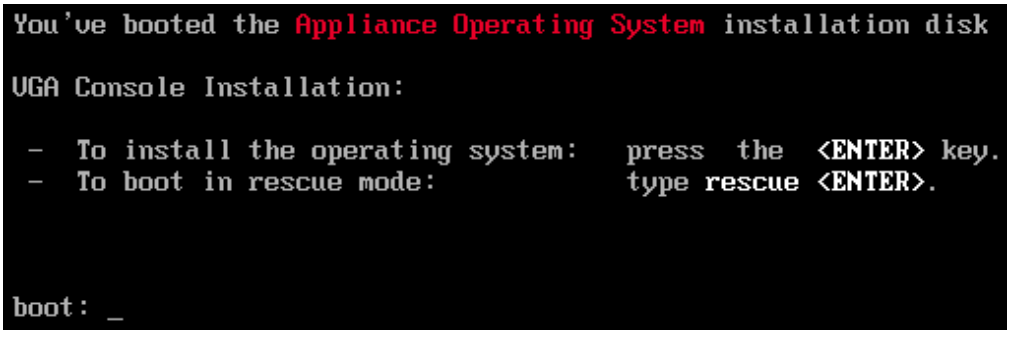
1. Connect the keyboard and monitor to the node.
2. If you are using the DVD, connect the external DVD drive to a USB port on the node
3. Insert the Appliance OS USB stick into a USB port on the nodeor the DVD into the external drive.
4. Reboot the node.
5. If this is the first time you are installing the OS, skip ahead to sub-step 8. If there was a previous failure installing the OS, and you are attempting to re-install the OS, continue with the following instructions.
6. During the POST portion of the system boot, press the F11 key to enter the Boot Options Menu.

7. When prompted to enter the password, type hosyu95 and press Enter.


8. At the Boot Options Menu, as shown below, arrow down to select the USB stick as the boot device and press Enter.

**Note:** Depending on the USB stick used, the text shown below may be different.


9. The installation program prompts for the installation mode.



**10.** Either press Enter, or let the program default to the installation option after 75 seconds.

The installation program prompts whether to preserve or clear existing storage volumes.

```
P) Preserve storage volumes during installation
C) Clear storage volumes during installation
E) Exit the installation

Type your selection and press enter [pce]: _
```

**11.** Enter *c* to clear existing storage volumes or *p* to preserve existing storage volumes.

**12.** In response to the confirming prompt, enter *y*.

```
You have chosen to clear the storage volumes

  THIS OPTION WILL DESTROY ANY DATA ON THE STORAGE VOLUMES.

Are you sure you want to clear the storage volumes (yN): _
```

If the installation program detects that the Appliance operating system is already installed on the node, it prompts you to confirm that you want to continue the Appliance OS installation.

Enter *YES* in response to this prompt and press Enter.

```
The Appliance OS installer has detected that you are using a volume
that was previously used as an OS volume for HCP.

You may be trying to install the OS on an already installed node.

If the volume is on a SAN array, it may be improperly mapped.

If either of these is the case and you install the OS on this volume,
any prior system configuration and HCP installation will be destroyed,
and you will need to perform the node recovery procedure.

Are you sure you want to install the OS?

Type 'YES' to continue, 'NO' to exit the installation: _
```

Take one of these actions:

- To continue the OS installation, enter *YES*. This value is case sensitive.

For SAIN systems, if the installation program detects that the storage that's managed by the node has failed over to the peer node, the program prompts you to decide what to do about the failure.

```
R) Rescan for failed-over volumes
I) Ignore the failed-over state and clear the volumes
E) Exit the installation

Type your selection and press Enter [rie]: _
```

Take one of these actions:

- If you are reinstalling the OS as part of a node recovery procedure and the peer node is healthy, use the HCP System Management Console to first disable zero-copy failover and then restart the peer node. Then enter *r* in response to the prompt shown above.
- If you are reinstalling the OS as part of a fresh installation of HCP or as part of a node recovery procedure where the peer node is not healthy, enter *i*.
- To continue the installation, enter *i*.
- To stop the OS installation, enter *e*. To restart OS installation after entering *e*, you need to reboot the node.

○ To stop the OS installation, enter *NO*. This value is case sensitive.

The installation program exits. To restart the OS installation after entering *NO*, you need to reboot the node.

**13.** When prompted, enter the bonding mode for the HCP system. Valid responses are *active-backup* and *802.3ad*.

```
Enter the front-end bonding mode ([active-backup],802.3ad):
```

**14.** When prompted, enter the front-end network IP mode for the node. The IP mode that you specify is used to set both the system-level IP mode and the [hcp_system] network IP mode. Valid responses are *IPv4*, *IPv6*, and *Dual*.

```
Enter the front-end network IP mode ([IPv4],IPv6,Dual):
```

**15.** If the installer detects both BaseT and SFP+ network interface cards in this system, you will be prompted to enter the front-end network interface types for the HCP system. Valid responses are *BaseT*, *SFP+.*

```
Enter the front-end network interface type   ([BaseT],SFP+):
```

**16.** When prompted, enter *y* to indicate that you want to provide a VLAN ID for the [hcp_system] network or *n* to indicate that you don't want to provide a VLAN ID.

```
Do you want to provide a VLAN ID for the front-end network? [n]:
```

**17.** If you entered *y* in response to the previous step, when prompted, enter the VLAN ID for the [hcp_system] network. Valid values are integers in the range 0001 through 4,094. The VLAN ID you specify can include leading zeroes but cannot be more than four digits long.

```
Enter the front-end network VLAN ID [0000]:
```

If you entered *n* in response to the prompt in the previous step, the installation program does not prompt you to enter a VLAN ID.

**18.** If you entered *IPv4* or *Dual* in response to the prompt in step 14 above, specify the IPv4 node IP address, subnet mask, and gateway IP address for the front-end network, otherwise go to step 19.

**a.** When prompted, enter the IPv4 address assigned to the node for the front-end network.

```
Enter the front-end IPv4 IP address []:
                              --->
```

**b.** When prompted, enter the IPv4 address subnet mask for the front-end network.

```
Enter the front-end IPv4 netmask [255.255.255.0]:
                              --->
```

**c.** When prompted, enter the IPv4 gateway IP address for the front-end network.

```
Enter the front-end IPv4 gateway IP address [172.20.43.254]:
                             --->
```

If you entered *IPv4* in response to the prompt in step 14 above, you are finished entering front-end network configuration information for the node. Skip the next step in this procedure, and go to step 20. If you entered *IPv6* or *Dual* proceed to step 19.

**19.** If you entered *IPv6* or *Dual* in response to the prompt in step 14 above, specify the primary IPv6 node IP address, prefix length, and gateway IP address for the front-end network:

**a.** When prompted, enter the primary IPv6 address assigned to the node for the front-end network.

```
Enter the front-end IPv6 IP address []:
                                --->
```

**b.** When prompted, enter the primary IPv6 address prefix length for the front-end network.

```
Enter the front-end IPv6 prefix length [64]:
                                --->
```

**c.** When prompted, enter the primary IPv6 gateway IP address for the front-end network.

```
Enter the front-end IPv6 gateway IP address []:
                                --->
```

**d.** When prompted, enter *y* to indicate that you want to assign a secondary IPv6 address to the node for the front-end network or *n* to indicate that you don't want to assign a secondary IPv6 address to the node for the front-end network.

```
Do you want to provide a second IP for the front-end IPv6 network? [n]:
```

**e.** If you entered *y* in response to the prompt in step d above, specify the secondary IPv6 node IP address, prefix length, and gateway IP address for the front-end network:

**1.** When prompted, enter the secondary IPv6 address assigned to the node for the front-end network.

```
Enter the front-end IPv6 secondary IP address []:
                                --->
```

2. When prompted, enter the secondary IPv6 address prefix length for the front-end network.

```
Enter the front-end IPv6 secondary prefix length [64]:
                              --->
```

3. When prompted, enter the secondary IPv6 gateway IP address for the front-end network.

```
Enter the front-end IPv6 secondary gateway IP address []:
                              --->
```

**20.** When prompted, enter the back-end network IP address for the node.

```
Enter the back-end IPv4 IP address []:
                              --->
```

The installation program displays your responses to all of the previous prompts and asks you to confirm them.

**21.** In response to the confirming prompt:

- To confirm your responses, enter *y*.
- To change any of your responses, enter *n*. In this case, the installation program repeats the prompts, starting again with the front-end network bonding mode.

At this point, the installation program runs a precheck to see if LUNs 0 or 128 exist on the nodes. If the precheck finds these LUNs on a G10 Node, the install fails. You need to remove the LUNs before proceeding.

The installation program reformats the system volume and installs the OS. This process takes several minutes. While installing the OS, the installer should report its progress to the console.

If the OS installation is not proceeding as expected, you can press Alt+F2 to display a command prompt. This enables you to enter commands that can help you diagnose the problem. Pressing Alt+F2 to display a command prompt works only during OS installation. To return to the OS installation display, press Alt+F1.

When the installation is complete, the node reboots automatically. If the node does not reboot automatically, the OS installation failed. In this case, please contact your authorized HCP service provider for help.

Once the node reboots and shows the AOS login screen on the console the node is ready for the HCP software installation. You should remove the USB installation media from the node at this time.

4

# Installing the HCP software

After installing the Appliance OS on every node in an HCP system, you can install the HCP software. This chapter describes the program you use to install the software and contains installation instructions.

**Important:** This chapter assumes that the OS is installed and healthy on each node in the system.

**Caution:**

- Installing the HCP software erases everything on the HCP nodes except the OS. Before installing, be very sure you're supposed to be doing a fresh installation and not an upgrade.
- The HCP software installation program also provides access to the procedures for upgrading and adding nodes and storage to an HCP system. *These procedures are reserved for authorized HCP service providers. Do not try to perform them yourself.* Performing these procedures incorrectly carries the risk of destroying data in the repository and/or leaving the system inoperable.

## HCP Setup program

The program that installs the HCP software is named **HCP Setup**. This program includes a wizard that walks you through the HCP system configuration.

## Using the HCP Setup wizard menus

The HCP Setup wizard is menu driven. Below each menu, the wizard prompts for the number or letter of a menu option, as in this example showing the HCP Setup wizard **New Install** menu:

```
HCP Setup: New Install Menu
===========================================

[1] HCP Nodes
[2] Distributor/OEM Key Access (Arizona)
[3] Networking Settings
[4] DNS Settings
[5] Time Settings
[6] Internal Configuration Settings
[7] Encryption Settings

[r] Restore Default Configuration
[q] Review Current Configuration

[x] Install a New HCP System with This Configuration

[w] Exit/Write out Configuration File
[q] Return to Configuration Menu

Enter your choice.
[Default: 2]: _
```

Each prompt for a menu selection displays a default value:

- To accept the default, press Enter.
- To select a different option, type the number or letter you want. Then press Enter.

You use the menu options to navigate through the wizard and to enter configuration values:

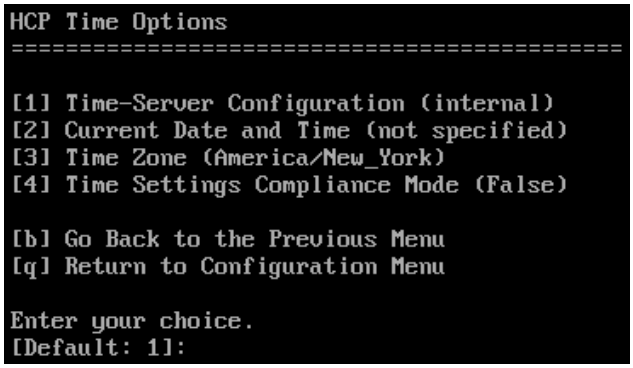
- When you select a numbered menu option, the wizard displays either a lower-level menu or a prompt for a configuration value.
- From any lower-level menu, you can select the **b** menu option to go back to the previous menu.
- When you return to a menu, the default option is the one following the option you most recently selected.
- From any menu, you can select the **q** option to exit the wizard without saving any of the configuration information you've entered.

- If you select an option to perform an operation that cannot be undone (for example, the **q** option described above), the wizard prompts you twice to confirm your selection before performing the operation.

For pictures of all the HCP Setup wizard menus, see Appendix B: "HCP Setup wizard menus" on page 69.

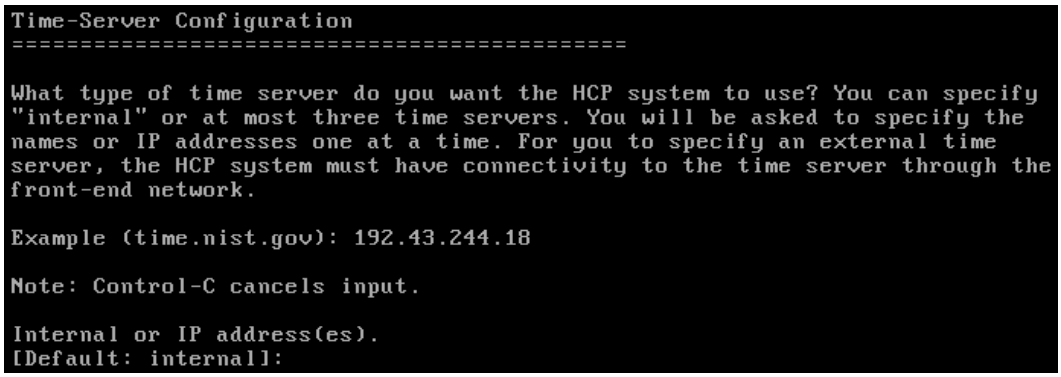
## Specifying configuration values

The options displayed on the lowest-level menus in the HCP Setup wizard are used to enter values for specific configuration settings. For example, the **HCP Time Options** menu displays the options used to enter values for the HCP system time configuration settings, as shown in the example below:




Most of the options in these menus display the currently configured value as the default.

When you select an option to specify values for one or more configuration settings, the wizard prompts you to enter the value you want to use for each setting and displays the default value for that setting, as in this example:




When specifying configuration values in the wizard:

- When the wizard prompts you to enter a value for a configuration setting, to accept the default value that's displayed, press Enter.
- When the wizard prompts you to enter **yes** or **no** in response to a question, *y*, *yes*, *n*, and *no* are all acceptable responses.
- The wizard prompts you to confirm each configuration value that you specify.
- For certain settings, changing the currently configured value for one setting may change the default configuration values for other settings. For example, changing the time server configuration setting from **internal** to a specified external time server changes the default value for the **Current Date and Time** setting to **not available with time server**.
- After selecting an option from a menu, if you're prompted to enter a value for a specific configuration setting, you can press Ctrl+C to return to the menu without changing the currently configured value for that setting.
- At any time, you can use the **v** option on the **New Install** menu to review the current configuration settings.

## Saving the system configuration

At any time during the configuration process, you can save the configuration you've specified so far and exit the wizard. To do this, you use the **w** option on the **New Install** menu. When you restart the wizard, it reads

in the saved configuration. This enables you to configure the HCP system in multiple wizard sessions.

### Resetting configuration options to their default values

While using the HCP Setup wizard, you can use the menu options to return to any configuration settings page in the wizard and change any of the configuration values you've already entered. You can also reset all configuration settings to their default values. To do this, you use the **r** option on the **New Install** menu.

## Resources you need for an HCP software installation

To install the HCP software, you need:

- From the HCP distributor:
  - The HCP software installation USB flash drive or DVD
  - The name of the distributor key for the installation
- If you are using a DVD for the software installation, an external DVD drive.
- A keyboard and monitor

## Before you install the HCP software

Before you install the HCP software:

- Complete the "HCP Software Installation Information" on page 65 so the information you need for the HCP software installation is readily available.
- Check the HCP release notes for any last minute installation information.
- Ensure that the Appliance OS is installed on each node in the system and that each node is running.
- For SAIN systems with spindown storage, ensure that all spindown volumes allocated to the HCP system are spun up.

- If you configured the Appliance OS for link aggregation, ensure that the front-end Ethernet switch is already configured for 802.3ad bonding.

**Note:** If this is the first time you're installing an HCP system, be sure to read "HCP Setup program" on page 41 before you begin.

# Performing the HCP software installation

To install the software for an HCP system, follow the steps outlined in the table below. If you want to enable encryption, please contact your service provider before beginning the installation.

**Note:** While you can install HCP software without assistance from support personnel, it is not possible to enable data at rest encryption (DARE) unless there is an authorized HCP service provider on site. DARE encrypts data on primary storage and data tiered to external storage pools. If you plan to utilize DARE features, please contact your authorized HCP service provider before performing the software installation.

| Step | Activity | More information |
|---|---|---|
| 1 | Log into the highest-numbered storage node in the HCP system. | Step 1: "Log in" on the facing page |
| 2 | Retrieve the HCP software installation files. | Step 2 (conditional): "Retrieve the HCP software installation files" on page 49 |
| 3 | Identify the nodes in the HCP system. | Step 3: "Identify the nodes in the HCP system" on page 50 |
| 4 | Configure the HCP system. | Step 4: "Configure the HCP system" on page 52 |
| 5 | Execute the installation. | Step 5: "Execute the installation" on page 57 |

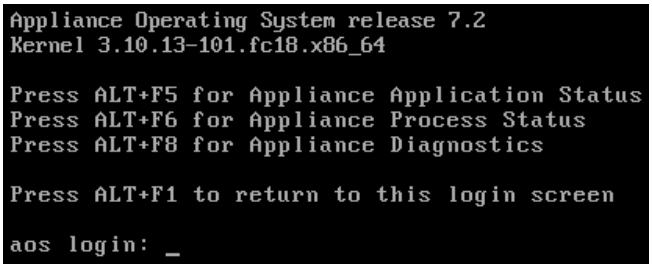
**Note:** For HCP SAIN systems, if any of the nodes in the system do not have the required version of the HBA firmware, the installation fails.

## Step 1: Log in

To begin the procedure for installing the HCP software, you need to log in as the *install* user and then change the password for that user:

1. If you are using a DVD to perform the installation, connect the external DVD drive to a USB port on the node.
2. Connect the keyboard and monitor to the highest-numbered storage node in the system.

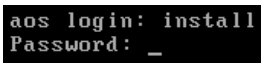
   The console displays the login prompt.




**Tip:** If you don't see the login prompt, press Enter a few times.

3. Insert the HCP software installation DVD into the DVD drive for that node or the USB into the USB port.
4. Enter: *install*

   A password prompt appears.




5. Enter: *Chang3Me!*

   As you type, the characters do not show.

**Note:** If you've previously changed the password for the *install* user, enter that password instead. Then continue the installation procedure from where you ended the last session.

If you haven't previously changed the *install* user password, HCP Setup prompts for the current password again.

```
Changing password for user install.
Changing password for install
(current) UNIX password: _
```

6. Enter: *Chang3Me!*

   The system prompts for a new password for the *install* user.

   ```
   New password:
   ```

7. Enter a new password for the *install* user.

   Passwords must follow the standard rules for Unix passwords. In particular, to be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and special characters. Also, a password cannot be a word found in the dictionary.

Changing the *install* user password is a one-time event. Be sure to remember the new password. You will need it if you use multiple HCP Setup sessions to perform the HCP software installation. You will also need to give it to your authorized HCP service provider for procedures such as upgrades and node additions.

**Tip:** For the new password, use **hcpinsta11**, where the last two characters are the number one.

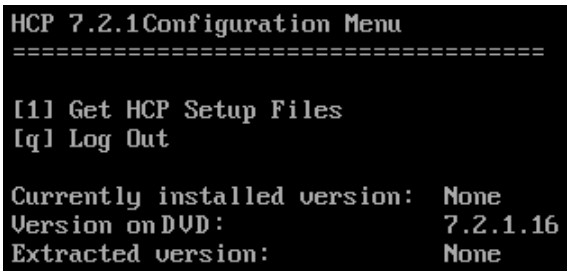
8. When prompted, enter the new password again.

   The system changes the password and prompts you to continue.

   ```
   Password updated.

   If you install your application from this node, the new password
   will be propagated to all other nodes.

   Press ENTER to continue: _
   ```

9. Press Enter.

   The **HCP 7.3 Configuration** menu appears.




## Step 2 (conditional): Retrieve the HCP software installation files

The HCP software installation files are extracted as part of the OS installation. Confirm this by checking that the **Extracted version** listed in the **HCP Configuration Menu** matches the version you are installing. If the **Extracted version** listed in the **HCP Configuration Menu** is **None**, the installation files have not been extracted in which case you need to retrieve them from the USB or DVD.

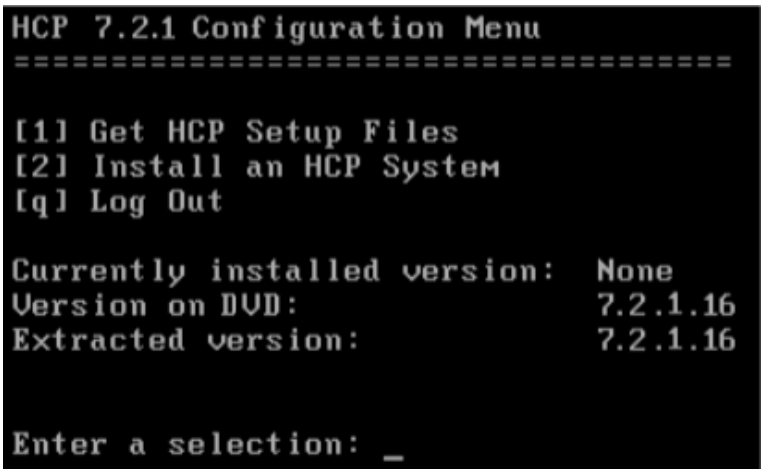
To retrieve the HCP software installation files from the HCP software installation USB or DVD:

1. From the **HCP 7.3 Configuration** menu, enter **1** (one) to retrieve the installation files from the USB or DVD.

2. In response to the confirming prompt, enter *y* or *yes* to confirm your entry or *n* or *no* to try again.

   When you enter *y* or *yes*, HCP Setup copies the HCP software installation files from the USB or DVD to the node and prompts for you to remove the USB or ejects the DVD tray.

The **HCP 7.3 Configuration** menu reappears. The menu now includes the option to install HCP.




**Note:** Do not remove the HCP software installation USB or DVD until HCP requests that you remove it.

## Step 3: Identify the nodes in the HCP system

To identify the nodes in the HCP system:

1. From the **HCP 7.3 Configuration** menu, enter **3** to run the HCP Setup wizard.
2. In response to the confirming prompt, enter *y* or *yes* to confirm your entry or *n* or *no* to try again.

   When you enter *y* or *yes*, a data-in-flight encryption installation user prompt appears.
3. In response to the data-in-flight encryption prompt, enter *y* or *yes*.
4. In response to the confirming prompt, enter *y* or *yes* to confirm your entry or *n* or *no* to try again.

   When you enter *y* or *yes*, the HCP Setup wizard **New Install** menu appears.

```
HCP Setup: New Install Menu
===========================================

[1] HCP Nodes

[r] Restore Default Configuration
[v] Review Current Configuration

[x] Install a New HCP System with This Configuration

[w] Exit/Write out Configuration File
[q] Return to Configuration Menu

Enter your choice.
[Default: 1]: _
```

5. Enter **1** to identify the nodes in the HCP system.

   The **HCP Nodes** menu appears.

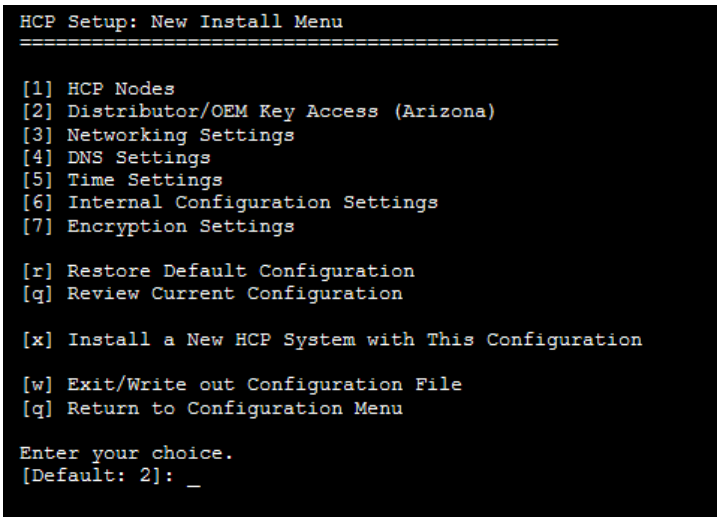
```
HCP Nodes Menu
==============================================

[1] Storage Node Back-end IP Addresses

[b] Go Back to the Previous Menu
[q] Return to Configuration Menu

Enter your choice.
[Default: 1]:
```

6. From the **HCP Nodes** menu, enter **1** to identify the storage nodes in the HCP system. Use the *back-end IP address* to identify each node.

**Tip:** If you chose to enter the node IP addresses as literal values, enter the IP address of the lowest-numbered node first. For subsequent IP addresses, HCP Setup presents a default value that's one greater than the previous IP address that you entered.

7. From the **HCP Nodes** menu, enter b to return to the **New Install** menu.

   The **New Install** menu now includes additional options for configuring the HCP system.




## Step 4: Configure the HCP system

From the **New Install** menu, execute the additional options for configuring the HCP system. Each option either opens a lower-level menu with configuration options or opens a page in the wizard that displays a prompt to enter a value for a configuration setting.

For pictures of all the HCP Setup wizard menus, see Appendix B: "HCP Setup wizard menus" on page 69.

To configure the HCP system:

1. Enter **3** to change these networking settings:
   - One or more of the IPv4 and IPv6 gateway IP addresses that you specified during the OS installation
   - Multicast IP address
2. Enter **4** to change these DNS settings:
   - Whether HCP should use DNS services
   - Domain name for the HCP system (this is required regardless of whether you use DNS)
   - The list of IPv4 and IPv6 addresses that HCP needs to use to forward DNS requests to each of your corporate DNS servers

**Note:** Each DNS server IP address that you specify must be routable from the [hcp_system] network.

**Tip:** If the front-end network IP mode is set to Dual, you should specify both IPv4 and IPv6 DNS server IP addresses. This ensures that all client requests can use the HCP system domain name for access to the system, regardless of which type(s) of IP addresses each client is configured to use.

3. Enter **5** to change these time settings:
   - Whether the time source is internal or external, and if it's external, the IP addresses or hostnames of the time servers that you want to use with HCP

**Note:**
- HCP creates a comma-delimited list of the external time server IP addresses and hostnames that you specify. The comma-delimited list of external time servers can be at most 143 characters long (including the commas).
- Each external time server IP address that you specify must be routable from the [hcp_system] network. If you specify the hostname of an external time server, that server must have at least one IPv4 or IPv6 address that's routable from the [hcp_system] network.

   - Current date and time (internal time source only)
   - Time zone

**Tip:** To see a list of valid time zones, enter *view*. To return to the prompt to enter a time zone for the HCP system, press the Q key.

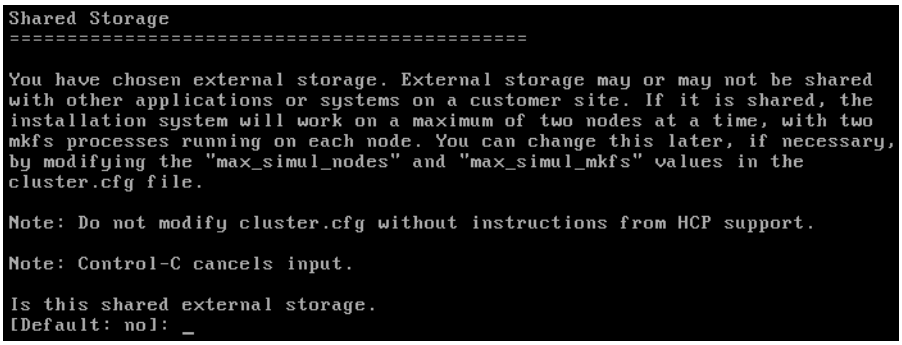
   - Time compliance mode

4. Enter **6** to change these internal settings:
   - Whether the HCP storage is internal or external.

     **If you specify internal storage,** continue by selecting the option to set the serial number for the system.

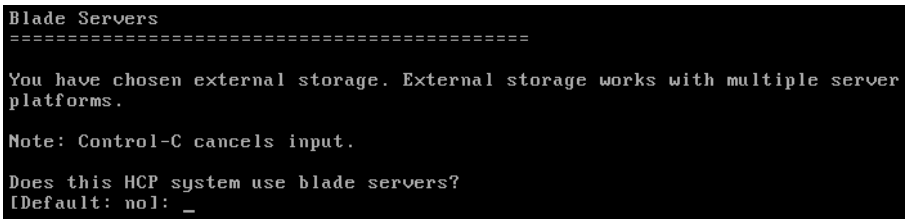
**If you specify external storage,** the wizard prompts you to:

1. Enter *y* or *yes* to indicate that the storage is shared with other applications, or enter *n* or *no* to indicate that the storage is used exclusively for HCP.




   If you answer *y* or *yes*, HCP Setup slows down its formatting during installation to minimize the disruption to the other applications that use the shared storage.

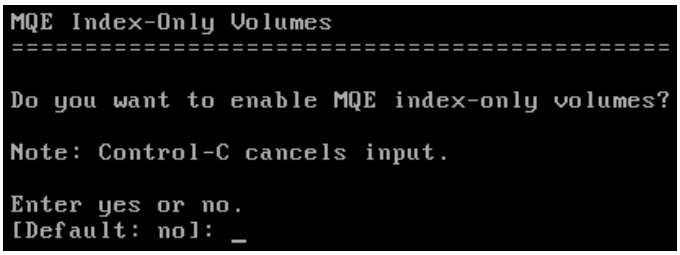
2. Enter *y* or *yes* to indicate that the HCP system uses blade servers, or enter *n* or *no* to indicate that the HCP system doesn't use blade servers.




   If you answer *y* or *yes*, the wizard prompts you to enter the IP addresses that HCP needs to use to communicate with the blade server chassis.

**At this point, if you've specified external storage,** HCP Setup analyzes the identified storage nodes to determine whether they have any logical volumes in the index-only and spindown ranges:

1. **If HCP Setup finds any index-only volumes,** the wizard prompts you to indicate whether you want to enable index-only volumes.




   In response to this prompt, enter *y* or *yes* if you want to enable index-only volumes or *n* or *no* if you don't want to enable them.

   **If you enter** *y* **or** *yes* **and all the storage nodes have the same number of index volumes (more than one each),** the wizard lists all the index volumes and prompts you to confirm that the list is correct:

   - Enter *y* or *yes* to confirm that the list is correct and continue the installation.
   - Enter *n* or *no* to return to the **HCP 7.3 Configuration** menu.

     If the list of index volumes is not correct, tell your SAN administrator to reconfigure the logical volumes at the storage tier. After the reconfiguration is complete, reinstall the OS on the affected nodes. Then start the HCP software installation procedure again.

   **If you enter** *y* **or** *yes* **and not all the storage nodes have the same number of index volumes or if you enter** *n* **or** *no***,** the wizard returns an error.

   After returning an error, the wizard prompts you to press Enter:

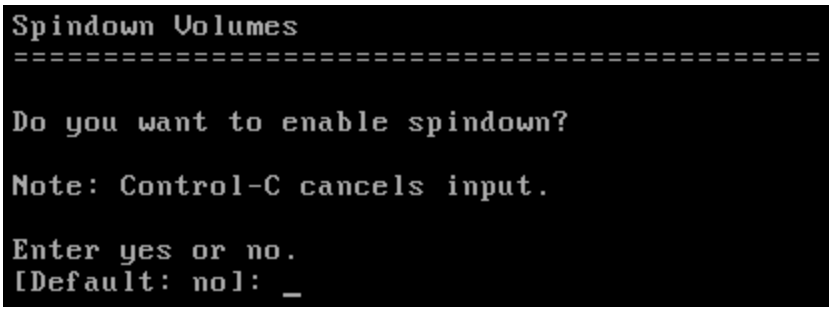
   1. Press Enter.

      The **HCP 7.3 Configuration** menu reappears.

2. If the storage configuration is incorrect, tell your SAN administrator to reconfigure the logical volumes at the storage tier. Then wait until the reconfiguration is complete.

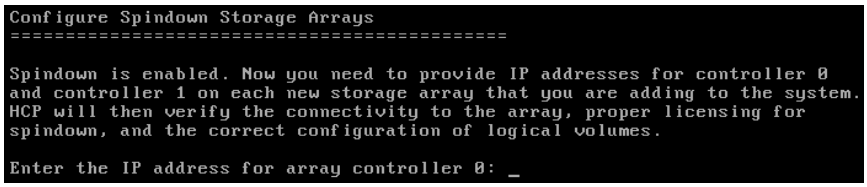
3. Reinstall the OS on the affected nodes. Then start the HCP software installation procedure again.

2. **If HCP Setup finds any spindown volumes,** the wizard prompts you to indicate whether or not you want to enable spindown.




In response to this prompt, enter *y* or *yes* if you want to enable spindown or *n* or *no* if you don't want to enable it:

- **If you enter** *y* **or** *yes***,** the wizard prompts you to enter the IP addresses that HCP needs to use to communicate with the controllers in each of the storage arrays that have spindown volumes for the HCP nodes.




After you enter all of the controller IP addresses, the wizard lists all the spindown volumes and prompts you to confirm that the list is correct, enter *y* or *yes* to confirm that the list is correct and continue the installation or enter *n* or *no* to return to the **HCP 7.3 Configuration** menu.

If the list of spindown volumes is not correct, tell your SAN administrator to reconfigure the logical volumes at the

storage tier. After the reconfiguration is complete, reinstall the OS on the affected nodes. Then start the HCP software installation procedure again.

- **If you enter** *n* **or** *no***,** the wizard returns an error. To continue, press Enter, reinstall the OS on the affected nodes, and start the HCP software installation procedure again.

- HCP system serial number.

- Enter *y* or *yes* to indicate that you want to enable replication, or enter *n* or *no* to indicate that you don't want to enable replication.

**Important:** Do not enable replication if you have not purchased this feature. Doing so makes the system violate the customer's license agreement.

If you answer *y* or *yes* to enable replication, the wizard prompts you to indicate whether this is a reinstallation of one system in a replication pair after a failover to the other system in the pair with DNS failover enabled. If you enter *y* or *yes* in response to this prompt, HCP continues to handle all requests that target replicated namespaces in the system by redirecting those requests to the other system until failback occurs.

- Specify contact information for HCP customer support.

  To specify no contact information, enter a space.

5. Encryption is disabled by default. If you want to enable encryption, contact your authorized HCP service provider.

## Step 5: Execute the installation

**Note:** If possible, if you enabled primary storage encryption in the system configuration, your security administrator should be present for this step. The security administrator can then be the sole person to see the encryption key.

To execute the HCP software installation:

1. From the **New Install** menu, enter **x**.

2. In response to the prompt about data-in-flight encryption, take one of these actions:

   - If data-in-flight encryption is configured correctly:

     1. Enter *y* or *yes*.
     2. In response to the confirming prompt enter *y* or *yes* to confirm your entry or *n* or *no* to try again.

        When you enter *y* or *yes*, the wizard displays the system configuration.

   - If data-in-flight encryption is not configured correctly:

     1. Enter *n* or *no*.
     2. In response to the confirming prompt enter *y* or *yes* to confirm your entry or *n* or *no* to try again.

        When you enter *y* or *yes*, the wizard returns to the **New Install** menu, from which you can correct the configuration.

3. Review the configuration.
4. Take one of these actions:

   - If the configuration is correct:

     1. Enter *y* or *yes*.
     2. In response to the confirming prompt, enter *y* or *yes* to confirm your entry or *n* or *no* to try again.

     When you enter *y* or *yes*, HCP Setup performs a set of installation prechecks and, if they are successful, installs the HCP software on all nodes in the system. This can take from several minutes to several hours, depending on the size of the logical volumes.

**Note:** As part of the precheck process, the installation program checks whether each node has more than the minimum recommended amount of RAM (32 GB). If one or more nodes have less than 32 GB of RAM, the installation program prompts you to enter *y* or *yes* to continue the installation, or enter *n* or *no* to cancel the installation and return to the **HCP 7.3 Configuration** menu.

When the installation is complete, HCP Setup logs you out and reboots the nodes. The console then displays the login prompt.

If HCP Setup exits at any time before the installation processing is complete, make a note of all error messages and then contact your authorized HCP service provider for help.

- If the configuration is not correct:

  1. Enter *n* or *no*.
  2. In response to the confirming prompt, enter *y* or *yes* to confirm your entry or *n* or *no* to try again.

  When you enter *y* or *yes*, the wizard returns to the **New Install** menu, from which you can correct the configuration.

# Verifying the HCP installation

You use the HCP System Management Console to verify that the HCP system installed correctly. To do this:

You use the HCP System Management Console to verify that the HCP system installed correctly. To do this:

1. Open the System Management Console for the HCP system in a web browser on a client computer:

   - If the HCP system is configured for DNS, enter this URL:

     **https://admin.***hcp-domain-name*:8000

   - If the HCP system is not configured for DNS, enter this URL:

     **https://***node-ip-address*:8000

     *node-ip-address* is any valid front-end network IP address for any storage node in the HCP system.

**Note:** If you inadvertently use *http* instead of *https* in the URL, the browser returns an error. Enter the URL again, this time using https.

2. When prompted, accept the self-signed HCP SSL server certificate either permanently or temporarily for this Console session only. You would do the latter, for example, if you plans to install a trusted certificate later on.

   The System Management Console login page appears.

   If the browser cannot find the System Management Console login page, wait a few minutes; then try again.

   If the login page still doesn't open after a few minutes, please contact your authorized HCP service provider for help.

3. Check the serial number on the login page. If the serial number is incorrect, contact your authorized HCP service provider for help.

4. Log into the System Management Console with this username and password:

   Username: **security**
   Password: **Chang3Me!**

   The Console displays either the **Change Password** page or the **Hardware** page.

   If the Console displays the **Hardware** page, the nodes are still in the process of starting HCP. This process can take several minutes. When more than half of the nodes have completed their startup processing, the Console automatically displays the **Change Password** page.

   If the **Hardware** page remains displayed after several minutes, please contact your authorized HCP service provider for help.

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

   - In the **Existing Password** field, type: *Chang3Me!*
   - In the **New Password** field, type a new password. Passwords must be from one through 64 characters long and can contain any UTF-8 characters, including white space. The minimum 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. For example, *P@sswOrd* is a valid password; *password* is not.

- In the **Confirm New Password** field, type your new password again.

6. Click on the **Update Password** button.
7. In the top-level menu, click on **Hardware**.
8. 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), the installation was successful, and you can begin creating tenants and namespaces. However, you may not want to do this until after the additional system setup is complete.

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 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.

9. Take one of these actions:
   - Perform additional system configuration, as described in "Performing additional system configuration procedures" below. Do this only if the installation was successful.
   - Log out of the System Management Console and close the browser window to ensure that no one can return to the Console without a fresh login.

# Performing additional system configuration procedures

After verifying that the HCP system installed correctly, you can perform additional system configuration procedures, as necessary, to configure HCP to meet your business requirements. For example, you can enable syslog logging or disable **ping**.

To perform additional system configuration procedures:

1. Log into the HCP System Management Console as the *security* user (if you're not already logged in).
2. Create a new user account with the administrator role.

   Alternatively, you can add the administrator role to the *security* user account and then skip step 3 below.
3. Log out of the System Management Console. Then log in again using the new account with the administrator role.
4. Perform the required configuration procedures.
5. Log out of the System Management Console. Then log in again using the *security* account.
6. Log out of the System Management Console and close the browser window to ensure that no one can return to the Console without a fresh login.

For information on creating user accounts and performing system configuration procedures, see *Administering HCP* .

# Forms

This appendix contains forms that you can use to facilitate some of the procedures presented in this book:

- "Appliance OS Installation Information" below lets you record the information you need for an Appliance OS installation.
- "HCP Software Installation Information" on page 65 lets you record the information you need for an HCP software installation.
- "Encryption Key" on page 68 lets you record the encryption key displayed during HCP installation processing.

## Appliance OS Installation Information

*Use this form to record the information for an Appliance OS installation.*

**General front-end network configuration settings**

Front-end network bonding mode: ☐ Active-backup ☐ 802.3ad

Front-end network IP mode: ☐ IPv4 ☐ IPv6 ☐ Dual

Front-end network VLAN ID: ☐ Yes:_____ ☐ No

**Front-end network subnet configuration settings**

IPv4 address subnet mask:

IPv4 gateway IP address:

Primary IPv6 address prefix length:

Primary IPv6 gateway IP address:

Secondary IPv6 address prefix length:

Secondary IPv6 gateway IP address:

**Front-end and back-end network IP addresses assigned to the node**

For each node, specify the front-end network IPv4 address/primary IPv6 address/secondary IPv6 address/back-end network IP address:

Node 1:

Node 2:

Node 3:

Node 4:

Node 5:

Node 6:

Node 7:

Node 8:

Node 9:

Node 10:

Node 11:

Node 12:

# HCP Software Installation Information

*Use this form to record the information for an HCP software installation.*

**Storage nodes**

Back-end IP addresses of storage nodes (list or range):

**Distributor key**

Distributor key:

**Networking**

**Front-end network gateway IP addresses**

IPv4 gateway IP address:

Primary IPv6 gateway IP address:

Primary IPv6 gateway IP address:

**Back-end network multicast IP address**

Multicast IP address: _____

**DNS**

Enable DNS: ☐ Yes ☐ No

Domain name of the HCP system:

If DNS enabled, list all IPv4 and IPv6 addresses that HCP needs to use to forward DNS requests to each corporate DNS server:

**Time**

Time source: ☐ Internal ☐ External

If external, for each time server, either the hostname or the list of IPv4 and IPv6 addresses that HCP needs to use to communicate with the server:

Time zone:

Time compliance mode: ☐ Yes ☐ No

**Internal Configuration Settings**

**Storage configuration settings**

Type of storage used: ☐ Internal ☐ External

If external, shared storage: ☐ Yes ☐ No

If external, blade servers: ☐ Yes ☐ No

If blade servers, chassis IP addresses:

If external, index volumes: ☐ Yes ☐ No

If external, spindown volumes: ☐ Yes ☐ No

If spindown volumes, array serial numbers and controller IP addresses:

| Array serial number | Controller 0 | Controller 1 |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**Serial number**

HCP system serial number: _____

**Replication**

Enable replication: ☐ Yes ☐ No

If replication is enabled, is this a reinstallation of a failed system for which seamless DNS failover is in effect: ☐ Yes ☐ No

**Customer support**

Customer support contact information:

**Security**

Enable encryption: ☐ Yes ☐ No

# Encryption Key

*Use this form to record the key displayed during installation processing for an HCP system with encryption enabled.*

HCP system serial number:

Encryption key:

**Caution: KEEP THIS KEY IN A SECURE LOCATION.** Loss of this key will most likely result in unrecoverable data in the case of catastrophic system failure.

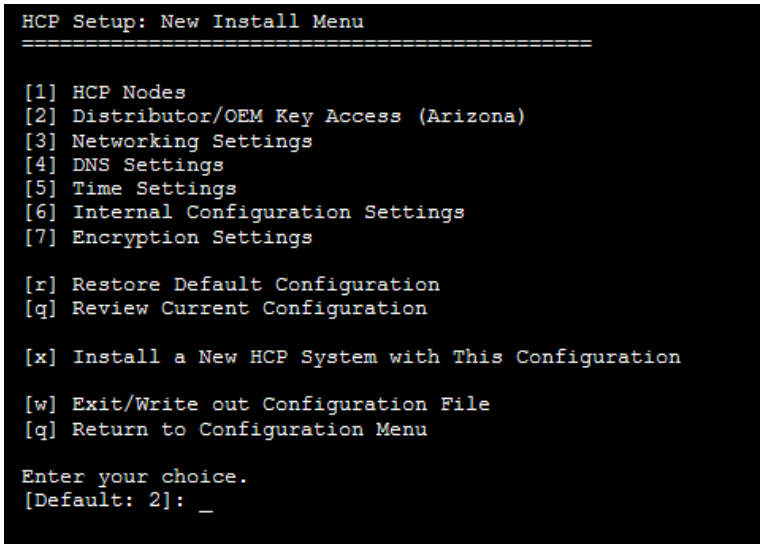
# B

# HCP Setup wizard menus

The program you use to install to an HCP system is called HCP Setup. It uses a menu-based wizard to step you through the installation procedure. This appendix shows each of the wizard menus. It presents them in the order in which they occur when you follow the default path through the wizard.

For general instructions on using the HCP Setup wizard, see "HCP Setup program" on page 41.

Option **2** on the **HCP 7.3 Configuration** menu displays the wizard New Install menu.




When you select option **1** on the **New Install** menu, the wizard presents the **HCP Nodes** menu.

```
HCP Nodes Menu
==============================================

[1] Storage Node Back-end IP Addresses

[b] Go Back to the Previous Menu
[q] Return to Configuration Menu

Enter your choice.
[Default: 1]:
```

When you select option **3** on the **New Install** menu, the wizard presents the **HCP Networking Options** menu.

```
HCP Networking Options
==============================================

[1] Gateway Router IP Address (192.168.195.1,2001:0db8::1)
[2] Multicast Network (238.177.1.1)

[b] Go Back to the Previous Menu
[q] Return to Configuration Menu

Enter your choice.
[Default: 2]:
```

When you select option **4** on the **New Install** menu, the wizard presents the **HCP DNS Options** menu.

```
HCP DNS Options
==============================================

[1] Enable DNS (Yes)
[2] Domain Name for the System (None)
[3] DNS Server(s) (172.18.4.45)

[b] Go Back to the Previous Menu
[q] Return to Configuration Menu

Enter your choice.
[Default: 1]:
```

When you select option **5** on the **New Install** menu, the wizard presents the **HCP Time Options** menu.

```
HCP Time Options
==============================================

[1] Time-Server Configuration (internal)
[2] Current Date and Time (not specified)
[3] Time Zone (America/New_York)
[4] Time Settings Compliance Mode (False)

[b] Go Back to the Previous Menu
[q] Return to Configuration Menu

Enter your choice.
[Default: 1]:
```

When you select option **6** on the **New Install** menu, the wizard presents the **Internal Configuration Settings** menu.


When you select option **7** on the **New Install** menu, the wizard presents the **HCP Security Settings** menu.

# Glossary

## A

### access protocol

See namespace access protocol

### Active Directory (AD)

A Microsoft product that, among other features, provides user authentication services.

### AD

*See* "Active Directory (AD)".

### Appliance Operating System

The operating system installed on each HCP node.

## B

### bond

A pair of ports that share an IP address.

## C

### capacity

The total amount of primary storage space in HCP, excluding the space required for system overhead for all data to be stored in primary running storage and primary spindown storage, including the fixed-content data, metadata, any redundant data required to satisfy services plans, and the metadata query engine index.

### CIFS

Common Internet File System. One of the namespace access protocols supported by HCP. CIFS lets Windows clients access files on a remote computer as if the files were part of the local file system.

### core software

See HCP core software.

## D

### data protection level (DPL)

The number of copies of the data for an object HCP must maintain in the repository. The DPL for an object is determined by the service plan that applies to the namespace containing the object.

### default namespace

A namespace that supports only anonymous access through the HTTP protocol. An HCP system can have at most one default namespace. The default namespace is used mostly with applications that existed before release 3.0 of HCP.

### distributor key

The name that determines the SSH keys required for access to the HCP nodes when they're locked down and for general troubleshooting purposes.

### DNS

*See* "domain name system".

### domain

A group of computers and devices on a network that are administered as a unit.

### domain name system

A network service that resolves domain names into IP addresses for client access.

### downstream DNS server

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

### DPL

*See* "data protection level (DPL)".

### dynamic DPL

A namespace data protection level that, at any given time, matches the system-level DPL setting.

## E

### economy storage

See HCP S Series Node.

### external storage volume

A logical volume on storage managed by a device that is outside the HCP system.

## F

### fixed-content data

A digital asset ingested into HCP and preserved in its original form as the core part of an object. Once stored, fixed-content data cannot be modified.

## H

### HCP core software

The software, other than the Appliance Operating System, that's installed on each HCP storage node to create an HCP system.

### HCP management API

A RESTful HTTP interface to a subset of the administrative functions of an HCP system. Using this API, you can manage tenants, namespaces, content classes, retention classes, and tenant-level user and group accounts.

### HCP namespace

A namespace that supports user authentication for data access through the HTTP, HS3, and CIFS protocols. HCP namespaces also support storage usage quotas, access control lists (HCP 5.0 and later), and versioning. An HCP system can have multiple HCP namespaces.

### HCP node

See node.

### HCP service

See "service" on page 82.

### HCP Setup

The program you use to install, upgrade, and add nodes to an HCP system.

### HCP software

The HCP software that runs on each storage node in the HCP system. The HCP software does not include the Appliance Operating System.

### HCP S Series Node

HCP Series Nodes serve as storage tiering platforms, known as economy storage, for HCP systems. HCP uses the S Series HS3 API, which is compatible with Amazon® S3™, to write, retrieve, and otherwise manage objects in an S Series Node. A single HCP system can seamlessly tier data across multiple S Series Nodes, thereby enabling scalability in both capacity and performance.

### HDDS

*See* "hitachi data discovery suite (HDDS)"

### HDDS search facility

One of the search facilities available for use with the HCP Search Console. This facility interacts with Hitachi Data Discovery Suite. To use this facility, HDDS needs to be installed and configured. HDDS is a separate product from HCP.

### highest-numbered node

The HCP node with the highest-numbered fourth octet in its back-end IP address.

### Hitachi Content Platform (HCP)

A distributed object-based storage system designed to support large, growing repositories of fixed-content data. HCP provides a single scalable environment that can be used for archiving, business continuity, content depots, disaster recovery, e-discovery, and other services. With its support for multitenancy, HCP securely segregates

data among various constituents in a shared infrastructure. Clients can use a variety of industry-standard protocols and HCP-specific interfaces to access and manipulate objects in an HCP repository.

### hitachi data discovery suite (HDDS)

A Hitachi product that enables federated searches across multiple HCP systems and other supported systems.

### HS3 API

One of the namespace access protocols supported by HCP. HS3 is a RESTful, HTTP-based API that is compatible with Amazon S3. Using HS3, users and applications can create and manage buckets and bucket contents.

### HSwift API

One of the namespace access protocols supported by HCP. HSwift is a RESTful, HTTP-based API that is compatible with OpenStack. Using HSwift, users and applications can create and manage containers and container contents.

### HTTP

HyperText Transfer Protocol. One of the namespace access protocols supported by HCP. In the context of namespace access, the HTTP protocol is also called the REST API.

HCP also uses HTTP for:

- Client communication with the System Management
- Client communication with the Tenant Management
- Client communication with the Search Consoles
- Client access through the HCP management API
- HCP-DM access to namespace content
- HCP Search Console communication with Console clients
- Access to namespace content through the metadata query API.

### HTTPS

HTTP with SSL security. See HTTP and SSL.

# I

### index

An index of the objects in namespaces that is used to support object-based queries and search operations.

For object-based queries, HCP builds this index from object metadata, including custom metadata and ACLs.

For search operations, each of the two search facilities, the metadata query engine and the HDDS search facility, creates and maintains its own separate index. The metadata query engine builds this index from object metadata, including custom metadata and ACLs. The HDDS search facility index is built and maintained by HDDS.

### IP mode

A front-end network property that determines whether the network can be configured to use IPv4 addresses, IPv6 addresses, or both.

# L

### link

See replication link.

### local storage volume

A logical volume on storage that's managed by HCP.

### logical volume

A logical unit of storage that maps to the physical storage managed by a node. Logical volumes can be local or external.

# M

### management API

See HCP management API.

### metadata

System-generated and user-supplied information about an object. Metadata is stored as an integral part of the object it describes, thereby making the object self-describing.

### metadata query API

A RESTful HTTP interface that lets you search HCP for objects that meet specified metadata-based or operation-based criteria. With this API, you can search not only for objects currently in the repository but also for information about objects that are no longer in the repository.

### metadata query engine

One of the search facilities available for use with HCP. The metadata query engine works internally to perform searches and return results either through the metadata query API or to the HCP Metadata Query Engine Console (also known as the HCP Search Console).

### Metadata Query Engine Console

The web application that provides interactive access to the HCP search functionality provided by the metadata query engine.

## N

### namespace

A logical partition of the objects stored in an HCP system. A namespace consists of a grouping of objects such that the objects in one namespace are not visible in any other namespace. Namespaces are configured independently of each other and, therefore, can have different properties.

HCP-DM treats HCAP 2.x archives and local file systems as namespaces.

### namespace access protocol

A protocol that can be used to transfer data to and from namespaces in an HCP system. HCP supports the HTTP, HS3, WebDAV, CIFS, NFS, and SMTP protocols for access to HCP namespaces and the default namespace. HCP also supports the NDMP protocol for access to the default namespace.

### NDMP

Network Data Management Protocol. The namespace access protocol HCP supports for backing up and restoring objects in the default namespace.

### NFS

*See* "network file system" on page 1.

### network

In an HCP system that supports virtual networking, a named network configuration that identifies a unique subnet and specifies IP addresses for none, some, or all of the nodes in the system.

### node

A server or virtual machine running HCP-VM software. Two nodes are networked together to form an HCP-VM system.

## O

### object

An exact digital representation of data as it existed before it was ingested into HCP, together with the system and custom metadata that describes that data. Objects can also include ACLs that give users and groups permission to perform certain operations on the object.

An object is handled as a single unit by all transactions, services, and internal processes, including shredding, indexing, versioning, and replication.

## P

### permission

One of these:

- In POSIX permissions, the ability granted to the owner, the members of a group, or other users to access an object, directory, or symbolic link. A POSIX permission can be read, write, or execute.
- In a data access permission mask, the condition of allowing a specific type of operation to be performed in a namespace.
- In a tenant-level user account, the granted ability to perform a specific type of operation in a given namespace.
- In an ACL associated with a bucket or an object, the granted ability to perform a specific type of operation on the bucket or object.
- The granted ability to access the HCP System Management Console, Tenant Management, or HCP Search Console and to perform a

specific activity or set of activities in that Console. Permissions of this type are granted by roles associated with the user account.

### ping

A utility that tests whether an IP address is accessible on the network by requesting a response from it. Also, to use the ping utility.

### policy

One or more settings that influence how transactions, services, and internal processes work on objects. Such a setting can be a property of an object, such as retention, or a property of a namespace, such as versioning.

### protocol

See namespace access protocol.

## R

### RAIN

*See* "redundant array of independant nodes (RAIN)" on page 1.

### replica

For an active/passive link, the HCP system to which the replication service copies objects and other information from the primary system during normal replication.

### replication

The process of keeping selected HCP tenants and namespaces and selected default-namespace directories in two HCP systems in sync with each other. This entails copying object creations, delections, and metadata chages from each system to the other or from one system to the other. HCP also replicates tenant and namespace configuration, tenant-level user and group accounts, retention classes, content classes, all compliance log messages, and all HCP tenant log messages.

### replication link

A configurable, secure trust relationship between two HCP systems that determines what is replicated between the systems and how data is transmitted between the systems.

### repository

The aggregate of the namespaces defined for an HCP system.

### retention period

The period of time during which an object cannot be deleted (except by means of a privileged delete).

### role

A named collection of permissions that can be associated with an HCP user account, where each permission allows the user to perform some specific interaction or set of interactions with the HCP System Management Console, the Tenant Management Console, the HCP management API, the metadata query API, or, for default namespaces only, the HCP Search Console. Roles generally correspond to job functions.

### running storage

Storage on continuously spinning disks.

## S

### SAIN

*See* "SAN-attached array of independent nodes (SAIN)" on page 1.

### search console

The web application that provides interactive access to HCP search functionality. When the Search console uses the hcp metadata query engine for search functionality, it is called the Metadata Query Engine Console.

### search facility

An interface between the HCP Search console and the search functionality provided by the metadata query engine or HDDS. Only one search facility can be selected for use with the Search Console at any given time.

### service

A background process that performs a specific function that contributes to the continuous tuning of the HCP system. In particular, services are responsible for optimizing the use of system resources and maintaining

the integrity and availability of the data stored in the HCP repository.

**SMTP**

Simple Mail Transfer Protocol. The namespace access protocol HCP uses to receive and store email data directly from email servers.

**SNMP**

*See* "simple network management protocol (SNMP)" on page 1.

**spindown storage**

Storage on disks that can be spun down and spun up as needed.

**SSH**

*See* "secure shell" on page 1.

**SSL**

*See* "secure sockets layer" on page 1.

**SSL server certificate**

A file containing cryptographic keys and signatures. When used with the HTTP protocol, an SSL server certificate helps verify that the web site holding the certificate is authentic. An SSL server certificate also helps protect data sent to or from that site.

**storage node**

An HCP node that manages the objects that are added to HCP and can be used for object storage. Each storage node runs the complete HCP software (except the HCP search facility software).

**subdomain**

A subset of the computers and devices in a domain.

**syslog**

A protocol used for forwarding log messages in an IP network. HCP uses syslog to facilitate system monitoring through an external interface.

**system management console**

The system-specific web application that lets you monitor and manage HCP.

# T

### tagged network

A network that has a VLAN ID.

### tenant

An administrative entity created for the purpose of owning and managing namespaces. Tenants typically correspond to customers or business units.

### tenant management console

The tenant-specific web application that lets you monitor and manage tenants and namespaces.

# U

### unix

Any UNIX-like operating system (such as UNIX itself or Linux).

### untagged network

A network with that does not have VLAN ID.

### upstream DNS server

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).

### user account

A set of credentials that gives a user access to one or more of the System Management Console, Tenant Management Console, HCP management API, HCP Search Console, or namespace content through the namespace access protocols, metadata query API, HCP Data Migrator, and a given tenant and its namespaces.

# V

### virtual networking

A technology that enables the overlay of multiple logical network configurations onto a single physical network.

### VLAN

See Virtual Local Area Network (VLAN).

### VLAN ID

An identifier that's attached to each packet routed to HCP over a particular network. This function is performed by the switches in the physical network.

### volume

See logical volume.

## W

### WebDAV

Web-based Distributed Authoring and Versioning. One of the namespace access protocols supported by HCP. WebDAV is an extension of HTTP.

### WORM

Write once, read many. A data storage property that protects the stored data from being modified or overwritten.

# Index

## O



## P



## R



## S



## T



## U



## V

## W

**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-99ARC026-15**