Hitachi Content Platform

9.1.0

Deploying an HCP VM System on ESXi

This book is the setup guide for Hitachi Content Platform Virtual Machine systems. It describes how to deploy a virtualized HCP system in your VMware vSphere® environment.

MK-94HCP010-03

Contents

Preface

This book is the setup guide for Hitachi Content Platform (HCP) Virtual Machine (VM) systems. It provides the information you need to deploy a virtualized HCP system in your VMware vSphere® environment. To complete the installation, there are instances where you may want to reference other materials.

Intended audience

This book is intended for the people responsible for deploying an HCP VM system on a VMware vSphere® environment at a customer site. It assumes that you have experience with computer networking and creating virtual machines, familiarity with VMware products and concepts, and a basic understanding of HCP systems.

Product version

This book applies to release 9.1.0 or later of HCP.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on Hitachi Vantara Support Connect:

https://knowledge.hitachivantara.com/Documents

Related documents

The following documents contain additional information about Hitachi Content Platform:

- *HCP System Management Help* — This help system is a comprehensive guide to administering and using an HCP system. The Help describes how to configure, manage, and maintain HCP system-level and tenant-level features and functionality. The help also describes the properties of objects stored in HCP namespaces and explains how to access those objects.

- *HCP Tenant Management Help* — This help system describes how to configure, manage, and maintain HCP namespaces. The help also describes the properties of objects stored in HCP namespaces and explains how to access those objects.

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

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

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

- *Deploying an HCP VM System on KVM* — This book describes how to install and configure an HCP VM system. The book also includes requirements and guidelines for configuring the KVM environment in which the system is installed.

- *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 Hitachi Remote Ops to monitor the nodes in an HCP system.

- *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 Hitachi Remote Ops to monitor the nodes in an HCP system.

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

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

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

Accessing product documentation

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

Getting help

Hitachi Vantara Support Portal is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

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

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

Comments

Please send us your comments on this document:

HCPDocumentationFeedback@HitachiVantara.com

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

Thank you!

1

HCP system overview

This chapter introduces Hitachi Content Platform. It describes the architecture of an HCP VM system installed in a VMware vSphere environment.

Introduction to Hitachi Content Platform

Hitachi Content Platform (HCP) is a distributed storage system designed to support large, growing repositories of fixed-content data. An HCP system consists of both hardware (physical or virtual) and software.

HCP stores objects that include data and the metadata that describes the data. HCP distributes these objects across the storage space. HCP represents objects either as URLs or as files in a standard file system.

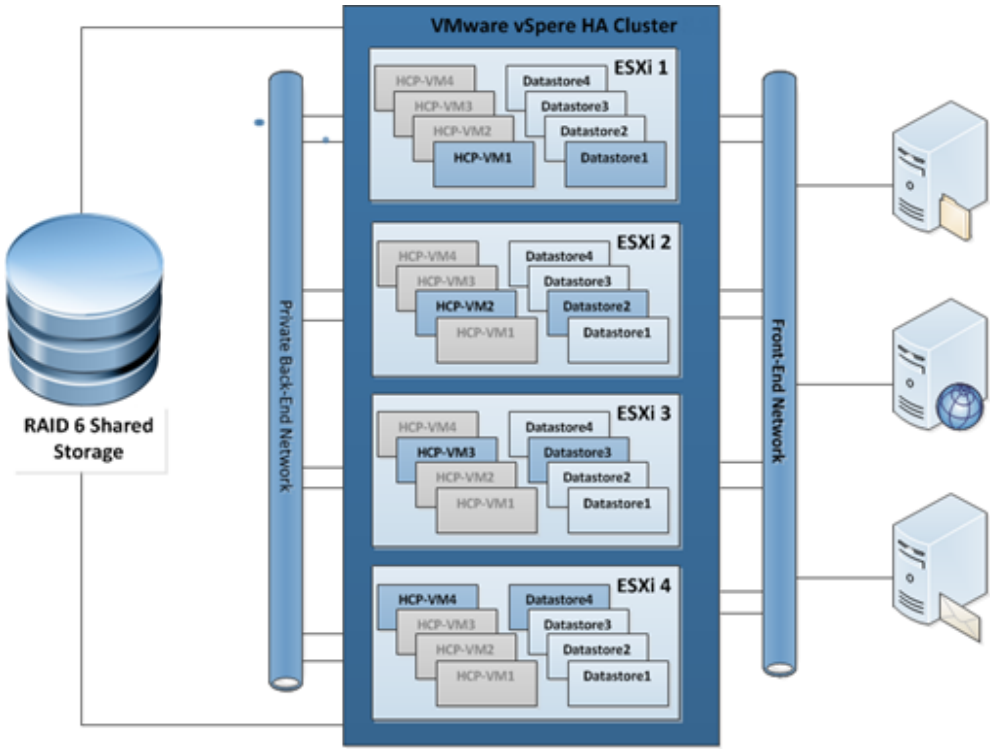
An HCP **repository** is partitioned into namespaces. Each **namespace** consists of a distinct logical grouping of objects with its own directory structure. Namespaces are owned and managed by tenants.

HCP provides access to objects through a variety of industry-standard protocols as well as through various HCP interfaces.

HCP VM system components and architecture

This section describes the components and architecture of an HCP VM system.

The next figure describes the architecture of an HCP VM system running on VMware infrastructure.



Host platform

In an HCP VM system, each HCP VM node runs in a virtual machine on an VMware ESXi host.

Compute

An HCP VM node must have at least eight virtual CPUs and 32 GB of allocated RAM.

The minimum processing requirements ensure that HCP VM system performance is not slowed by multiple client logins, and that activities like encryption, scheduled services, and routine database maintenance continue running.

If you are deploying an HCP VM small-instance configuration, each HCP VM node must have at least four virtual CPUs and 16 GB of allocated RAM.

Storage

HCP VM storage infrastructure is highly available and fault tolerant. It is recommended for the physical servers that the ESXi hosts run on to be connected to shared SAN storage with RAID 6 protection or Hitachi NAS (**HNAS**).

The HCP SAN storage needs to have at least two paths to each logical unit number (**LUN**) and each LUN needs to have the same LUN number (**HLUN**) on each ESXi host.

A datastore will be created from each LUN or export, creating one Virtual Machine File System (**VMFS**) volume per LUN or export. A single datastore is not shared by HCP VM nodes. However, HCP VM nodes can have multiple datastores. Each datastore is carved into one or multiple Virtual Machine Disks (**VMDK**) which are presented to the HCP OS as local disks. The HCP OS recognizes its storage as internal drives similar to an HCP appliance with a local storage configuration. The disks are controlled by the VMware Paravirtual SCSI controller (**PVSCSI**). VMware recommends PVSCSI for better overall performance.

Tip: The PVSCSI adapter reduces CPU utilization and potentially increases throughput compared to default virtual storage adapters

Each VMDK can be a maximum size of 15.90TB.

In addition to the recommended RAID 6, shared SAN storage configuration, and HNAS datastores, HCP VM also supports the following for storage configurations:

- Shared SAN arrays with virtual volumes created from Hitachi Dynamic Provisioning (DP) pools. This configuration does not support thin provisioning. It is recommended to spread datastores across multiple DP Pools to avoid resource contention and single points of failure.
- Shared SAN arrays with LUNs configured using Raw Device Mapping (**RDM**) in vSphere® Client or vCenter™. The RDM is to be configured in Physical Mode.
- VMware vSAN datastores.

    - VMware vSAN aggregates direct attached storage (DAS) devices to create a single storage pool that is shared across all VMware vSphere ESXi hosts in the vSAN cluster.
    - Choose vSAN datastore for storing VMDK files for HCP node VMs.
    - Use thick eager-zeroed VMDK to avoid over provisioning storage that is used by HCP VMs.
    - Follow VMware best practices to configure vSAN storage-backed ESXi environments.
    - For optimal performance, use VM storage policy to ensure that all VM files for an HCP VM node reside on storage of the same ESXi server that is running the HCP VM node.
- Other devices like HNAS that export NFS v3 shares, which are mounted and used as NFS datastore.
    - It is required to use thick, eager zero when formatting NFS datastores, so additional ESXi plug-ins may be required from your vendor. Hitachi provides a VAAI plug-in that enables this functionality on the HNAS platform.
    - It is recommended to not have multiple datastores on the same file system or the same underlying disk due to performance and availability considerations.
    - Follow the vendors best practice for configuring NFS datastores.
- RAID-protected storage that's internal to the ESXi hosts. Each LUN created from this storage corresponds to a Virtual Machine File System datastore. This configuration does not support vSphere High Availability (HA). The underlying storage in this configuration must be RAID protected.

If you deviate from the recommended configuration, you need to consider the possible ramifications to performance, availability, backup, security, ease of management, and data integrity. Ensure that you completely understand failure scenarios, HDD failure rates, RAID protection levels, RAID rebuild times, and support windows before changing configurations. System health must be closely monitored to prevent service failures and ensure that the underlying storage does not fail.

For information about supported storage vendors and devices, see the applicable VMware documentation.

HCP network connectivity

HCP VM network connectivity is provided to the HCP guest operating system by VMware VMXNET3 vNICs, vSwitches, and distributed switches.

For the VMXNET3 vNIC, the back-end vSwitch must be configured to provide access to one vmNIC, and the front-end vSwitch must be configured to provide access to a different vmNIC.

Front-end network

The HCP front-end network is used for client and management access. For HCP front-end networks, it is recommended that the ESXi host create one vNIC mapping to two physical NICs (pNICs) on the ESXi host. Having two pNICs dedicated to HCP ensures redundancy and consistent performance.

Back-end network

The HCP private back-end network is used for internode communication and data transfer. The ESXi host has one vmNIC that maps to two physical NICs on the ESXi host server.

The physical NICs dedicated to the back-end network must be connected to two physical switches on an isolated network. pNIC-1 on all ESXi hosts must connect to the same physical switch (switch1), and pNIC-2 on all ESXi hosts must connect to the same second physical switch (switch2). The physical switches must be cabled for an inter-switch connection. To guarantee data security and HCP reliability, back-end switches must be configured with spanning tree disabled and multicast traffic enabled. The back-end switches must be at least 1 GbE and must be dedicated to HCP.

To support HCP VM inter-node communication, the back-end network must have multicast enabled. In most cases, enabling multicast on the switch is not sufficient to allow for multicast traffic. Most switches require additional configuration parameters. To allow multicast traffic between the HCP VM nodes, follow the switch-vendor documentation to configure the network.

Note: The HCP VM system can be deployed without multicast enabled on the switches. However, if the switches are not configured for multicast, the HCP VM nodes cannot communicate.

If the HCP VM back-end network is on a public network, the HCP VM system should reside on its own VLAN.

Management port network

The HCP management port is a separate network that can be used to isolate management access from client access. For the management port network, a single virtual Network Interface Card (**NIC**) needs to be created on the ESXi host on a single physical NIC.

Storage network

Hitachi Vantara recommends that the VMkernel network be set up in a private network or with a unique VLAN ID that provides network isolation.

Dedicated database volume

A separate volume can be created on each HCP virtual machine to separate the storage of user data and metadata from the HCP database. During the installation, you are asked if you want a dedicated database volume if each virtual machine is configured with three or more data disks, at least one of which is greater than 50 GB.

Hardware monitoring and alerting

HCP hardware has built-in redundancy, monitoring, alerting, and failover behavior that cannot be used in a virtualized environment.

To maintain performance and data integrity on an HCP VM system, the system must be connected to Hitachi Remote Ops. For more information, see Chapter 6: "Configuring HCP monitoring with Hitachi Remote Ops" on page 77.

Hitachi Remote Ops supports Hitachi hardware only. To monitor hardware supplied by other vendors, you must use third-party monitoring tools.

HCP software

An HCP VM system uses the same HCP operating system and software as HCP RAIN and SAIN systems. Data is RAID protected, and HCP policies and services ensure data integrity, data security, and storage optimization. HCP VM management and data access interfaces are the same as that of HCP RAIN and SAIN systems.

Because HCP VM software is not bound to hardware, the software does not support zero-copy failover, and hardware cannot be monitored in the system management console.

HCP upgrades

HCP v5.0 introduced HCP Evaluation Edition for proof of concept (POC) and test activities at Hitachi Vantara partner and customer sites. Upgrades from the Evaluation Edition single node and Evaluation Edition multi-node to HCP VM are not supported. HCP VM supports upgrades from the initial 6.0 release to future releases of HCP VM.

HCP search nodes

HCP search has reached end of service life. As such, HCP search nodes are not available for HCP VM systems. As with physical HCP systems, this functionality is provided by Hitachi HDDS Enterprise search products.

HCP VM node failover (vCenter and vSphere HA)

To configure automatic failover in the event of an ESXi host failure, an instance of the VMware vCenter Server must be available. Failover functionality is provided by a vSphere High Availability (HA) cluster.

A vSphere HA cluster allows a collection of ESXi hosts to work together to optimize their levels of availability. The system administrator is responsible for configuring the cluster to respond to host and virtual machine failures.

The system administrator will configure each ESXi host participating in an HCP VM system to be part of a single vSphere HA cluster in vCenter. This enables high availability in cases where one or more servers or ESXi hosts fail. When the master host detects a server or ESXi host failure, it can restart the HCP VM node that was running on the failed server or ESXi host to other healthy ESXi hosts in the cluster.

The master host monitors the status of slave hosts in the cluster through network heartbeat exchanges every second. If the master host stops receiving heartbeats from a slave, it checks for liveness before declaring a failure. The liveness check determines if the slave is exchanging heartbeats with a datastore.

The HCP VM system administrator will not configure the HCP VM vSphere HA cluster to automatically move the failed-over HCP VM node back to its original ESXi host once the host is available. The system administrator will manually shut down the HCP VM node, and the vCenter administrator will manually move the HCP VM node onto the preferred ESXi host and power on the HCP VM node. Once the node boots, it will re-join the HCP VM system.

In the case of network isolation, the HCP VM vSphere HA cluster will be configured to leave the HCP VM node powered on. This means that the HCP VM node will still be able to communicate over its private back-end network with the other HCP VM nodes in the system. As in the case of a physical HCP node, the HCP VM node and the data it is managing will remain available to the system through the front-end of the other nodes in the HCP VM system.

The vCenter Server used to configure the vSphere HA cluster of ESXi hosts for the HCP VM system either can be a pre-existing server in the customer environment, or can be allocated as part of the HCP VM HA cluster of ESXi hosts. It is a best practice to have the vCenter Server separate from the HCP VM HA cluster. The vCenter Server can consume a fair amount of resources on the ESXi host that could be used by the HCP VM nodes.

The rules for creating a vSphere HA cluster for use with HCP VM are very specific. If the HCP VM system will be added to an existing HA cluster, ensure that the cluster is configured exactly to the specifications in this guide.

Storage licensing

HCP VM systems come with a basic storage license that provides two terabytes of active and HCP S Series storage. The basic storage license also provides two terabytes of extended storage. If you need additional storage, contact your Hitachi Vantara sales representative.

For more information about storage licensing, see HCP System Management Help.

2

Configuration guidelines for the HCP VM environment

This chapter describes the requirements and guidelines for installing and using an HCP VM system.

Supported VMware versions

HCP VM supports multiple versions of VMware.

For a list of supported VMware versions, see the release notes on Hitachi Vantara Support Connect:.

https://knowledge.hitachivantara.com/Documents

Supported VMware functionality

HCP VM supports the following VMware functionality:

- vSphere HA cluster
- HCP VM node shutdown from the vCenter management console. This functionality is provided by the VMware tools package, which is included in the HCP OS with HCP VM.

Note: Pausing live migration and other functionality enabled by the VMware tools package are not currently supported.

- DRS when used in a manual capacity to assist with virtual machine-to-host affinity. See Appendix B: "Modifying the DRS settings" on page 89 for details.

The current version of HCP VM does not support the following VMware functionality:

- Other failover capabilities provided by VMware, such as vMotion, storage vMotion, and DRS with FT
- Software used for VM replication

The following HCP features are specific to the physical HCP appliances (HCP RAIN system, HCP SAIN system) and are not applicable to HCP VM:

- **Autonomic tech refresh**: Provides the capability of migrating a VM to a different host, allowing for server refresh. The raw storage layer is obscured from HCP in the VMware environment; any storage refresh must be handled at the VMware layer.
- **Zero-copy failover**: VMware HA replaces this capability by restarting an HCP VM on an ESXi host after it is lost due to a host failure. This storage availability is provided by shared SAN storage.
- **Spindown**, **Indexing-only LUNs)**: Spindown is not compatible with the VMware environment. Indexing-only LUNs are not available in HCP VM with this release. Shared-index LUNs are standard as with all other HCP systems.
- **HCP integrated HDvM monitoring**: The raw storage layer is obscured from HCP in the VMware environment. Storage connected to HCP VM needs to be monitored at the customer site using their preferred mechanism.
- **VLAN tagging**: Active-active NIC Teaming in VMware is designed for load balancing and redundancy. Both physical NICs must be configured with the same VLAN tagging. Also, VMware vSwitch is a layer 3 switch and will not route traffic out physical NICs per VLAN tagging. You cannot configure physical vmNIC2 to be tagged on VLAN 20 and physical vmNIC3 to be tagged on VLAN 30 so that VMware will route HCP traffic out the appropriate physical NIC.

HCP VM hardware requirements

HCP VM systems can be configured in two ways: standard and small instance.

Standard HCP VM system
To deploy a standard HCP VM system, you need:

- A shared SAN storage. RAID 6 system is recommended.
- A minimum of four 1.2 TB LUNs for the default VMDK size deployment.

Note: Due to the overhead associated with disk formatting and database storage, the estimated usable storage available with this minimum is approximately 3.66 TB.

- A minimum of four HCP VM nodes
- A minimum of two 500 GB VMDKs on each HCP VM node
- A minimum of eight virtual CPUs on each HCP VM node
- A minimum of 32 GB of RAM on each HCP VM node

Note: To avoid the possibility of slowing system performance, do not commit more than 256 GB of RAM for an HCP VM node.

- Recommended volume size for NFS datastores: Contact your storage array vendor or NFS server vendor for information about the maximum NFS volume size.
- Two physical NICs on each ESXi host in the vSphere HA cluster dedicated to the HCP VM back-end network
- Two physical NICs for the VMware management network for vSphere HA and HCP VM front-end network
- Two port fibre channel HBA cards (or VMware compatible IO device) for shared SAN storage connectivity (when applicable)
- ESXi requires a minimum of 2 GB of physical RAM. VMware recommends providing at least 8 GB of RAM to take full advantage of

ESXi features and run virtual machines in typical production environments.

- To ensure continuous availability and fault tolerance for your HCP cluster, an ESXi server can host one HCP VM. In addition, the same ESXi server can host one or more workloads unrelated to HCP. However, you must ensure that the HCP VM has access to the necessary CPU, memory, network, and disk resources to operate. For more information, see "HCP VM availability considerations" on the facing page.

Small-instance HCP VM system
A small-instance HCP VM system has the same requirements as a standard configuration with the following exceptions:

- A minimum of 4 virtual CPUs on each HCP VM node
- A minimum of 16 GB of RAM on each HCP VM node

A small-instance deployment can support:

- Five tenants
- 25 namespaces
- A single active/passive replication link
- An ingest duty cycle of 12 hours per day, 5 days per week

Other factors can affect whether the small-instance deployment meets your performance requirements, such as heavy metadata query engine (MQE) querying or object and directory counts above published maximums.

HCP VM system limits

There are system limits for an HCP VM system.

For a standard HCP VM system configuration, the following limits are supported:

- 40 HCP VM nodes
- 59 data LUNs on each HCP VM node (ESXi guest OS limitation)

- Maximum open VMDK storage per host (ESXi limitation). See the VMware documentation for the ESXi limitations associated with the version that you are running.

For an HCP VM system small-instance configuration, the following limits are supported:

- 16 HCP VM nodes
- 59 data LUNs on each HCP VM node

HCP VM availability considerations

An HCP cluster is considered in a state of continuous availability if there is one HCP VM node per ESXi host, and if over half of the HCP VM nodes are healthy and running. When the HCP cluster is in this state, the system can survive a single ESXi host failure without affecting HCP functionality.

If your HCP cluster is not in a state of continuous availability because you have multiple HCP VM nodes per ESXi host and one of your ESXi hosts fails, the HCP VM system enters a state of metadata unavailability. Metadata unavailability prohibits HCP namespaces from accepting write requests. The data stored in the affected nodes becomes inaccessible until the HCP system repairs itself. The repair process can take between one and five minutes.

HCP VM systems do not support zero-copy failover. If a namespace has a data protection level of one, the loss of a single HCP VM node causes the node to enter a state of data unavailability until the node is restored.

Oversubscribing the CPU, RAM, or disk of ESXi hosts can cause HCP system instability.

A vSphere HA cluster is recommended, but not required.

3

Configuring the HCP VM environment

This section provides the information and steps required to provision the VMware environment for an HCP VM deployment.

ESXi considerations

You might want to deploy the HCP VM system on existing VMware ESXi hosts in your environment. Before doing this, make sure that the hosts meet the minimum requirements for compute and memory cataloged in "HCP VM hardware requirements" on page 11.

Depending on the versions of VMware ESXi, VMware vCenter Server, and VMware vSphere that you are running, steps and terminology might be different in the GUI. This document is applicable to VMware vSphere versions 6.5 and later; however, you can also use it as a reference for earlier versions. For information about ESXi versions 6.0 and earlier, see the revision of this document available with HCP version 8.0.

For a list of supported VMware versions for a specific HCP version, see the HCP Release Notes associated with that version.

For information about VMware functionality that HCP VM supports, see "Supported VMware functionality" on page 9.

When provisioning storage to use with HCP VM, be sure to review and follow the VMware ESXi storage guides and the relevant storage vendor's VMware best practices guide. For more information about provisioning storage to use with HCP VM, see "Provisioning HCP VM storage" on page 18.

Important: All ESXi hosts that will contain an HCP VM node must have Network Time Protocol (NTP) enabled. To enable NTP, you use the time configuration option in the vSphere client on each ESXi host.

Enabling NTP for the ESXi hosts

Procedure

1. Access your vSphere client.
2. Select the ESXi host for which you want to enable NTP.
3. Click **Configure**.
4. Under **System**, click **Time Configuration**.
5. Click **Edit**.
6. Specify whether you want to manually configure the date and time for the host, or if you want to enable the NTP client. Enabling the NTP client enables date and time synchronization with an NTP server.
7. For the NTP service startup policy, select **Start and stop with host**.
8. In the **NTP Servers** section, enter the time server or servers that you want to use.
9. Click **OK** and then start or restart the NTP service.
10. Repeat the procedure with the same time server for all ESXi hosts that will reside on an HCP VM node.

Tip: Write down the NTP server used in your ESXi hosts. You will use this information during the HCP VM installation.

Configuring a vSphere HA cluster for HCP VM

A VMware vSphere HA cluster lets a collection of ESXi hosts work together to optimize their levels of availability. You are responsible for configuring the cluster to respond to host and virtual machine failures.

Step 1: Create a datacenter

Procedure

1. Access the vSphere client.
2. In the left navigation pane, right-click your server and select **New Datacenter**.

3. Enter a name for your HCP VM datacenter. For example, `hcp-vm-center-1`.

4. Click **OK**.

Step 2: Add a cluster

Procedure

1. In the left navigation pane, right-click the datacenter you just created and select **New Cluster**.

2. Enter a name for the cluster. For example, `hcp-vm-cluster-1`.

3. Select the checkbox to turn on vSphere HA.

Important: Do not select the option to turn on DRS.
You can enable DRS later to define VM affinity to a particular host or group of hosts. This function does not provide further failover automation. The setting assists with keeping virtual machines on a given host, and alert you if the rule cannot be followed. For information about the required DRS settings, see "Appendix B: Modifying the DRS settings" on page 89.

4. Click **OK**.

Step 3: Add ESXi hosts

Before you begin

For information about the maximum number of ESXi hosts allowed in a vSphere HA cluster, see the VMware documentation.

Procedure

1. In the left navigation pane, right-click the cluster you created and select **Add Host**.

2. In the **Add Host** wizard, enter the ESXi host connection information.

3. Enter the username and password for the ESXi host.

4. Review the host summary.

5. Enter the license information for the ESXi host if it is not already assigned.

6. Optional: To increase security on your ESXi host and prevent remote users from logging in directly, select **Lockdown mode**.

Note: The customer should make the decision whether to implement lockdown mode.

7. Review your choices and click **Finish**.

   The ESXi host is added to the vSphere HA cluster.

8. Repeat this procedure for each ESXi host in the system.

Provisioning HCP VM storage

When provisioning storage to use with HCP VM, be sure to review and follow the VMware ESXi storage guides and the relevant VMware best practices guide from the storage vendor.

You can provision HCP VMs in a local storage configuration or shared SAN storage configuration. Local storage is not recommended due to its increased data availability risk. For this reason, if you provision HCP VM in a local storage configuration, it is a best practice to set your data protection level (DPL) to two. For more information about data protection levels, see the HCP System Management Help.

The following guidelines are for provisioning shared SAN storage for use with HCP VM with the recommended configuration:

- Datastores used for HCP VM nodes must be backed by shared RAID 6 storage.
- Each datastore should only consist of one LUN.
- HCP VM nodes cannot share datastores.
- All LUNs will be mapped to ESXi hosts in the vSphere HA cluster.
- All LUN IDs must be consistent across hosts. For example, LUN 1 should be mapped to host 1, host 2, host 3 and host 4 as LUN 1.
  - This is also true for VMDK and RDM.

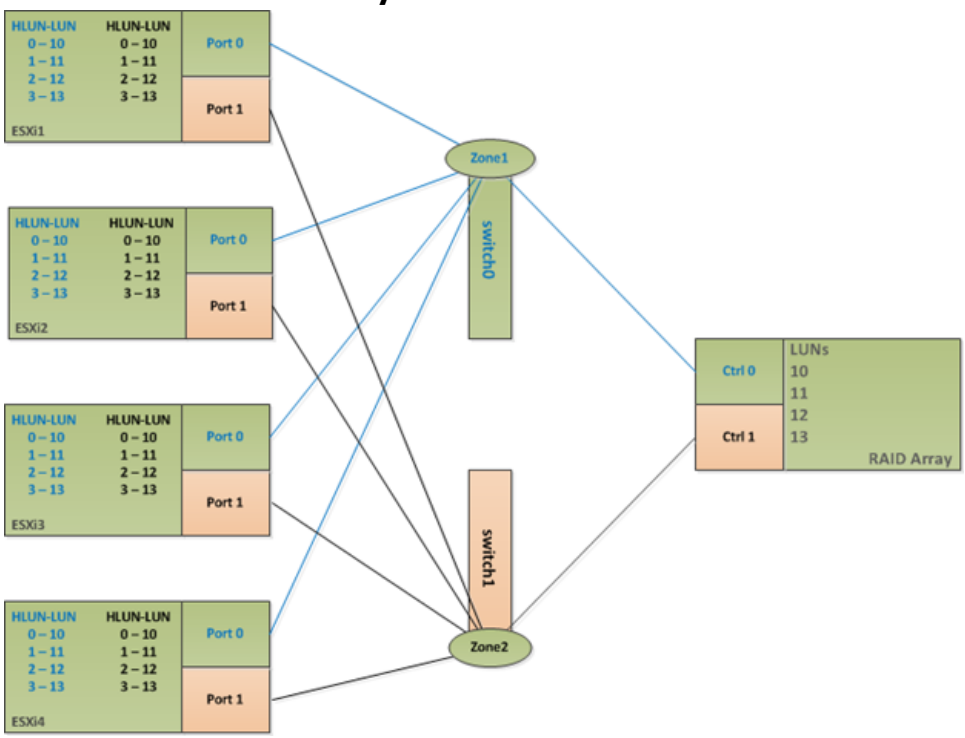
  - For Network File System (NFS), all ESXi hosts must mount the export with the same datastore name.

- All SAN LUNs will have at least two paths (multipathing) presented to the ESXi host.
- If fabric is connected, redundant FC switches will be deployed as part of the HCP VM storage environment to ensure maximum availability.
  - To ensure maximum data security, it is recommended to use WWN zoning (not port) for HCP VM Zones.
- If loop is connected, redundant controllers must be provisioned for the HCP VM storage environment to ensure maximum availability. Do not use different ports on the same array controller.

The next figure illustrates a sample SAN layout for VMDK and RDM. The number of storage controller ports dedicated to an HCP VM system is dependent on the capabilities of the storage array. For Hitachi Vantara mid-range storage, the best practice is to spread host access across all cores.

Consult the storage vendor documentation for sizing and configuration options.

Fibre Channel Connectivity



FC Switch 1, HCP VM path 1

Zone name	Zone member wwpn	Zone member wwpn
HCP_VM_cluster_1_path_1	Storage controller 0	ESXi_host1_port0
	Storage controller 0	ESXi_host2_port0
	Storage controller 0	ESXi_host3_port0
	Storage controller 0	ESXi_host4_port0

FC Switch 2, HCP VM path 2

Zone name	Zone member wwpn	Zone member wwpn
HCP_VM_cluster_1_path_2	Storage controller 1	ESXi_host1_port1
	Storage controller 1	ESXi_host2_port1
	Storage controller 1	ESXi_host3_port1
	Storage controller 1	ESXi_host4_port1

The following tables are sample Host Group / LUN layouts that display the same LUNs mapped with the same HLUN to each ESXi host.

These examples assume that the ESXi OS LUN has already been provisioned, but it can be provisioned from the SAN as well. In the case of the OS LUN being provisioned on the SAN, only the ESXi host that is booting from the LUN should be granted access.

Array path 1

Host Group Name	Hosts	HLUN	ArrayLUN	VMware datastore
HCP_VM_cluster_1_path_1	ESXi-1 ESXi-2 ESXi-3 ESXi-4	1	10	hcp-vm_cluster-1_node_1_datastore_1
		2	11	hcp-vm_cluster-1_node_2_datastore_1
		4	12	hcp-vm_cluster-1_node_3_datastore_1
		5	13	hcp-vm_cluster-1_node_4_datastore_1

Array path 2

Host Group Name	Hosts	HLUN	ArrayLUN	VMware datastore
HCP_VM_ cluster_1_path_ 2	ESXi-1 ESXi-2 ESXi-3 ESXi-4	1	10	hcp-vm_cluster-1_node_1_ datastore_1
		2	11	hcp-vm_cluster-1_node_2_ datastore_1
		4	12	hcp-vm_cluster-1_node_3_ datastore_1
		5	13	hcp-vm_cluster-1_node_4_ datastore_1

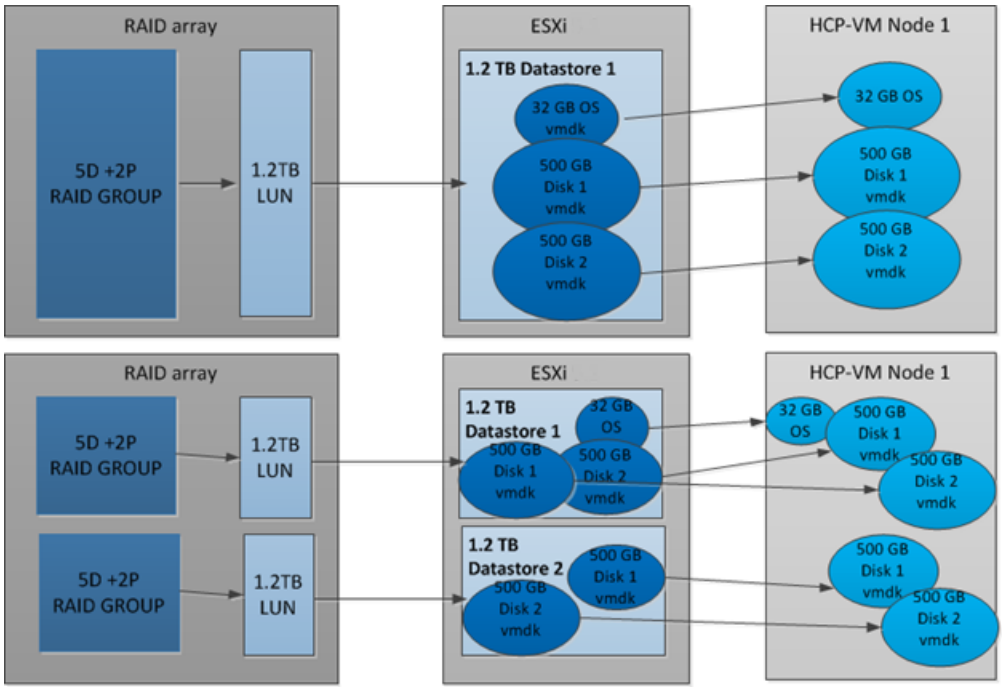
Adding VMFS datastores to a vSphere HA cluster

It is recommended to have only one LUN from a RAID Group in the HCP VM system. Adding multiple LUNs from the same RAID Group increases the risk of data loss in the event of a failure.

A datastore can only be set for one HCP VM node, but each HCP VM node can have multiple datastores.

In an HCP VM system using VMware version 5.5 or later, the largest a disk can be is 16 TB.

Here is a visual depiction of the cluster layout.



Procedure

1. Access your vSphere Client.
2. In the **Datastores** section, click the option to create a new datastore.
3. To specify the datastore type, select **VMFS**.
4. Enter a meaningful name for the datastore. For example, `hcp-vm_cluster_1_node_1_datastore_1`.
5. Select the VMFS version for the datastore (VMFS 6 is recommended).
6. Specify partition configuration details for the datastore.
7. Review your choices. Then click **Finish** to create the VMFS datastore.

   The datastore should now be initialized and mounted. If it is, then in the **Recent Tasks** section of the vSphere Client, a **Rescan VMFS** alarm should be issued for all other ESXi hosts in the cluster.

   The new datastore should be automatically added to the inventory of all the other ESXi hosts.
8. Repeat this procedure for any other datastore LUNs with all the same values and verification except for the datastore name.

Here are examples of other identifiable datastore names you can use:

- LUN2 = `hcp-vm_cluster_1_node_2_datastore_1`
- LUN3 = `hcp-vm-cluster_1_node_3_datastore_1`
- LUN4 = `hcp-vm-cluster_1_node_4_datastore_1`

About NFS datastores

You can configure HNAS file systems and their underlying storage in a variety of different ways. To achieve the best performance, follow these recommendations for configuring HNAS in a VMware vSphere environment:

- In general, a 4 KB file system block size is recommended. 32 KB can be used in instances where all VMs on a specific HNAS file system perform large block requests.
- Set cache-bias to large (cache-bias --large-files).
- Disable shortname generation and access time maintenance (shortname –g off, fs-accessed-time --file-system <file_system> off).
- Disable the quick start option for HNAS read ahead when VM IO profiles are primarily random. (read-ahead --quick-start disable).
- NFS exports: Do not export the root of the file system.
- File system utilization: Maintain at least 10% free space in each file system utilized by ESXi hosts.
- Storage pools: Do not mix disk types in the same storage pool.
- Limit ownership of all file systems that are created on a storage pool to one EVS.
- Configure a minimum of four (4) System Drives (SD) in a storage pool.
- Configure one (1) LU\LDEV per RAID group consuming all space (if possible).

Creating an NFS datastore

Procedure

1. Access your vSphere Client.
2. In the **Datastores** section, click the option to create a new datastore.
3. To specify the datastore type, select **NFS**.
4. Enter a meaningful name for the datastore. For example, `hcp-vm_cluster_1_node_1_datastore_1`.
5. Select the NFS version for the datastore.
6. Enter the server name and the mount point folder name.

   If you are using NFS version 4.1, you can optionally enable and configure Kerberos authentication to secure NFS messaging.
7. Select the hosts that require access to the datastore.
8. Review your choices. Then click **Finish** to create the NFS datastore.

Important: Ensure that you mount datastores with the same volume label on all vSphere ESXi hosts within VMware HA environments.

Configuring networking

Networks should be configured for specific switches in the system before the ISO file is deployed. HCP supports both VMware vSphere standard virtual switches (VSS) and vSphere distributed virtual switches (VDS).

Be sure to review HCP System Management Help for the latest information about HCP network administration.

To configure standard VMware vSwitch networking for front-end switching, back-end switching, and management port switching, complete the following applicable procedures.

To configure distributed vSwitch networking for VMware vCenter Server in your HCP environment, follow VMware best practices. Dedicated distributed vSwitches are required for each front-end switching, back-end switching, and management switching HCP network.

Configuring networking for front-end switching

Procedure

1. From the vSphere Client, select an ESXi host.
2. Click **Configure**.
3. In the **Networking** section, click **Virtual Switches**.
4. Click **Add Host Networking**.
5. Select **Virtual Machine Port Group for a Standard Switch** and click **Next**.
6. Click **Select an existing standard switch**. Then click **Browse**.
7. Select the default **vSwitch0**, click **OK**, and then click **Next**.
8. For the **Network label**, enter **Front-end Network** and click **Next**.
9. Review your settings. Then click **Finish**.

Configuring networking for back-end switching

Procedure

1. Click **Add Host Networking**.
2. Select **Virtual Machine Port Group for a Standard Switch** and click **Next**.
3. Click **New standard switch**. Then click **Next**.
4. Click the **Add adapters** icon.
5. Select your configured back-end network adapter, click **OK**, and then click **Next**.
6. For the **Network label**, enter **Back-end Network** and click **Next**.
7. Review your settings. Then click **Finish**.

(Optional) Configuring networking for management port switching

Procedure

1. Click **Add Host Networking**.
2. Select **Virtual Machine Port Group for a Standard Switch** and click **Next**.

3. Click **New standard switch** and click **Next**.

4. Click the **Add adapters** icon.

5. Select your configured management port network adapter, click **OK**, and then click **Next**.

6. For the **Network label**, enter **Management Port Network** and click **Next**.

7. Review your settings. Then click **Finish**.

4

Creating the HCP VM system

For general installation recommendations prior to performing the HCP software installation on an HCP VM system, review the documentation for *Installing an HCP System*.

Unpacking and uploading the ISO zip file

Before you can create a new virtual machine, you need to unpack the ISO.zip archive and upload the ISO file to a datastore.

Procedure

1. Download the `HS222_x.x.x.x.iso.zip` archive onto your computer.
2. Unpack the ISO.zip archive to extract the ISO file.
3. Start your VMware vSphere client.
4. Click **Datastores**. Then select the datastore to which you want to upload the ISO file.
5. Navigate to the datastore.
6. Click the **Upload a file to the Datastore** icon.
7. Locate the ISO file that you unpacked, and upload the file to the datastore.

Creating and configuring the new virtual machine

To create and configure the new virtual machine, you must complete the next procedures for each node in your HCP system. The procedures use the New virtual machine wizard in your VMware vSphere client.

Before you begin

Ensure that you have reviewed the configuration guidelines in Chapter 2: "Configuration guidelines for the HCP VM environment" on page 9.

Step 1: Create the virtual machine

Procedure

1. Log in to your vSphere client.

   You should see the datacenters, clusters, and VMware ESXi hosts that were previously added to VMware vCenter.

2. Connect to the vCenter server where you configured the vSphere HA cluster for HCP VM.

3. In the navigation bar, right-click the ESXi host that you plan to use for the deployment and select the option to create a new virtual machine.

   The New virtual machine wizard is displayed.

4. Select **Create a new virtual machine** and click **Next**.

5. Enter a name for the new virtual machine, select a datacenter, and click **Next**.

6. Select a host and click **Next**.

7. Select the datastore and click **Next**.

8. Select the compatibility for the virtual machine.

Note: Ensure that you select the version that corresponds to the ESXi host software version that you are using.

   Then click **Next**.

9. For **Guest OS family**, select **Linux**.

10. For **Guest OS version**, select **Red Hat Enterprise Linux 6 (64-bit)**, and click **Next**.

11. Specify the following information:

    - For **CPU**, select **8**.

- For **Cores per socket**, select **4**.
- For **Memory**, specify at least **32 GB**.
- For **Hard disk 1** (the OS disk), specify at least **32 GB**.
- For **Disk provisioning**, select **Thick provisioned, eager zeroed**.
- Select **SCSI controller 0** and **SCSI (0:0)**.

12. Create additional VMDK or RDM data disks, as needed.

Note: You need to create a minimum of two additional hard disks, or three if you need a dedicated database volume.

- To create additional VMware VMDK hard disks:
  - **a.** From the **New device** menu, select **New Hard Disk** and click **Add**.
  - **b.** For the first additional hard disk, select **SCSI (0:1)**.For the second additional hard disk, select **SCSI (0:2)**, and so on.
  - **c.** Specify a size of at least **500 GB** for a user database volume, or at least **50 GB** for a dedicated database volume.
  - **d.** For **Disk provisioning**, select **Thick provisioned, eager zeroed**.
- To create additional RDM hard disks:
  - **a.** From the **New device** list, select **SCSI Controller** and click **Next**.

    For better performance, it is a best practice to use a separate SCSI controller for the RDM hard disk.
  - **b.** From the **New device** list, select **RDM Disk** and click **Add**.
  - **c.** For the first additional hard disk, select **SCSI (1:0)**. For the second additional hard disk, select **SCSI (1:1)**, and so on.
  - **d.** Specify a size of at least **500 GB**.
  - **e.** For **Disk provisioning**, select **Thick provisioned, eager zeroed**

Step 2: Configure the network adapters

You must configure at least two network adapters. The first adapter is for the front-end network, and the second adapter is for the back-end network.

Procedure

1. Create the network adapter for the front-end network.
   a. In the **New virtual machine** wizard, from the **New Network** list, select the front-end network that you defined in "Configuring networking" on page 24
   b. Specify the following information:
      - Set the first network adapter to the **Front-end Network**.
      - Select **Connect At Power On**.
      - Set **Adapter Type** to **VMXNET 3**.
      - Set **MAC Address** to **Automatic**.
2. Create a network adapter for the back-end network.
   a. From the **New device** list, select **Network** and click **Add**.
   b. Specify the following information:
      - Set the second network adapter to the **Back-end Network**.
      - Select the **Connect At Power On** option.
      - Set the **Adapter Type** to **VMXNET 3**.
      - Set the **MAC Address** to **Automatic**.
3. Optional: Create a network adapter for the HCP management port network.
   a. From the **New device** list, select **Network** and click **Add**.
   b. Specify the following information:
      - Set the third network adapter to the **Management Port Network**.
      - Select **Connect At Power On**.

- Set **Adapter Type** to **VMXNET 3**.
- Set **MAC Address** to **Automatic**.

4. From the **New CD/DVD Drive** list, select **Datastore ISO file**.
5. Next to **CD/DVD Media**, click **Browse** and select the ISO image that you unpacked and uploaded in "Unpacking and uploading the ISO zip file" on page 27. Then click **OK**.
6. Select **Connect At Power On**.
7. Click **Next**.
8. Review your settings. Then click **Finish**.

Result
The new virtual machine is created.

Step 3: Delete the ISO image connection

Once the new virtual machine is created, delete the connection to the ISO image.

Important: Failure to delete the connection to the ISO image could lead to accidental reinstallation of the appliance operating system, or nodes failing to start.

Procedure

1. In the **New Virtual Machine** wizard, right-click the virtual machine that is connected to the ISO image and click **Edit settings > VM Hardware**.

   The Edit Settings page opens.to the **Virtual Hardware** tab.
2. Expand **New CD/DVD Drive** <*drive number*>.
3. Clear the **Connect At Power On** option.
4. Clear the **Connected** check box in the same row as **New CD/DVD Drive** <*drive number*>.
5. Click the **x** icon next to the **Connected** check box.

Result
The connection to the ISO image is deleted.

Installing the Appliance Operating System

After deploying the ISO file, you need to complete the next procedure for each HCM VM node in the vSphere cluster.

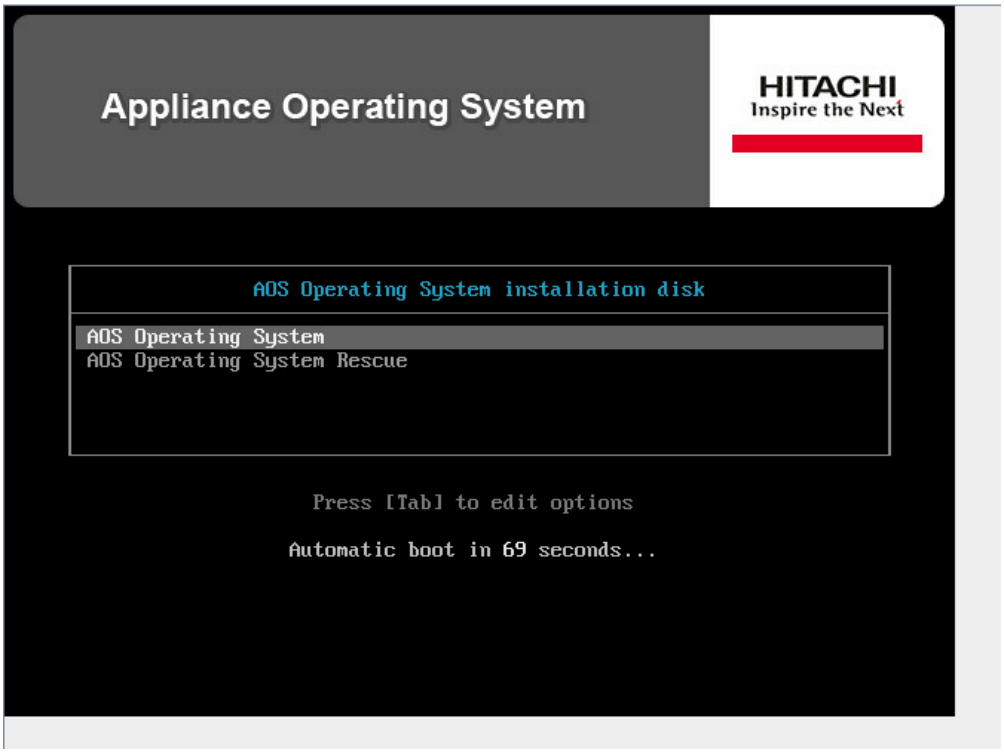
Before you begin

You will need the front-end IP addresses, network mask, default gateway and back-end IP addresses from the network administrator at the customer site. All back-end IP addresses must be on the same subnet. For easier installations and support, request the last octet of the front-end and back-end be sequential.

Procedure

1. Power on the first node.
2. Start the vSphere Client.
3. In the left navigation bar, right-click the lowest numbered node and click **Open Console**.

   The installation program prompts for the installation mode.



4. 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.

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

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

5. Enter *c* to clear existing storage volumes.

6. In response to the confirmation 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): _
```

7. 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):
```

8. 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 do not want to provide a VLAN ID.

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

   - If you entered *y*, 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*, the installation program does not prompt you to enter a VLAN ID.

9. If you entered *IPv4* or *Dual*, specify the IPv4 node IP address, subnet mask, and gateway IP address for the front-end network.

   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]:
                                 --->
   ```

10. If you entered *IPv6* or *Dual*, respond to the additional configuration prompts.

11. 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 the previous prompts and asks you to confirm.

12. Respond as appropriate.

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

    When the installation is complete, the node reboots and displays the Appliance OS login screen on the console. The node is ready for the HCP software installation.

Note: If the node does not automatically reboot, the Appliance OS installation failed. Contact your authorized HCP service provider for assistance.

13. Complete the previous steps on each node of the HCP VM system.

Installing the HCP software

The HCP installation is performed from the node with the highest last octet in its back-end IP address.

For example, if the four back-end IP addresses for a system are *172.21.150.150*, *172.21.150.151*, *172.21.150.152*, and *172.21.150.153*, you would perform the HCP software installation on node *172.21.150.153*.

Note: Although you can install the HCP system, you cannot enable data-at-rest encryption (DARE). DARE encrypts data on primary storage and data tiered to external storage pools. If you plan to use DARE features, contact your authorized HCP service provider before performing the software installation.

Procedure

1. Access the vSphere client.
2. In the left navigation bar, select the node with the highest last octet in its back-end IP address.
3. Right-click the VM and click **Open Console**.
4. Log in to the HCP VM node console with the default login information:
   - Username: `install`
   - Password: `Chang3Me!`
5. Change the password to hcpinsta11 (the last two characters are the number one).
6. Press Enter to display the HCP Configuration menu.

   The next screen is included for illustrative purposes. Your screen will specify the HCP version that you are running.

```
HCP 8.1 Configuration Menu
==================================
[1] Get HCP Setup Files
[2] Install an HCP System
[3] Upgrade an HCP System
[4] Add a Node to an HCP System
[5] Perform Checks for Offline Upgrade
[6] Perform Checks for Online Upgrade
[v] Add Logical Volumes to an HCP System
[s] Perform a Service Procedure
[q] Log Out

Currently installed version:  8.1.0.1
Version on CD/DVD:               None
Extracted version:            8.1.0.1

Enter a selection: 2

You chose: "2", is this correct? [Default: yes]:
```

7. Enter 2.

8. In response to the confirmation prompt, press Enter.

The New Install menu in the HCP Setup wizard is displayed.

```
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] Security and Encryption Settings

[c] Load HCP Configuration File
[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]:
```

Step 1: Identify the nodes in the HCP system

Procedure

1. In the HCP Setup wizard **New Install** menu, enter **1**.

```
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] Security and Encryption Settings

[c] Load HCP Configuration File
[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]: 1
```

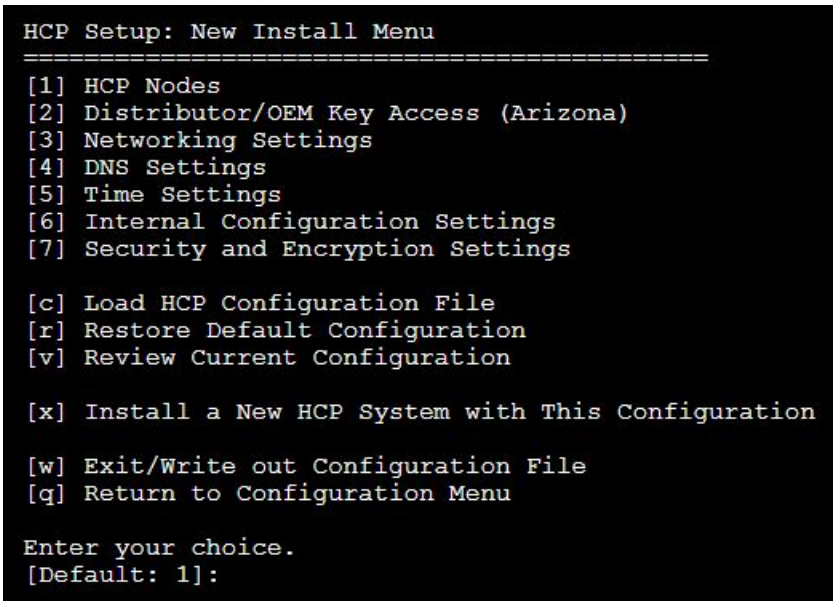
When you enter **1**, the **HCP Nodes** menu appears.

```
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]:
```

2. 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 is one greater than the previous IP address that you entered.

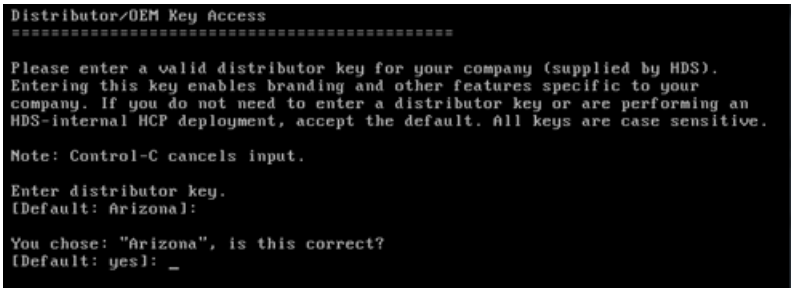
3. From the **HCP Nodes** menu, enter **b** to return to the **New Install** menu.



Step 2: Configure the HCP system

Procedure

1. From the **New Install** menu, enter **2** to change the key access settings.



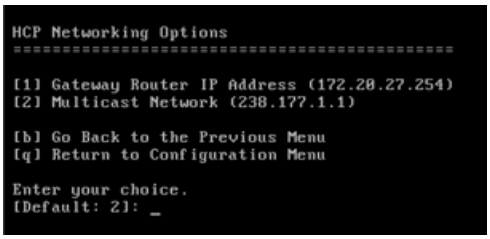
2. Change the distributor key.

Tip: If this system is provided by Hitachi Vantara, keep the default Arizona key.

3. Enter *y* or *yes* to confirm the change.

   You are returned to the **New Install** menu.

4. Enter **3** to configure the networking options.



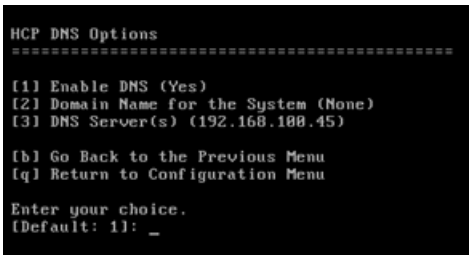
5. Enter **1** and change the **Gateway router IP address**.

6. Enter **2** and change the **Multicast Network**.

7. Enter **b**.

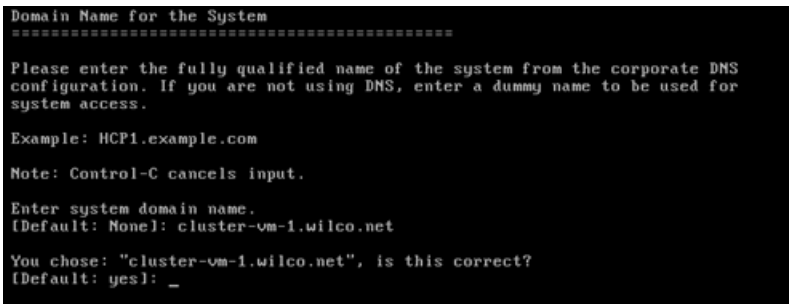
   You are returned to the **New Install** menu.

8. Enter **4** to configure the DNS options.



9. Enter **2** to input the domain name for the system.

10. Enter the system domain name.



11. If **Option 1: Enable DNS** is not set to yes, change it to yes.

12. If **Option 3: DNS Servers** is not set to the proper corporate DNS server, change it accordingly.

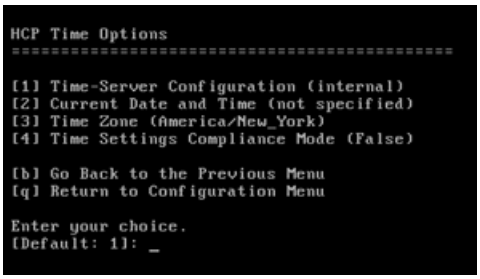
13. Enter **b**l

    You are returned to the **New Install** menu.

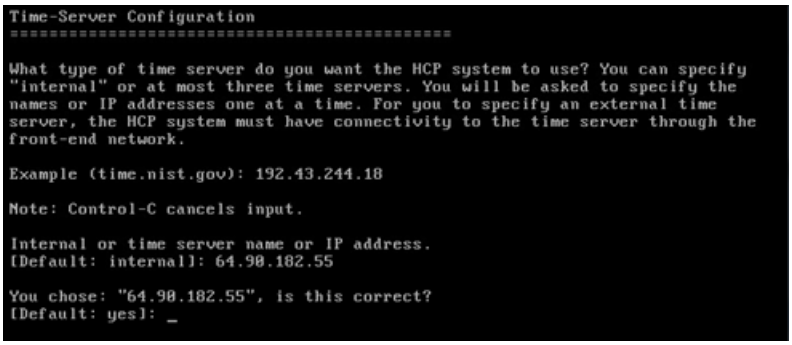
14. Enter **5** to configure the time settings.

15. Enter **1** and set the time configuration to a time server. Use the same time server that has been configured for all ESXi hosts in the HCP VM system.

    You previously configured the time server for all ESXi hosts in "Enabling NTP for the ESXi hosts" on page 16.



16. Specify an external time server or enter *internal*.



17. Enter *y* or *yes* to confirm the change.

    You are returned to the **New Install** menu.

18. Enter **6** to change the internal configuration settings.

When you enter **6**, the **Internal Configuration Settings** menu is displayed.

```
Internal Configuration Settings
===============================================
[1] Storage Configuration (Not Set)
[2] HCP System Serial Number (00001)
[3] Enable Replication on This System (Yes)
[4] Reinstallation with DNS Failover in Effect (No)
[5] Customer Support Contact Information

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

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

19. Enter **1** to set the storage configuration.

```
Storage Configuration
=============================================
What type of storage does this HCP system use? If the storage is
local/internal RAID, type "internal". If the storage is fibre channel or other
SAN-attached storage, type "external".

Note: Control-C cancels input.

Enter internal or external.
[Default: internal]: internal

You chose: "internal", is this correct?
[Default: yes]:

Do you want to configure a dedicated database volume?
[Default: no]: yes

You chose: "yes", is this correct?
[Default: yes]:
```

20. Type `internal`.

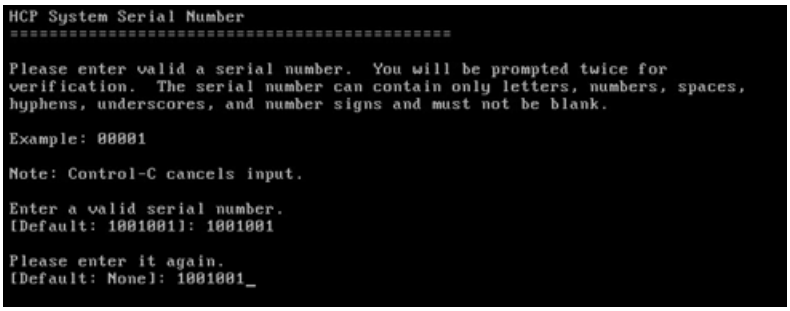
21. In response to the confirming prompt, press Enter .

Optionally, if you want to configure a dedicated database volume, the system needs to have at least three drives per node. Also, the dedicated database volume size needs to be at least 50 GB for a new installation. All dedicated database volumes need to be the same size. HCP Setup asks if you want to configure a dedicated database volume only if your system meets the above requirements.

22. If HCP Setup asks whether you want to configure a dedicated database volume, enter *yes* if you want to configure a dedicated database volume or *no* if you do not want to configure a dedicated database volume.

23. Press Enter to confirm your choices and return to the **Internal Configuration Settings** menu.

24. From the **Internal Configuration Settings** menu, enter **2** to set the serial number for the HCP system.



25. Enter the unique serial number for this HCP system.

26. Enter the serial number again for confirmation and return to the **Internal Configuration Settings** menu.

Important: The HCP system serial number is required to license the system. Omitting the serial number will cause the system to report that you are in violation of your license agreement.

27. From the **Internal Configuration Settings** menu, enter **3** to configure whether replication will be enabled.

    If you enter **yes** to enable replication, the wizard asks if this is a reinstallation of a primary system after a replication failover with DNS failover enabled. If you enter *yes* to this prompt, it requests that target replicated namespaces in this system will continue to be redirected to the replica until data recovery is complete, provided that those namespaces are configured to accept such requests.

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

28. From the **Internal Configuration Settings** menu, enter **4** to configure whether reinstallation with DNS failover will be enabled.

29. From the **Internal Configuration Settings** menu, enter **5** to set contact information. To specify no contact information, press the spacebar key.

30. Enter **b** to return to the **New Install** menu.

Step 3: Run the HCP installation

Before you begin

If you enabled encryption in the previous section, have your security administrator present for this procedure. The security administrator should be the only person to see the encryption key.

Procedure

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

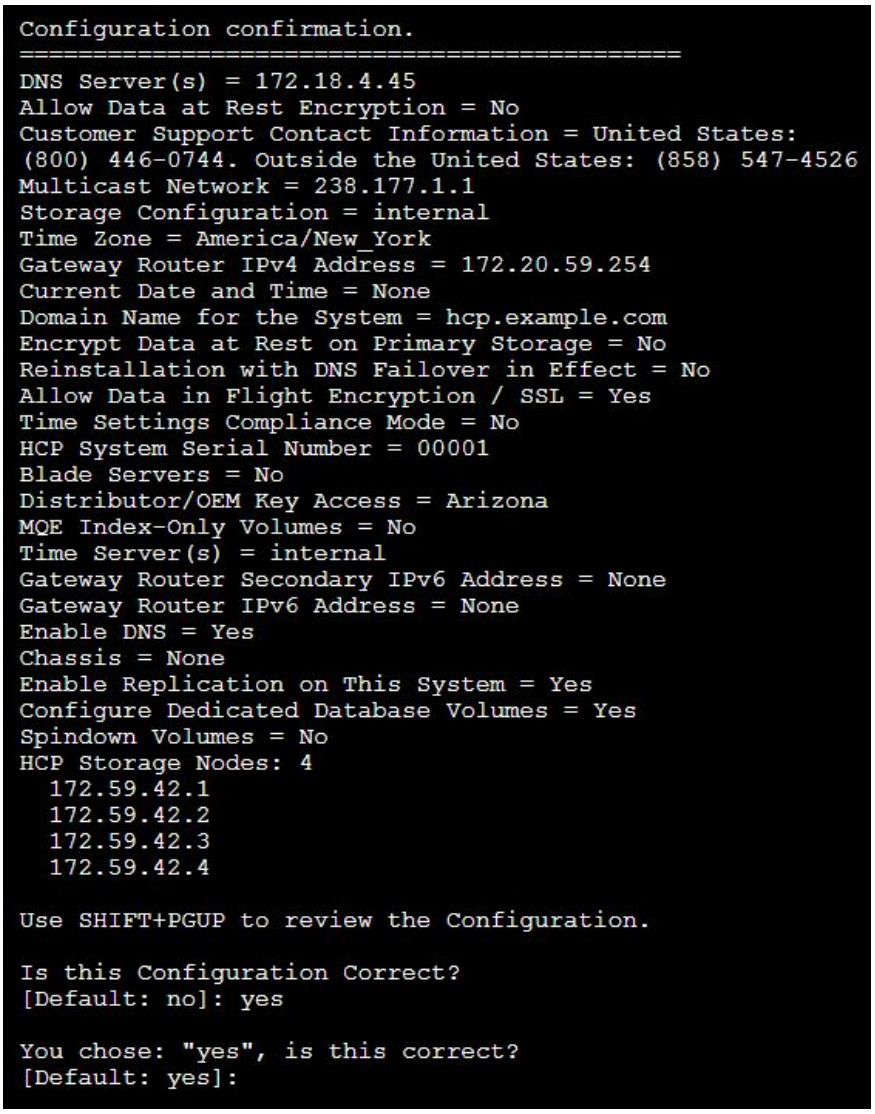
   If you running the installation as the install user, the wizard informs you that data-in-flight encryption is enabled. The wizard asks for confirmation that it is legal to ship a system with data-in-flight encryption enabled to the country where the system will be deployed.

```
Confirm Data in Flight Encryption / SSL
===============================================
Data-in-flight encryption has been enabled for this HCP system.  Global trade
compliance prohibits shipping HCP systems to restricted countries with this
feature enabled.  Are you sure it is legal to ship an HCP system with data-in-
flight encryption enabled to the country where the system will be deployed?

Note: Control-C cancels input.

Enter yes or no.
[Default: no]: yes

You chose: "yes", is this correct?
[Default: yes]:
```

2. Enter `yes` to continue.

3. Press Enter to confirm.

The wizard displays the configuration confirmation.



4. Review the configuration. Then complete one of the next actions.
   - If the configuration is not correct:
     a. Enter `n` or `no`.
     b. In response to the confirmation prompt, enter `y` or `yes`.
     c. Correct the configuration information.
   - If the configuration is correct:
     a. Enter `y` or `yes`.

b. In response to the confirmation prompt, enter `y` or `yes`.

5. After you confirm that the configuration information is correct, HCP Setup performs a set of installation prechecks.

```
You chose: "yes", is this correct?
[Default: yes]:
Verifying system name
Verifying run location
Verifying running as install
Verifying node connections
Verifying SSH keys
Verifying SSH
Verifying systemwide SSH
Verifying total memory > 32GB
Verifying all network links
Verifying software versions
Verifying 64-bit hardware platform
Verifying drive size
Verifying disk space
Verifying nobody using /fcfs_*
Verifying nobody using /fs/*
Verifying multicast enabled
Syncing install password to all nodes.
Updating EULA
Syncing timezone to all nodes
Syncing date to all nodes.
Generating auth keys
Generating system UUID
Syncing HCP package to all nodes
Checking to see if we need to run update schemaupgrade scripts False
Updating schema scripts for upgrade.
...
```

6. Conditional: If you previously selected that you want to configure dedicated database volumes, complete the next substeps.

a. When prompted, select the dedicated database volume for the first node.

b. Press Enter to confirm your selection.

c. Repeat the above two substeps for each node in the system.

d. After you select the dedicated database volumes for each node, HCP Setup confirms your selections and asks if you want to continue.

```
...
Select dedicated volume for each node.
Found these volumes:
       node 001:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 002:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 003:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 004:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)
Select dedicated database volume for node 001: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 002: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 003: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 004: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Following volumes will be configured as dedicated database volumes:
       node 001: 4. /dev/sde at 2:0:0:4 (1TB)
       node 002: 4. /dev/sde at 2:0:0:4 (1TB)
       node 003: 4. /dev/sde at 2:0:0:4 (1TB)
       node 004: 4. /dev/sde at 2:0:0:4 (1TB)
Do you want to continue? [Default: yes]?
...
```

e. Press Enter to continue.

If the prechecks are successful, the HCP software is installed on all nodes in the system. Depending on the size of the logical volumes, this can take from several minutes to several hours.

If you enabled encryption in the system configuration, HCP Setup performs some initial setup tasks and then displays the encryption key. It then prompts you to enter the key.

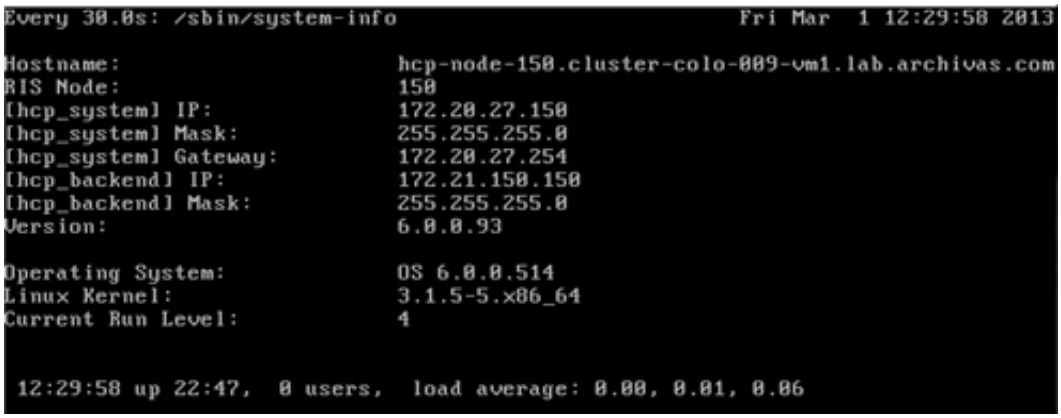
Important: Before entering the encryption key, record it. Once you enter the key, HCP Setup completes the installation. You do not get a second chance to see the key, and it is not stored for later retrieval.

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 before installation processing is complete, record all error messages. Then contact your authorized HCP service provider for assistance.

After the installation is complete, the HCP VM nodes reboot, and, instead of the operating system login prompt, you should see an **hcp-node-*nodeNumber*** prompt.

You can also check the run level of a node by pressing Alt+F5 at the console prompt.



Step 4: Verify the HCP software installation

Procedure

1. Open the System Management Console by entering one of the following URLs in a client web browser:

   - If the HCP system is configured for DNS:

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

   - If the HCP system is not configured for DNS:

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

     where *node-ip-address* is the front-end IP address of a storage node in the HCP system.

   If you enter *http* instead of *https*, the browser returns an error.

2. When prompted, accept the self-signed HCP SSL server certificate either permanently or temporarily. Set a temporary certificate if you plan to install a trusted certificate later on.

   The System Management Console login page is displayed.

Tip: If the browser cannot find the System Management Console login page, wait a few minutes and then try again. If the login page still does not open, contact your authorized HCP service provider.

3. Verify the serial number on the login page. If it is incorrect, contact your authorized HCP service provider.

4. Log in to the System Management Console with the following username and password:

   Username: `security`
   Password: `Chang3Me!`

   After you log in, the Console displays either the **Change Password** page or the **Hardware** page. Perform one of the following actions:

   - If the **Hardware** page is displayed, the nodes are still starting HCP. This process can take several minutes. When more than half the nodes have completed the startup process, the Console displays the **Change Password** page.

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

5. On the **Change Password** page, enter the following information:

   a. In the **Existing Password** field, enter `Chang3Me!`.

   b. In the **New Password** field, enter a new password.

   Password criteria:

   - Must contain UTF-8 characters, including whitespaces
   - Minimum of six characters
   - Maximum of 64 characters

- Must include at least one character from two of the following groups: alphabetic, numeric, and special characters.

  Examples:

  - Valid password: `P@sswOrd`
  - Invalid password: `password`

c. In the **Confirm New Password** field, retype your new password and click **Update Password**.

6. In the top-level menu, click **Hardware**.

7. On the **Hardware** page, ensure the following statuses:

- **Node status**: **Available**.
- **Status of each logical volume**: **Available**.

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

If all the nodes and logical volumes are available, the installation was successful and you can begin creating tenants. However, you may not want to do this until all additional setup is complete.

If any node has a status other than **Available**, or any logical volume associated with an available node has a status other than **Available** or **Spun down**, contact your authorized HCP service provider. Also contact your service provider if the number of logical volume icons for any node does not match the expected number of logical volumes for the node.

8. Complete either of the next steps.

- Set additional configuration options, as described in "Setting additional configuration options" on the next page. You can set additional configuration options only if the installation was successful.
- Log out of the System Management Console and close the browser window. This action ensures that no one else can use the Console without logging in.

Setting additional configuration options

After verifying that the HCP system was correctly installed, you can set additional configuration options.

You can set additional configuration options such as enabling the management port network, enabling syslog logging, or disabling ping.

Procedure

1. Log into the HCP System Management Console as the security user.
2. Create a new user account with the administrator role.

   Alternatively, you can add the administrator role to the security user account and then go to step 4.
3. Log out of the Administration Console. Then log in again using the new account with the administrator role.
4. Perform the configuration activities.
5. Log out of the System Management Console and close the browser window.

Monitoring and alerting

HCP hardware appliance features such as redundant hardware, monitoring, alerting and failover behavior cannot be used by VMware environment. To maintain performance and data integrity, HCP VM system hardware must be monitored for failures outside of the virtual machine environment.

Hitachi servers and network components that are part of the HCP VM system can be connected to Hitachi Remote Ops for monitoring. For more information, see Chapter 6: "Configuring HCP monitoring with Hitachi Remote Ops" on page 77

To monitor hardware supplied by vendors other than Hitachi, use a vendor-supplied or hardware-compatible software tool.

Any failures in the HCP VM infrastructure must be corrected as soon as possible. Drive failures, in particular, should be closely monitored, because of the possibility of long RAID rebuild times.

HCP Intelligent Platform Management Interface (IPMI) monitoring and Hitachi array monitoring is not available for HCP VMs.

Software monitoring

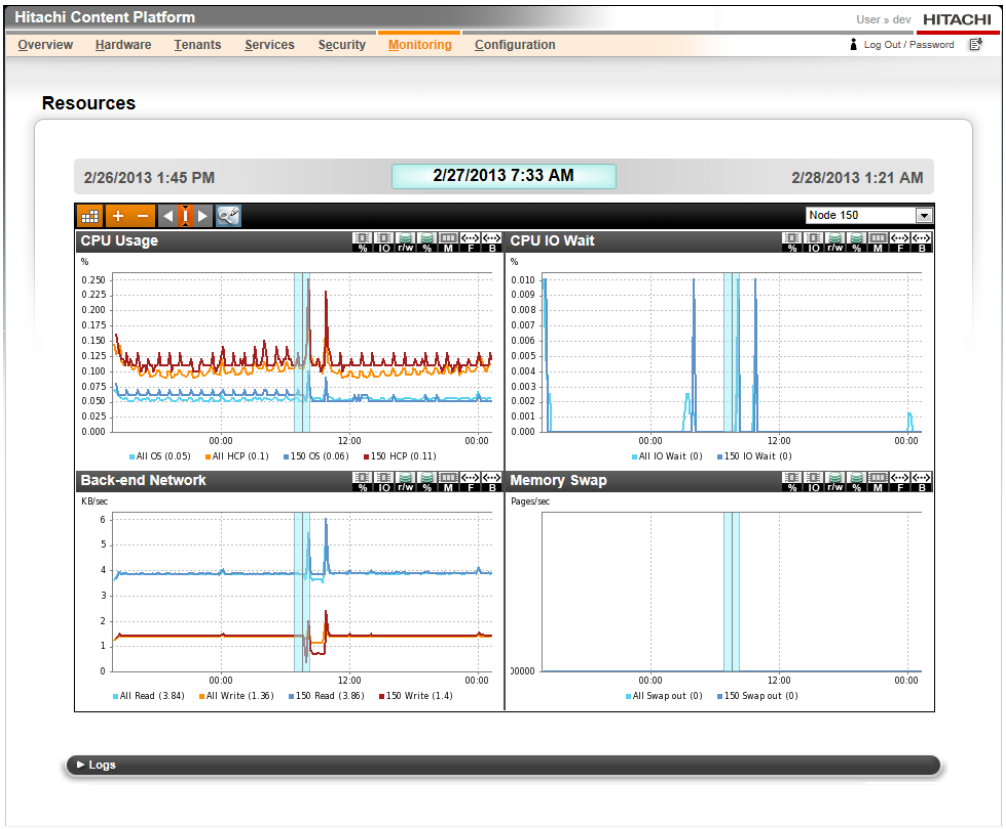
HCP maintains a system log that logs all system events. You can view this log in the HCP System Management Console. You can send system log messages to syslog servers, System Network Management Protocol (**SNMP**) managers, and email addresses. Additionally, you can use SNMP to view and, when allowed, change HCP system settings.

You can generate chargeback reports to track system capacity and bandwidth usage at the tenant and namespace levels.

You can use Hitachi Remote Ops to monitor the health of the HCP software. For more information, see Chapter 6: "Configuring HCP monitoring with Hitachi Remote Ops" on page 77

HCP VM resource monitoring

HCP uses System Activity Reporter (SAR) data for resource usage reporting. SAR runs on each node in the HCP system. Every ten minutes, SAR records statistics about the average use of resources in the node for the past time interval. The graphs on the resources page of the System Management Console show the statistics for a subset of those resources. The resources that are monitored include the CPU, logical volumes, memory, and networks.



HCP VM diagnostic menu

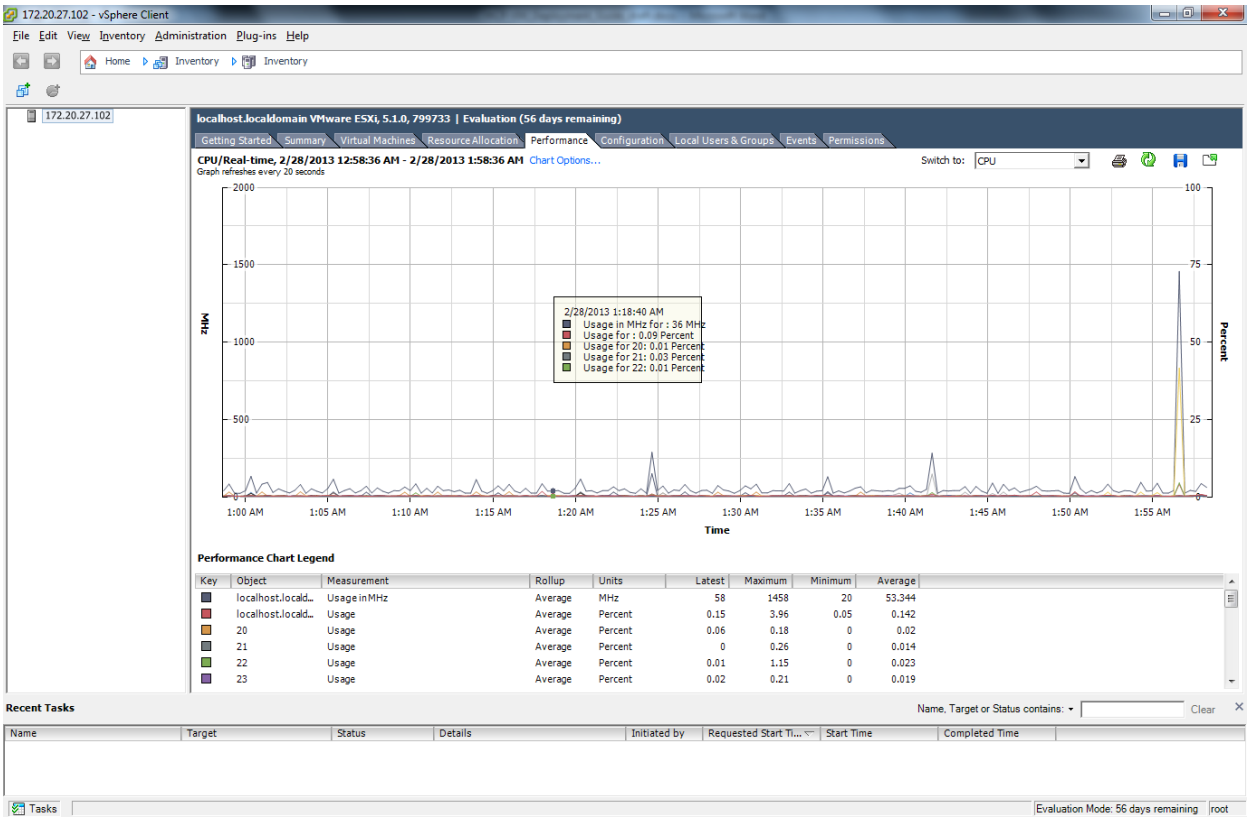
For any HCP VM node, you can run diagnostics that analyze and resolve issues with interactions between nodes and other components of the HCP environment.

HCP VM node diagnostics are available through the HCP System Management Console. The diagnostics let you:

- **Ping** - Test if a selected device is accessible through the network.
- **Traceroute** - Display the network path used for communication between the node and a specified device.
- **Dig** - Query the DNS for the records that match a specified IP address or domain name.
- **Route** - Display the routing table for a node.
- **Showmount** - Display the NFS exports table for a specified device.

For more information about HCP system monitoring, see the HCP System Management Help.

VMware Monitoring and Performance is the responsibility of the customer. In the vSphere center, under the performance tab, clients have multiple ways to monitor resources.



For more information about VMware vSphere monitoring options, see the VMware web site.

5

Maintenance procedures

This chapter describes how to keep your HCP VM system running at an optimal performance level.

Adding logical volumes

Procedure

1. Provision the LUNs to be added to each ESXi host in the system. See "Provisioning HCP VM storage" on page 18 for details.
2. Add the LUNs to new datastores, one LUN per datastore. See "Adding VMFS datastores to a vSphere HA cluster" on page 21 for details.
3. From the VMware Sphere client, right-click the HCP VM to which you want to add capacity and select **Edit Settings**.
4. In the **Virtual Machine Properties** window, click **Add**.
5. In the **Add Hardware** window, select **Hard Disk**.
6. Click **Next**.
7. Select **Create a new virtual disk**.
8. Click **Next**.
9. Set the capacity to be slightly smaller than the size of the provisioned LUN. VMware adds a small amount of overhead.
10. Select **Thick Provision Eager Zeroed**.
11. Browse to the new datastore to be added and click **Next**.

12. Select the next available SCSI disk in the Virtual Device node section and click **Next**.

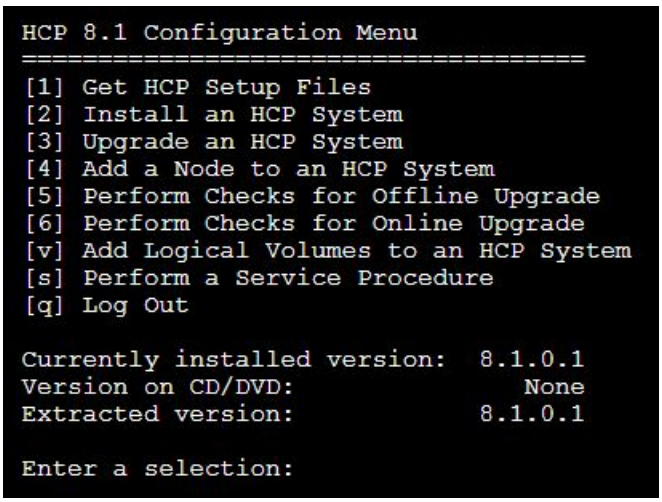
13. Verify the options selected and click **Finish**.

14. Back in the **Virtual Machine Properties** window, verify that the new hard disk is listed. Then click **OK**.

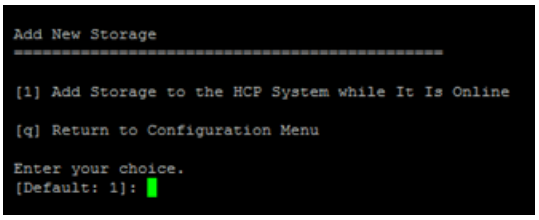
15. In the vSphere client, open the virtual machine console for the highest numbered storage node.

16. Log in as the install user.

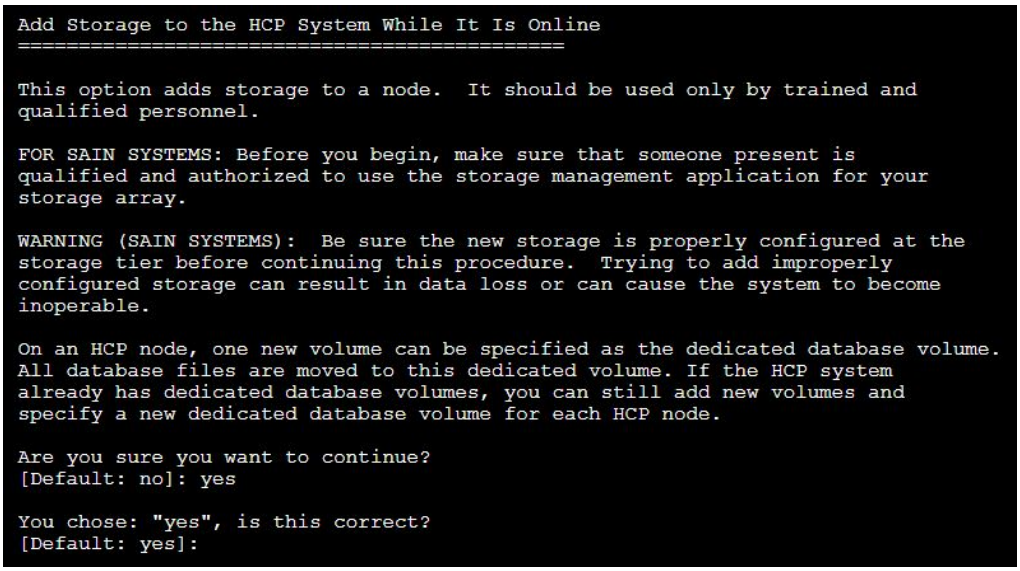
    The **HCP Configuration Menu** is displayed. The following screen is included for illustrative purposes. Your screen will specify the HCP version that you are running.



17. Enter *v* to add logical volumes to an HCP system.



18. Enter *1* to add storage to the HCP System while it is online.



19. Enter *yes* to continue the procedure.

20. Press Enter to confirm.

After you have confirmed that you want to add storage, HCP Setup performs a set of installation prechecks.

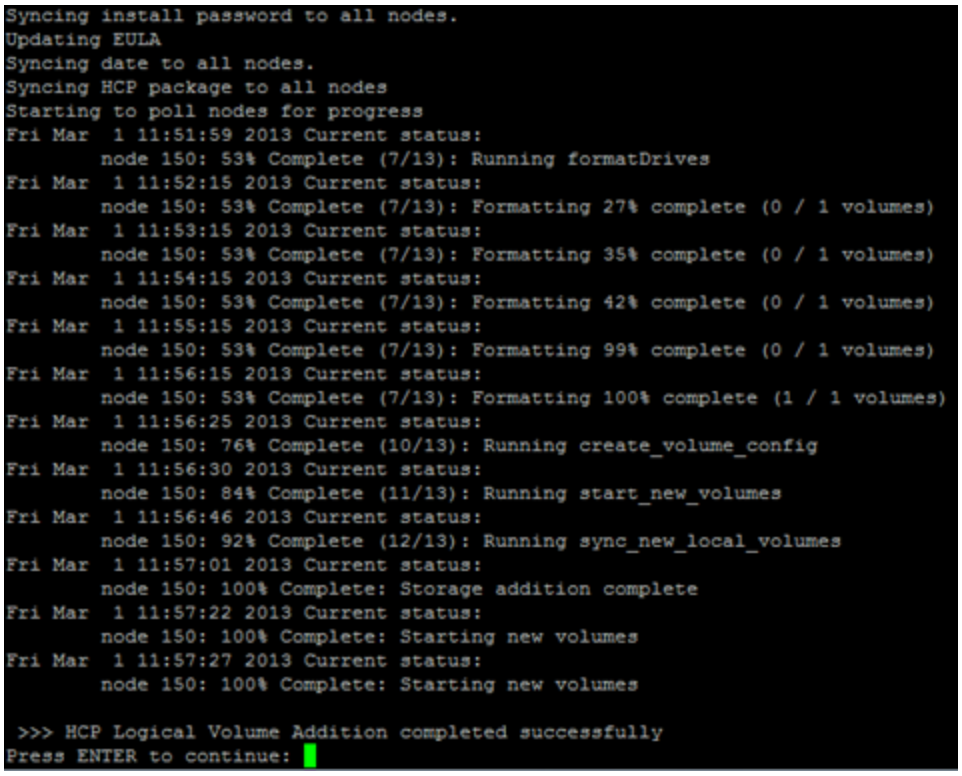
```
Verifying correct menu
Verifying system name
Verifying run location
Verifying running as install
Verifying node connections
Verifying SSH keys
Verifying SSH
Verifying systemwide SSH
Verifying all network links
Verifying software versions
Verifying all nodes available
Verifying upgrade state
Verifying 64-bit hardware platform
Verifying drive size
Verifying disk space
Verifying nobody using /fcfs_*
Verifying nobody using /fs/*
Verifying storage tiering service is disabled
Searching for new storage volumes
Verifying multicast enabled
Found these new volumes:
       node 001:
              1. /dev/sdd at 2:0:0:3 (500GB)
              2. /dev/sde at 2:0:0:4 (1TB)

       node 002:
              1. /dev/sdd at 2:0:0:3 (500GB)
              2. /dev/sde at 2:0:0:4 (1TB)

       node 003:
              1. /dev/sdd at 2:0:0:3 (500GB)

       node 004:
              1. /dev/sdd at 2:0:0:3 (500GB)

Is this correct? [y/n]: y
```

21. Enter *y* to verify the new volumes that were found. Typically this would show storage added to all nodes.

Optional: If you want to configure a dedicated database volume, the volume size needs to be at least 50 GB and at least 1.5 times the size of the existing database for each node. All dedicated database volumes need to be the same size. If you already have a dedicated database volume, any newly-added dedicated database volume needs to be larger than the current one.

22. If HCP Setup asks whether you want to select a dedicated volume for the database, perform one of the following:

- If you do not want to select a dedicated volume for the database, enter *no*. HCP Setup formats and adds the new volumes. During this process, HCP Setup reports on its progress.



- If you want to select a dedicated volume for the database, enter *yes*. Then complete the next substeps. , then:

  a. If you want to select a dedicated database volume for the first node, enter *yes*.

  b. If you entered *yes*, select the dedicated database volume for the first node.

  c. Press Enter to confirm your selection.

  d. Repeat the above three steps for each node in the system.

23. After you have selected the dedicated database volumes for each node, HCP Setup confirms your selections then asks if you want to continue the procedure. Enter *yes* to continue the procedure.

```
Do you want to select a dedicated volume for database? [Default: no]: yes
Do you want to select a new dedicated PG LUN for node 001? [Default: no]: yes
Enter a selection for node 001 [1, 2]: 2
You chose: "2. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]: yes
Do you want to select a new dedicated PG LUN for node 002? [Default: no]: yes
Enter a selection for node 002: 2
You chose: "2. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]: yes
Do you want to select a new dedicated PG LUN for node 003? [Default: no]: yes
Do you want to select a new dedicated PG LUN for node 004? [Default: no]: yes
This will add the new volumes and move database to the following dedicated
volumes. Do you want to continue?
   node 001: 2:0:0:4 (1TB)
   node 002: 2:0:0:4 (1TB)
   node 003: 2:0:0:3 (500GB)
   node 004: 2:0:0:3 (500GB)
[Default: no]: yes
```

HCP Setup formats and adds the new volumes. During this process, HCP Setup reports on its progress.

```
Syncing install password to all nodes.
Updating EULA
Syncing date to all nodes.
Syncing HCP package to all nodes
Starting to poll nodes for progress
Fri Mar  1 11:51:59 2013 Current status:
        node 150: 53% Complete (7/13): Running formatDrives
Fri Mar  1 11:52:15 2013 Current status:
        node 150: 53% Complete (7/13): Formatting 27% complete (0 / 1 volumes)
Fri Mar  1 11:53:15 2013 Current status:
        node 150: 53% Complete (7/13): Formatting 35% complete (0 / 1 volumes)
Fri Mar  1 11:54:15 2013 Current status:
        node 150: 53% Complete (7/13): Formatting 42% complete (0 / 1 volumes)
Fri Mar  1 11:55:15 2013 Current status:
        node 150: 53% Complete (7/13): Formatting 99% complete (0 / 1 volumes)
Fri Mar  1 11:56:15 2013 Current status:
        node 150: 53% Complete (7/13): Formatting 100% complete (1 / 1 volumes)
Fri Mar  1 11:56:25 2013 Current status:
        node 150: 76% Complete (10/13): Running create_volume_config
Fri Mar  1 11:56:30 2013 Current status:
        node 150: 84% Complete (11/13): Running start_new_volumes
Fri Mar  1 11:56:46 2013 Current status:
        node 150: 92% Complete (12/13): Running sync_new_local_volumes
Fri Mar  1 11:57:01 2013 Current status:
        node 150: 100% Complete: Storage addition complete
Fri Mar  1 11:57:22 2013 Current status:
        node 150: 100% Complete: Starting new volumes
Fri Mar  1 11:57:27 2013 Current status:
        node 150: 100% Complete: Starting new volumes

 >>> HCP Logical Volume Addition completed successfully
Press ENTER to continue:
```

24. When the formatting is complete, press Enter to continue.

25. Log in to the HCP System Management Console to verify the newly added volumes.

Moving storage node databases to optimal volumes

Procedure

1. From the **HCP Configuration** menu, enter `s` to display the **HCP Service** menu.

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 **HCP Service** menu appears.

```
HCP Service Menu
================================================
[1] Recover an HCP Node
[2] Display the Current System Status
[3] Shut down the HCP System
[4] Free Space on Nodes
[5] Install a Hotfix
[6] Finalize Migration
[7] Change Region Count
[8] Configure Routine Database Maintenance
[9] Configure Time Settings
[10] Migrate Metadata Regions
[11] Perform Node Swap
[s] Perform SSD Maintenance
[m] Manage Database Volumes

[q] Return to Configuration Menu

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

3. From the **HCP Service** menu, enter `m`.

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`, HCP Setup displays the **Manage Database Volumes** menu.

```
Manage Database Volumes
================================================

[1] Move Database

[d] Delete Old Database

[q] Return to Configuration Menu

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

5. From the **Manage Database Volumes** menu, enter **1**.

6. 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 displays the **Move Database** menu.

```
Move Database
=============================================

Volumes to move:

Node          |  Type   | Current volume     | New volume
              |         | (Available/Total)  | (Available/Total)
--------------|---------|--------------------|-------------------
172.20.59.125 | pgdata  | /RIS/archive33     | /RIS/archive94
              | pgidx   | (450M/100G)        | (180G/200G)
172.20.59.125 | pgxlog  | /RIS/archive34     | /RIS/archive95
              |         | (450M/100G)        | (180G/200G)
172.20.59.129 | pgxlog  | /RIS/archive33     | /RIS/archive94
              |         | (350M/100G)        | (150G/200G)

Executing this procedure will move the database from the current volume
to the new volume. This process cannot be undone after it is complete.
Please review the changes before proceeding.

Do you want to move the database?
[Default: no]: yes
You chose: "yes", is this correct?
[Default: yes]: yes
```

   From the **Move Database** menu, HCP setup asks you to review your database configuration and warns you that the process cannot be undone after the database move is complete.

7. When you have reviewed the configuration, enter `y` or `yes` to confirm the move or `n` or `no` to try again.

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

   Once the procedure is initiated, the progress of the database move appears and details the current status of the HCP Service Procedure.

```
 Starting to poll nodes for progress
Thu Jan 12 09:51:15 2017 Current status:
    node 042: 40% Complete (2/5): Running arcShutdown
Thu Jan 12 09:52:13 2017 Current status:
    node 042: 60% Complete (3/5): Running mountDisks
Thu Jan 12 09:52:48 2017 Current status:
    node 042: 80% Complete (4/5): Running move_pgdata
Thu Jan 12 09:52:55 2017 Current status:
    node 042: 100% Complete: Deploy complete
Thu Jan 12 09:54:07 2017 Current status:
    node 042: 100% Complete: Rebooting node
Thu Jan 12 09:54:12 2017 Current status:
    node 042: 100% Complete: Waiting for node to become available.
Thu Jan 12 09:56:12 2017 Current status:
    node 042: 100% Complete: Waiting for node to become available.
Thu Jan 12 09:58:13 2017 Current status:
    node 042: 100% Complete: Waiting for node to become available.
Thu Jan 12 10:00:03 2017 Current status:
    node 042: 100% Complete: All nodes available
Thu Jan 12 10:00:38 2017 Current status:
    node 042: 100% Complete: All nodes available and metadata is balanced

>>> HCP Service Procedure successful
Press ENTER to continue:
```

When the procedure is complete, press Enter to return to the **HCP Service** menu. You can now delete the database from the older database volume.

Deleting databases from older database volumes

Procedure

1. From the **HCP Configuration** menu, enter `s` to display the **HCP Service** menu.

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 **HCP Service** menu is displayed.

```
HCP Service Menu
================================================
[1] Recover an HCP Node
[2] Display the Current System Status
[3] Shut down the HCP System
[4] Free Space on Nodes
[5] Install a Hotfix
[6] Finalize Migration
[7] Change Region Count
[8] Configure Routine Database Maintenance
[9] Configure Time Settings
[10] Migrate Metadata Regions
[11] Perform Node Swap
[s] Perform SSD Maintenance
[m] Manage Database Volumes

[q] Return to Configuration Menu

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

3. From the **HCP Service** menu, enter **m**.

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`, HCP Setup displays the **Manage Database Volumes** menu.

```
Manage Database Volumes
=======================================

[d] Delete Old Database

[q] Return to Configuration Menu

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

5. From the **Manage Database Volumes** menu, enter **d**. You can delete the database from the older database volume only if you have completed the database move procedure.

6. 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 displays the **Delete Old Database** menu.

```
Delete Old Database
=========================================

WARNING: This procedure deletes the old HCP database from its original storage volumes.
The database on the optimal storage volumes will be preserved.

Do you want to continue? Yes or No.
[Default: no]: yes

Deleting the old database: #

The old database has been deleted. Press ENTER to continue:
```

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

   Once the procedure is complete, press Enter to return to the **HCP Service** menu.

Adding HCP VM nodes

Before you begin

1. Add new ESXi hosts or find existing ESXi hosts that can support an HCP node. For more information, see Chapter 3: "Configuring the HCP VM environment" on page 15.

2. Unpack and upload the ISO files to the selected ESXi hosts. For more information, see "Unpacking and uploading the ISO zip file" on page 27.

3. Create the new virtual machine. For more information, see "Creating and configuring the new virtual machine" on page 27.

4. Configure the HCP VM network on the newly deployed HCP VM nodes. For more information, see "Installing the Appliance Operating System" on page 32.

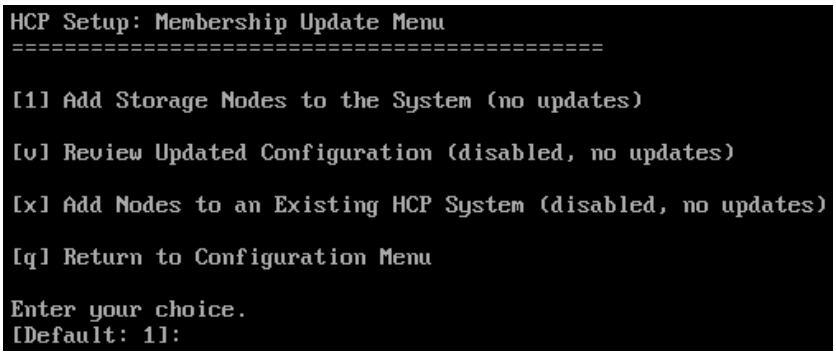
5. From the highest active HCP VM node, run the **Add Node** service procedure. For more information, see *Installing and Maintaining an HCP System*.

Procedure

1. From the **Configuration** menu, enter `4` 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`, the **Membership Update** menu is displayed.



3. From the **Membership Update** menu, enter `x` to perform the node addition.

   The wizard displays an explanation of the node addition procedure.

```
Add Nodes to an Existing HCP System
===========================================

This option will erase all data on the new nodes, install the HCP software on
those nodes, and add the nodes to the system configuration.

Note: Control-C cancels input.

Enter yes or no.
[Default: no]: _
```

4. In response to the confirming prompt, enter `y` or `yes` to confirm your entry, or `n` or `no`to back out.

   The wizard prompts again for confirmation.

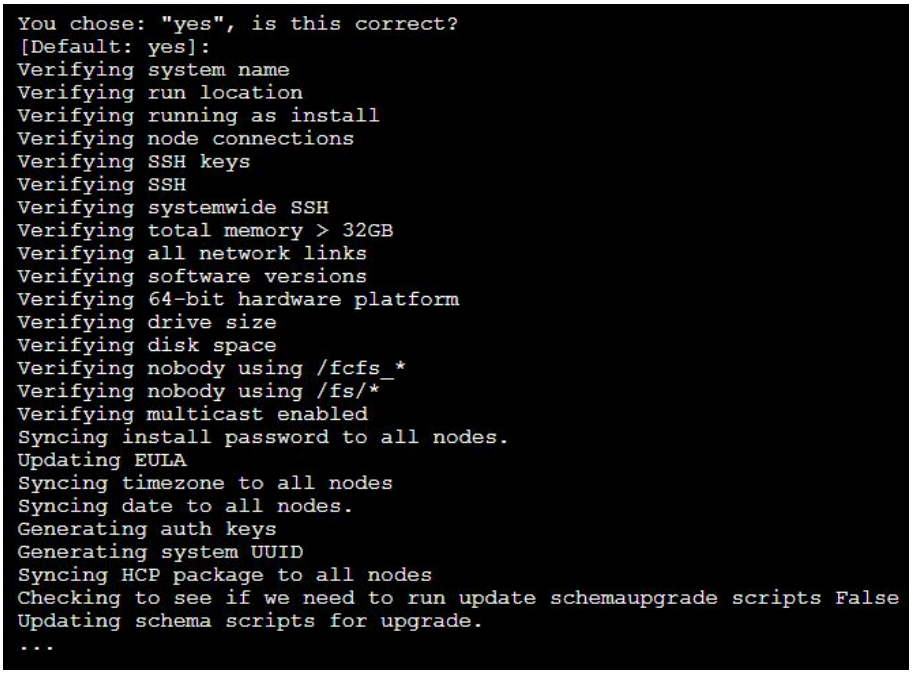
5. In response to the confirming prompt, enter `y` or `yes` to confirm your entry, or `n` or `no` to try again.

   After you confirm that you want to add nodes, the wizard downloads and displays the current system configuration.

```
Configuration confirmation.
===========================================
DNS Server(s) = 172.20.59.46
Allow Data at Rest Encryption = Yes
Customer Support Contact Information = United States:
(800) 446-0744. Outside  the United States: (858) 547-4526
Storage Configuration = internal
Gateway Router IPv4 Address = 172.20.59.254
Encrypt Data at Rest on Primary Storage = No
Time Settings Compliance Mode = No
HCP System Serial Number = 00001
MQE Index-Only Volumes = No
Enable DNS = Yes
Chassis = None
Enable Replication on This System = Yes
Multicast Network = 238.172.59.42
Time Zone = America/New_York
Current Date and Time = None
Domain Name for the System = hcp.example.com
Allow Data in Flight Encryption / SSL = Yes
Blade Servers = No
Distributor/OEM Key Access = Arizona
Time Server(s) = internal
Gateway Router Secondary IPv6 Address = None
Gateway Router IPv6 Address = None
Spindown Volumes = No
HCP Storage Nodes: 1
  172.59.42.5
Configure Dedicated Database Volumes = Yes

Use SHIFT+PGUP to review the Configuration.

Is this Configuration Correct?
[Default: no]: yes
```

6. Review the configuration and take one of the following actions.
   - If the configuration is incorrect:
     a. Enter *n* or *no*.
     b. In response to the confirming prompt, enter *y* or *yes*.
     c. Exit the wizard and contact your HCP support center for help.
   - If the configuration is correct:
     a. Enter enter `y` or `yes`.
     b. In response to the confirming prompt, enter `y` or `yes`.

        HCP Setup performs a set of prechecks.



        If your current HCP system has dedicated database volumes, each newly added node must have at least three volumes. Also, the dedicated database volume size needs to be at least 50 GB. All dedicated database volumes need to be the same size.

     c. Select dedicated database volumes.

1. When prompted, select the dedicated database volume for the first node.

2. Press Enter to confirm your selection.

3. Repeat the previous two substeps for each node in the system.

After you select the dedicated database volumes for each node, HCP Setup confirms your selections. Then the wizard asks if you want to continue the node addition.

```
...
Select dedicated volume for each node.
Found these volumes:
       node 001:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 002:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 003:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 004:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)
Select dedicated database volume for node 001: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 002: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 003: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 004: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Following volumes will be configured as dedicated database volumes:
       node 001: 4. /dev/sde at 2:0:0:4 (1TB)
       node 002: 4. /dev/sde at 2:0:0:4 (1TB)
       node 003: 4. /dev/sde at 2:0:0:4 (1TB)
       node 004: 4. /dev/sde at 2:0:0:4 (1TB)
Do you want to continue? [Default: yes]?
...
```

d. Press Enter to continue the procedure.

- If the prechecks are successful, the HCP software is installed on the new nodes. For RAIN and VM systems, the software is installed on four nodes at a time. For SAIN systems, the software is installed on one cross-mapped pair of nodes at a time.

After the software installation is complete, the nodes are rebooted. When the node addition is complete, the **HCP Configuration** menu redisplays.

- If any of the prechecks fail, HCP Setup exits. In this case, fix the problem and then start the node addition procedure again.
- If HCP Setup exits at any time before the node addition processing is complete, contact your HCP Support Center for help.

7. From the **HCP Configuration** menu, enter **q** to log out of the install shell.
8. In response to the confirming prompt, enter *y* or *yes* to confirm your entry, or *n* or *no* to try again.

Recovering storage nodes

The following sections describes how to recover storage nodes when preserving storage volumes, and how to recover storage nodes when clearing storage volumes. For more information about these and other procedures, refer to the *Installing and Maintaining an HCP System* manual.

Recovering storage nodes and preserving volumes

Procedure

1. From the **HCP Configuration** menu, enter **s** to display the **HCP Service** menu.
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 **HCP Service** menu appears.

```
HCP Service Menu
========================================
[1] Recover an HCP Node
[2] Display the Current System Status
[3] Shut down the HCP System
[4] Free Space on Nodes
[5] Install a Hotfix
[6] Finalize Migration
[7] Change Region Count
[8] Configure Routine Database Maintenance
[9] Configure Time Settings
[10] Migrate Metadata Regions
[11] Perform Node Swap
[s] Perform SSD Maintenance
[m] Manage Database Volumes

[q] Return to Configuration Menu

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

3. From the **HCP Service** menu, enter **1** for recovery operations.

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*, HCP Setup displays the **Node Recovery** menu.

```
HCP Setup:  Node Recovery Menu
==============================================

[1] Recover storage nodes
[2] Recover all storage nodes
[3] Reinitialize internal database

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

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

5. From the **Node Recovery** menu, take one of these actions:

   - To recover selected storage nodes, enter **1**. Then follow the on-screen instructions to identify the nodes you want to recover. Be sure to use the *back-end IP address* to identify each node.

Note: If you choose to use a range of IP addresses to identify the nodes, ensure that the range you specify includes only the nodes you want to recover.

- If you identify fewer than half of the nodes in the HCP system, HCP Setup asks whether you want to delete and then try to rebuild the database on those nodes.

```
 Do you want to delete the database and have HCP try to rebuild it?
 Enter yes only if you know that the database is unrecoverable.  If you
are unsure, enter no.
 [Default: no]:
```

  a. Enter *y* or *yes* to delete the database while recovering the OS or *n* or *no* to recover the OS without deleting the database.

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

  c. Optional: If you are performing the OS recovery on an HCP system with dedicated database volumes, HCP Setup displays the next prompt.

```
Do you want HCP to format the internal database drive before rebuilding it?
If you enter yes, only the internal database drive is formatted.
Enter yes only if you know that the internal database drive needs formatting.
If you are unsure, enter no.
[Default: no]:
```

  - To format only the internal database drive, enter *y* or *yes*.
  - To keep the internal database drive in its original state, enter *n* or *no*.

- If you identify half or more of the nodes in the HCP system, HCP Setup displays a unique key and prompts you to enter it.
- To recover all storage nodes, enter **2**. HCP Setup displays a unique key and prompts you to enter it back.

6. Enter the unique key exactly as it is shown.

HCP Setup performs a series of prechecks and, if they are successful, recovers the OS on the selected nodes or all nodes, as applicable. If any of the prechecks fail, HCP Setup exits. In this case, fix the problem and then start the OS recovery procedure again.

When the node recovery is complete, HCP reboots all the nodes that it recovered and displays this message:

```
>>> HCP Service Procedure successful
Press ENTER to continue:
```

7. If the node that you are logged in to is one of the recovered nodes, the SSH or console session is automatically terminated when HCP reboots the node. If this is not the case, in response to the prompt to continue, press Enter.

   The **HCP Service** menu is displayed.

Important: If HCP Setup exits at any time before the OS recovery processing is complete, contact your HCP Support Center. Do *not* try to recover the OS again.

8. From the **HCP Service** menu, enter **q** to return to the **HCP Configuration** menu.

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

10. From the **HCP Configuration** menu, enter **q** to log out of the install shell.

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

Recovering storage nodes and clearing volumes

Procedure

1. From the **HCP Configuration** menu, enter **s** to display the **HCP Service** menu.

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

   If you enter *y* or *yes*, the **HCP Service** menu is displayed.

```
HCP Service Menu
========================================
[1] Recover an HCP Node
[2] Display the Current System Status
[3] Shut down the HCP System
[4] Free Space on Nodes
[5] Install a Hotfix
[6] Finalize Migration
[7] Change Region Count
[8] Configure Routine Database Maintenance
[9] Configure Time Settings
[10] Migrate Metadata Regions
[11] Perform Node Swap
[s] Perform SSD Maintenance
[m] Manage Database Volumes

[q] Return to Configuration Menu

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

3. Enter **1** for recovery operations.

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

   If you enter *y* or *yes*, HCP Setup displays the **Node Recovery** menu.

```
HCP Setup:  Node Recovery Menu
==============================================

[1] Recover storage nodes
[2] Recover all storage nodes
[3] Reinitialize internal database

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

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

5. From the **Node Recovery** menu, enter **1** to recover selected storage nodes. Then follow the instructions to identify the nodes you want to recover. Be sure to use the *back-end IP address* to identify each node.

Note: If you choose to use a range of IP addresses to identify the nodes, ensure that the range you specify includes only the nodes you want to recover.

6. Optional: If you set FORCE_FORMAT to 1, when you enter *y* or *yes*, HCP Setup displays the **FORCE_FORMAT** prompt.

```
Enabling FORCE_FORMAT will format all disks. Are you sure you want to do this?
[Default: no]:
```

Important: If you receive this prompt, continuing with this procedure formats all disks and erases all data on the targetted node or nodes. The data *cannot* be recovered. Perform this action only if you are sure the data can be deleted.

7. Enter *y* or *yes* to allow the system to format all disks.

   Then follow the on-screen instructions to identify the node containing the logical volumes you want to recover.

   HCP Setup displays a unique key and prompts you to enter it back.

8. Enter the unique key exactly as it is shown.

   After you have entered the unique key, HCP Setup performs a set of prechecks.

```
You chose: "yes", is this correct?
[Default: yes]:
Verifying system name
Verifying run location
Verifying running as install
Verifying node connections
Verifying SSH keys
Verifying SSH
Verifying systemwide SSH
Verifying total memory > 32GB
Verifying all network links
Verifying software versions
Verifying 64-bit hardware platform
Verifying drive size
Verifying disk space
Verifying nobody using /fcfs_*
Verifying nobody using /fs/*
Verifying multicast enabled
Syncing install password to all nodes.
Updating EULA
Syncing timezone to all nodes
Syncing date to all nodes.
Generating auth keys
Generating system UUID
Syncing HCP package to all nodes
Checking to see if we need to run update schemaupgrade scripts False
Updating schema scripts for upgrade.
...
```

9. Conditional: Complete the next substeps only if your current HCP system has dedicated database volumes.

a. When prompted, select the dedicated database volume for the first node.

b. Press Enter to confirm your selection.

c. Repeat the above two steps for each node in the system.

After you have selected the dedicated database volumes for each node, HCP Setup confirms your selections then asks if you want to continue the node recovery.

```
...
Select dedicated volume for each node.
Found these volumes:
       node 001:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 002:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 003:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)

       node 004:
              1. /dev/sdd at 2:0:0:1 (500GB)
              2. /dev/sde at 2:0:0:2 (500GB)
              3. /dev/sdd at 2:0:0:3 (500GB)
              4. /dev/sde at 2:0:0:4 (1TB)
Select dedicated database volume for node 001: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 002: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 003: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Select dedicated database volume for node 004: 4
You chose: "4. /dev/sde at 2:0:0:4 (1TB)", is this correct? [Default: yes]:
Following volumes will be configured as dedicated database volumes:
       node 001: 4. /dev/sde at 2:0:0:4 (1TB)
       node 002: 4. /dev/sde at 2:0:0:4 (1TB)
       node 003: 4. /dev/sde at 2:0:0:4 (1TB)
       node 004: 4. /dev/sde at 2:0:0:4 (1TB)
Do you want to continue? [Default: yes]?
...
```

10. Press Enter to continue the procedure.

If the prechecks are successful, HCP Setup recovers all the logical volumes on the selected nodes or all nodes, as applicable. If any of the prechecks fail, HCP Setup exits. In this case, fix the problem and then start the node recovery procedure again.

When the node recovery is complete, the **HCP Service** menu is displayed.

Important: If HCP Setup exits before the node recovery processing is complete, contact your HCP Support Center Do *not* try the node recovery again.

11. From the **HCP Service** menu, enter **q** to return to the **HCP Configuration** menu.

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

13. From the **HCP Configuration** menu, enter **q** to log out of the install shell.

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

Adding a management port network

Procedure

1. On each node in the vSphere cluster, configure a network to be used as a management port network. See "Configuring networking" on page 24 for details.

2. Perform the following steps on each virtual machine in the HCP VM cluster:

   a. From the vSphere web client, select the HCP virtual machine.

   b. Click the **Configure** tab.

   c. Click **Edit**.

   d. In the **New device** dropdown menu, select **Network** then click **Add**.

   e. When the new network device appears, select **Management Port Network**.

   f. Click **OK**.

3. Configure the management port network from the System Management Console. See the HCP System Management Help for details.

6

Configuring HCP monitoring with Hitachi Remote Ops

Hitachi Remote Ops is a Hitachi Vantara product that enables remote monitoring of the nodes in an HCP VM system. This chapter assumes that Hitachi Remote Ops is installed and running according to the product documentation.

With Hitachi Remote Ops, you can view the status of nodes in an HCP VM system with a web browser. You can also configure Hitachi Remote Ops to send email notifications of error conditions as they occur. Additionally, you can configure Hitachi Remote Ops to report error conditions to Hitachi Vantara Support personnel.

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

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

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

Enabling SNMP in HCP

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

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

Procedure

1. Log in to the HCP System Management Console using the initial user account, which has the security role.
2. In the top-level menu of the Console, select **Monitoring ► SNMP**.
3. In the **SNMP Settings** section on the **SNMP** page:
   - Select the **Enable SNMP at snmp.***hcp-domain-name* option.
   - Select either **Use version 1 or 2c** (recommended) or **Use version 3**.

     If you select **Use version 3**, specify a username and password in the **Username**, **Password**, and **Confirm Password** fields.
   - Optional: In the **Community** field, type a different community name.
4. Click **Update Settings**.
5. In the entry field in the **Allow** section, type the IP address that you want HCP to use to connect to the server where Hitachi Remote Ops is installed. Then click **Add**.
6. Log out of the System Management Console, and close the browser window.

Configuring Hitachi Remote Ops

To configure Hitachi Remote Ops to monitor the nodes in the HCP system, follow the steps outlined in the next table.

Step	Activity	More information
1	Log into Hitachi Remote Ops.	Step 1: "Log in to Hitachi Remote Ops" on the facing page

Step	Activity	More information
2	Set the Hitachi Remote Ops base configuration, including the email addresses to which email about error conditions should be sent.	Step 2: "Set the base configuration" below
3	Optional: Configure transport agents for reporting error conditions to Hitachi Vantara support personnel.	Step 3: " (Conditional) Configure transport agents" on page 81
4	Identify the HCP system to be monitored.	Step 4: "Identify the HCP system" on page 81

Step 1: Log in to Hitachi Remote Ops

Procedure

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

   http://hitrack:6696

3. In the **Select one of the following UserIds** field, select **Administrator**.
4. In the **Enter the corresponding password** field, type the case-sensitive password for the Administrator user. By default, this password is *hds*.

   If Hitachi Remote Ops is already in use at your site for monitoring other devices, this password may have been changed. In this case, see your Hitachi Remote Ops administrator for the current password.

5. Click **Logon**.

Step 2: Set the base configuration

The Hitachi Remote Ops base configuration specifies information including the customer site ID, how frequently to scan devices, whether to report communication errors that occur between Hitachi Remote Ops and monitored devices, and the email addresses to send the error condition alerts to.

If Hitachi Remote Ops is already used at your site, the base configuration might already be set up. You can leave the configuration as is, or you can update it to accommodate additional HCP devices.

Procedure

1. In the row of tabs at the top of the Hitachi Remote Ops interface, click **Configuration**.

   The **Base** page is displayed.

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

   - In the **Site ID** field, type your Hitachi Vantara customer ID. If you do not know your customer ID, contact your authorized HCP service provider.
   - Optional: Update the field values to meet your site needs. For information about these fields, click **Help on this table's entries**.

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

   - In the **eMail Server** field, type the fully qualified hostname or a valid IP address of the email server through which you want Hitachi Remote Ops to send email about error conditions.
   - In the **Local Interface** field, select the Ethernet interface that has connectivity to the specified email server. This is the interface on the Hitachi Remote Ops server.
   - In the **User List** field, type a comma-separated list of the email addresses to which Hitachi Remote Ops should send email about error conditions.
   - In the **Sender's Email Address** field, type an email address to be used in the From line of each email.

     Some email servers require that the value in the **From** line be an email address that is already known to the server.

4. Click **Submit**.

5. Optional: To send a test email to the specified email addresses, click **Test Email**.

Step 3: (Conditional) Configure transport agents

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

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

Procedure

1. In the row of tabs below **Configuration**, click **Transport Agents**.
2. In the field below **Data Transfer Agents**, select the transfer method for the new transport agent.
3. Click **Create**.

   The new agent is displayed in the list of transport agents. A set of configuration fields is displayed below the list.
4. In the configuration fields, specify the applicable values for the new transport agent. For information about what to specify, see the Hitachi Remote Ops documentation.
5. Click **Submit**.

Step 4: Identify the HCP system

Procedure

1. In the row of tabs at the top of the Hitachi Remote Ops interface, click **Summary**.

   The **Summary** page displays up to four tables (device errors, communication errors, devices ok, and not monitored) that categorize the devices known to Hitachi Remote Ops.

   To show or hide these tables, toggle the check boxes below the table names at the top of the page and click **Refresh**.
2. Take one of these actions:

   - If the **Summary** page does not display any tables, an **Add a device** link is displayed. Click this link.

- If the **Summary** page displays one or more tables, click the **Item** column heading in any of the tables.

3. In the **Select Device Type** field, select **Hitachi Content Platform (HCP)**.

   A set of configuration fields is displayed.

4. In the **Name** field, type a name for the HCP system. The name is typically the system host name. The name can be from one to 40 characters long. Special characters and spaces are allowed.

5. In the **Location** field, type the location of the HCP system. The location can be from one to 40 characters long. Special characters and spaces are allowed.

6. In the **Group** field, type the name of a group associated with the HCP system. The group name can be from one to 40 characters long. Special characters and spaces are allowed. For example, Finance Department.

7. In the **Site ID** field, type your Hitachi Vantara customer ID. If you do not know your customer ID, contact your authorized HCP service provider.

8. In the **IP Address or Name (1)** field, type a valid front-end IP address for the lowest-numbered storage node in the HCP system.

9. In the **Local Interface** field, leave the value as **-any-**.

10. In the **IP Address or Name (2)** field, type a valid front-end IP address for the highest-numbered storage node in the HCP system.

11. In the **Local Interface** field, leave the value as **-any-**.

12. In the **SNMP Access ID** field, select the SNMP user that corresponds to the SNMP configuration in HCP. Typically, this is **public**.

13. In the **Comms Error Reporting** field, specify whether Hitachi Remote Ops should report communication errors between Hitachi Remote Ops and the HCP system. Values are:

    - **Yes** — Report communication errors.
    - **No** — Do not report communication errors.

- **Local** — Report communication errors only to the email addresses specified in the base configuration, not through the specified transport agents.
- **Default** — Use the setting in the base configuration.

12. Ensure that **Enabled** is selected.
13. Ensure that **Trace** is cleared.
14. Click **Add**.

When the operation is successful, a message is displayed indicating that the HCP system has been added.

Important: Do not click **Add** again. Doing so will add the system a second time.

Changing the HCP VM network adapters

This appendix describes how to change the supported network adapters on your HCP VMs.

About network adapters

Starting in HCP v7.2.1, all newly installed HCP VMs are automatically configured to use VMXNET3 adapters.

If you are upgrading from a previous HCP release, your configuration might include e1000 adapters. It is recommended that you update your ESXi configuration to use VMXNET3 adapters because HCP support for e1000 adapters is deprecated.

VMXNET3 adapters support both one- and 10-gigabit network configurations, whereas e1000 adapters support only one-gigabit network configurations.

VMXNET3 adapters are recommended in all new and upgraded configurations .

Disabling LRO on the ESXi host for VMXNET3

If you want to switch your HCP VMs to use the VMXNET3 network adapter, you need to disable large receive offload (LRO) in the guest operating system to prevent potential TCP performance degradation.

Procedure

1. Log in to the vSphere Client.
2. Click a server that hosts ESXi for your HCP VMs.

3. Click the **Configure** tab.

4. In the **System** menu, click **Advanced System Settings**.

5. In the inventory tree, click **Edit**.

6. Scroll down to the following parameters and change their parameter field from `1` to `0`.

   Net.Vmxnet2HwLRO
   Net.Vmxnet2SwLRO
   Net.Vmxnet3HwLRO
   Net.Vmxnet3SwLRO
   Net.VmxnetSwLROSL

7. Click **OK**.

8. From the vSphere client, reboot the server by right-clicking it and selecting **Reboot**.

Changing the HCP VM network adapter

You can configure an HCP VM to use VMXNET3 by removing the existing e1000 network adapter and replacing it with VMXNET3.

Step 1: Power off the HCP VM

Procedure

1. Open the VMware vSphere Client.

2. Right-click the HCP VM for which you want to replace the network adapters, hover over **Power**, and click **Shut Down Guest OS**.

Step 2: Remove the previous network adapters

Procedure

1. From the vSphere Client, right-click one of the powered-off HCP VMs.

2. Click **Edit Settings**.

   The Virtual Machine Properties window is displayed. The number of existing network adapters varies depending on whether the HCP VM is using e1000 or VMXNET3.

   - If the HCP VM is using e1000, remove four network adapters.

- If the HCP VM is using VMXNET3, remove two network adapters.

3. Click the **Virtual Hardware** tab.
4. Select a network adapter and click **Remove**.
5. Repeat Step 4 until all the network adapters are removed.
6. Click **OK**.

Step 3: Configure the front-end network adapters

Before you begin

If you are using the VMXNET3 adapter, the first VMXNET3 adapter must be connected to the front-end network, and the second VMXNET3 adapter must be connected to the back-end network.

Procedure

1. From the vSphere Client, right-click one of the powered-off HCP VMs and click **Edit Settings**.

   The **Virtual Machine Properties** window is displayed.

2. On the **Hardware** tab, click **Add**.

   The **Add Hardware** window opens.

3. Select **Ethernet Adapter** and click **Next**.
4. On the **Network Connection** page, in the **Adapter Type** pane, click the **Type** list and select **VMXNET3**.
5. In the **Network connection** pane, select **Named network with specified label**.
6. Select **Front-End Network** and click **Next**.
7. On the **Verification** page, click **Finish**.
8. Back on the **Virtual Machine Properties** window, click **OK**.

Step 4: Configure the back-end network adapters

Before you begin
The first VMXNET3 network adapter must be connected to the front-end network, and the second VMXNET3 network adapter must be connected to the back-end network.

Procedure

1. From the vSphere Client, right-click the powered-off HCP VM and click **Edit Settings**.

   The **Virtual Machine Properties** window is displayed.

2. In the **Edit Settings** window, **Hardware** tab, click **Add**.

   The **Add Hardware** window opens.

3. Select **Ethernet Adapter** and click **Next**.

4. On the **Network Connection** page, in the **Adapter Type** pane, click the **Type** list and select **VMXNET3**.

5. In the **Network connection** panel, select **Named network with specified label**.

6. Select **Back-End Network** and click **Next**.

7. On the **Verification** page, click **Finish**.

8. Back on the **Virtual Machine Properties** window, click **OK**.

Step 5: Power on the HCP VM

Procedure
From your vSphere Client, right-click the newly configured HCP VM, hover your cursor over **Power**, and click **Power On**.

Result
Once the HCP VM is powered on, you have successfully changed its network adapters. If you have multiple HCP VM nodes that require reconfiguring, repeat the instructions for each one.

B

Modifying the DRS settings

Procedure

1. Open the vSphere Client.
2. On the left navigation bar, select the datacenter.
3. In the right pane, click the **Getting Started** tab.
4. Click **Create a cluster**.
5. In the VMware Cluster Wizard, select **Turn On vSphere HA** and **Turn On vSphere DRS**.

Important: Enable this feature only if you fully understand its functionality.

6. Click **OK**.
7. For **DRS automation level**, select **Manual** to specify where VM guests should reside.
8. For **Power management**, select **Off**.
9. Select **Enable Host Monitoring** and keep the default settings.
10. Set **VM Monitoring** to **Disabled**.
11. Select **Disable EVC**.
12. Select where you want to store your `swapfile` location.
13. Review your settings. Then click **OK**.
14. On the left-navigation bar, right-click a cluster and click **Edit Settings**.

15. In the **Settings** window, on the left navigation bar, click **DRS Groups Manager**.

16. Create a group and add the virtual machines that you want to keep on the server.

17. Create one virtual machine DRS group for each host.

18. In the **Host DRS Groups** section, click **Add** and place one host from the cluster in each group. Then click **Next**.

19. In the **Settings** window, on the left navigation bar, click **Rules**.

20. Create a new rule to match each VM group to a host group, and set the rule type to **Virtual Machines to Hosts**.

21. Select **Should run on hosts in group** and click **OK**.

    This setting creates a rule that lets VMs run on other hosts in the cluster in the event of a failure.

Important: If you select **Must Run on Hosts in Group**, HA will not start the server on another host in the cluster, which defeats the purpose of HA.

22. Set an alarm to alert you if a failure occurs.

    a. Right-click the cluster and click **Alarm > Add Alarm**.

    b. In the **Alarm Settings** window, name your alarm and set **Monitor** to **Virtual Machines**.

    c. Select **Monitor for specific event occurring on this object**.

    d. Click the **Triggers** tab.

    e. Select **VM is violating a DRS VM Host affinity rule**.

    f. Set the status to either **Warning** or **Alert**.

    g. In the **Trigger Conditions** section, from the **Argument of VM** list, select a name.

    h. Set the value to each VM you want to monitor.

    i. Add one argument for each VM.

j. Set the actions you want the system to take.

C

Configuring the HCP VM small instance

If you are deploying an HCP VM system as a small-instance system, you must change the CPU count and RAM for each node before powering on the HCP VM nodes.

Procedure

1. In vSphere Client, right-click the HCP VM node and click **Edit Settings**.
2. In the **Virtual Machine Properties** window, select the **Hardware** tab .
3. From the **Hardware** list, select **Memory** and in the **Memory Configuration** pane, adjust the allocation to 16 GB.
4. From the **Hardware** list, select **CPUs** and adjust the **Number of virtual sockets** and **Number of core per sockets** so that the **Total number of cores** equals 4.
5. Click **OK**.

   The **Virtual Machine Properties** window closes.

D

Managing failover

The HCP VM vSphere HA cluster does not automatically move a failed-over HCP VM node back to its original ESXi host once the host is available. Instead, the HCP VM system administrator must manually shutdown the HCP VM nodes that need to be moved to another ESXi host.

Alternatively, the vCenter administrator can shut down the HCP VM nodes from the vCenter management console. Then, the administrator can manually move the HCP VM nodes onto the preferred ESXi host and power on the nodes. Once an HCP VM node boots, it will re-join the HCP VM system.

After powering down an HCP VM node and attempting to move the VM to another ESXi host, an error message might display. You can ignore the message.

Glossary

A

access control list (ACL)

Optional metadata consisting of a set of grants of permissions to perform various operations on an object. Permissions can be granted to individual users or to groups of users.

ACLs are provided by users or applications and are specified as either XML or JSON in an XML request body or as request headers.

ACL

See access control list (ACL).

Active Directory (AD)

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

AD

See Active Directory (AD).

alert

A graphic that indicates the status of some particular element of an HCP system in the System or Tenant Management Console.

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, 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.

custom metadata

User-supplied information about an HCP object. Custom metadata is specified as one or more annotations, where each annotation is a discrete unit of information about the object. Users and applications can use custom metadata to understand repurpose object content.

D

database

An internal component of an HCP VM system that contains essential data about the system, users, and user's files. The database is maintained by one node and copied to the other.

data center

In VMware vSphere, a logical unit for grouping and managing hosts.

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.

datastore

A representation of a location in which a virtual machine stores files. A datastore can represent a location on a host or an external storage location such as a SAN LUN.

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.

DNS

See domain name system.

DPL

See data protection level (DPL).

E

ESXi

See "VMware ESXi".

H

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 various HCP-specific interfaces to access and manipulate objects in an HCP repository.

HCP VM system

An HCP VM in which the nodes are virtual machines running in a KVM or VMware vSphere environment.

HDDS

See "Hitachi Data Discovery Suite (HDDS)"

Hitachi Data Discovery Suite (HDDS)

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

host

A physical computer on which virtual machines are installed and run.

L

logical unit number (LUN)

A number used to identify a logical unit, which is a device addressed by the Fibre Channel.

logical volume

A logical unit of storage that maps to the physical storage managed by a node. The physical storage can be storage that's managed by HCP or storage on an external NFS device.

LUN

See "logical unit number (LUN)".

M

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.

multipathing

In SAIN systems, multiple means of access to a logical volume from a single node.

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.

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.

network file system

One of the namespace access protocols supported by HCP. NFS lets clients access files on a remote computer as if the files were part of the local file system.

network interface controller (NIC)

A hardware interface that connects the computer to its appropriate network. NICs can be physical (pNIC) or virtual (vNIC).

NFS

See network file system.

NIC

See "network interface controller (NIC)".

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.

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.

pNIC

See "network interface controller (NIC)".

Q

query

A request submitted to HCP to return metadata for objects or operation records that satisfy a specified set of criteria. Also, to submit such a request.

R

RAIN

See redundant array of independant nodes (RAIN).

redundant array of independant nodes (RAIN)

An HCP system configuration in which the nodes use internal or direct-attached storage.

replication

A process by which selected tenants and namespaces are maintained on two or more HCP systems and the objects in those namespaces are managed across those systems. Typically, the systems involved are in separate geographic locations and are connected by a high-speed wide area network. This arrangement provides geographically distributed data protection (called **geo-protection**).

repository

The aggregate of the namespaces defined for an HCP system.

running storage

Storage on continuously spinning disks.

S

SAIN

See "SAN-attached array of independent nodes (SAIN)".

SAN-attached array of independent nodes (SAIN)

An HCP system configuration in which the nodes use SAN-attached storage.

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.

secure shell

A network protocol that lets you log into and execute commands in a remote computer. SSH uses encrypted keys for computer and user authentication.

secure sockets layer

Secure Sockets Layer. A key-based Internet protocol for transmitting documents through an encrypted link.

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.

service plan

A named specification of an HCP service behavior that determines how HCP manages objects in a namespace. Service plans enable you to tailor service activity to specific namespace usage patterns or properties.

simple network management protocol (SNMP)

A protocol HCP uses to facilitate monitoring and management of the system through an external interface.

SNMP

See "simple network management protocol (SNMP)".

SNMP trap

A type of event for which each occurrence causes SNMP to send notification to specified IP addresses. SNMP traps are set in management information base (MIB) files.

spin-down storage

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

SSH

See "secure shell".

SSL

See secure sockets layer.

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.

switch

A device used on a computer network to connect devices together.

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

tag

An arbitrary text string associated with an HCP tenant or namespace. Tags can be used to group tenants or namespaces and to filter tenants or namespace lists.

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.

transaction log

A record of all create, delete, purge, and disposition operations performed on objects in any namespace over a configurable length of time ending with the current time. Each operation is represented by an operation record.

U

unix

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

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 following interfaces: HCP System Management Console, HCP Tenant

Management Console, HCP management API, HCP Search Console, namespace content through the namespace access protocols, HCP metadata query API, and HCP Data Migrator.

user authentication

The process of checking that the combination of a specified username and password is valid when a user tries to log into the System Management Console, Tenant Management Console, HCP Search Console, tries to access the HCP system through the management API, or tries to access a namespace.

V

vCenter

See "VMware vCenter Server".

versioning

An optional namespace feature that enables the creation and management of multiple versions of an object.

virtual local area network (VLAN)

A distinct broadcast domain that includes devices within different segments of a physical network.

virtual machine

A piece of software that emulates the functionality of a physical computer.

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.

vmNIC

A representation in VMware vSphere of one of the physical NICs on a host.

VMware ESXi

The underlying operating system for the VMware vSphere product.

VMware vCenter Server

A VMware product that allows you to manage multiple ESXi hosts and the virtual machines that they run.

vNIC

See "network interface controller (NIC)".

Z

zero-copy failover

The process of one node automatically taking over management of storage previously managed by another node that has become unavailable.

Index

T

V

Hitachi Vantara

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

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