Redbooks
ibm.com/redbooks

IBM Power Systems HMC Implementation and Usage Guide

Sylvain Delabarre

Sorin Hanganu

Thomas Libor, PhD

Cloud

Power Systems

IBM

Redbooks

International Technical Support Organization

IBM Power Systems HMC Implementation and Usage Guide

April 2016

SG24-8334-00

Note: Before using this information and the product it supports, read the information in “Notices” on page xi.

First Edition (April 2016)

This edition applies to Version 8, Release 8, Modification 4 of the Hardware Management Console (program number 5765-MHV).

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Active Memory™
AIX®
AIX 5L™
developerWorks®
Electronic Service Agent™
Enterprise Workload Manager™
GPFS™
HACMP™
i5/OS™
IBM®
IBM Flex System®
Lotus®
Micro-Partitioning®
POWER®
Power Systems™
POWER6®
POWER6+™
POWER7®
POWER7 Systems™
POWER7+™
POWER8®
PowerHA®
PowerLinux™
PowerVM®
Rational®
Redbooks®
Redpaper™
Redbooks (logo) ®
System i®
SystemMirror®
Tivoli®
WebSphere®

The following terms are trademarks of other companies:

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

ITIL is a Registered Trade Mark of AXELOS Limited.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.

TOC
Redbooks
Creating Hybrid Clouds with IBM Bluemix Integration Services
Cloud
Analytics
IBM.
Solution Guide

Find and read thousands of IBM Redbooks publications

- Search, bookmark, save and organize favorites
- Get personalized notifications of new content
- Link to the latest Redbooks blogs and videos

Get the latest version of the Redbooks Mobile App

iOS **Download Now** Android

Promote your business in an IBM Redbooks publication

Place a Sponsorship Promotion in an IBM® Redbooks® publication, featuring your business or solution with a link to your web site.

Qualified IBM Business Partners may place a full page promotion in the most popular Redbooks publications. Imagine the power of being seen by users who download millions of Redbooks publications each year!

ibm.com/Redbooks
About Redbooks → Business Partner Programs

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

The IBM® Hardware Management Console (HMC) provides to systems administrators a tool for planning, deploying, and managing IBM Power Systems™ servers. This IBM Redbooks® publication is an extension of *IBM Power Systems HMC Implementation and Usage Guide*, SG24-7491 and also merges updated information from *IBM Power Systems Hardware Management Console: Version 8 Release 8.1.0 Enhancements*, SG24-8232. It explains the new features of IBM Power Systems Hardware Management Console Version V8.8.1.0 through V8.8.4.0. The major functions that the HMC provides are Power Systems server hardware management and virtualization (partition) management.

Further information about virtualization management is in the following publications:

- *IBM PowerVM Virtualization Managing and Monitoring*, SG24-7590
- *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940
- *IBM PowerVM Enhancements What is New in 2013*, SG24-8198
- *IBM Power Systems SR-IOV: Technical Overview and Introduction*, REDP-5065

The following features of HMC V8.8.1.0 through HMC V8.8.4.0 are described in this book:

- HMC V8.8.1.0 enhancements
- HMC V8.8.4.0 enhancements
- System and Partition Templates
- HMC and IBM PowerVM® Simplification Enhancement
- Manage Partition Enhancement
- Performance and Capacity Monitoring
- HMC V8.8.4.0 upgrade changes

Authors

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Sylvain Delabarre is a Certified IT Specialist at the IBM Client Center in Montpellier, France. He has been with IBM France since 1988. He works as a Power Systems Benchmark Specialist since 2010. He also has more than 20 years of IBM AIX® System Administration and Power Systems experience, working in service delivery, AIX, Virtual I/O Server, and HMC support for EMEA. He is a Red Hat Certified System Administrator.

Sorin Hanganu is an Accredited Product Service professional. He has more than ten years of experience working on Power Systems and IBM i products. He is an IBM Certified Solution Expert for IBM Dynamic Infrastructure and also an IBM Certified Systems Expert for Power Systems, AIX, PowerVM virtualization, IT Infrastructure Library (ITIL), and IT service management (ITSM). He works as a System Services Representative for Power Systems in Bucharest, Romania.

Thomas Libor, PhD is an IT Specialist with IBM Germany. He has 14 years of experience in Power Systems and AIX. He is an IBM Certified Advanced Technical Expert for Power Systems with AIX. His areas of expertise include virtualization, high availability, IBM Storage, Linux, and networking. He holds a PhD in chemistry from the Philipps-University in Marburg, Germany.

The project that produced this publication was managed by:
Scott Vetter, PMP

Thanks to the following people for their contributions to this project:

Dave Bennin, Ella Buslovich, Richard M. Conway
International Technical Support Organization, Poughkeepsie Center

Shamsundar Ashok, Moises D Carrillo, Chet Mehta, Amartey Pearson
IBM Systems in Austin, TX

Alex Rodriguez
IBM Security in Costa Mesa, CA

Thanks to the authors of the previous editions of this book and white paper:

- *IBM Power Systems HMC Implementation and Usage Guide*, SG-24-7491, published in April 2013:

  Attha Surya Dharma, Mark Hais, Minsung Kang, Scott Vetter, and Yuta Wakayama

- *IBM Power Systems Hardware Management Console: Version 8 Release 8.1.0 Enhancements*, SG24-8232, published in October 2014:

  Steve Biggs, Guillermo Corti, Craig Hunt, and Indra Suyatama

- *IBM Hardware Management Console Best Practices*, published in January 2007:

  Ron Barker, Minh Nguyen, and Shamsundar Ashok

  Find the white paper at the following location:

  `https://ibm.biz/Bd4miU`

Now you can become a published author, too!

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Hardware Management Console overview

This chapter provides an overview of the Hardware Management Console (HMC) and the HMC V8 enhancements through Release 8.4.0.

This chapter describes the following topics:

- Overview of Hardware Management Console (HMC)
- Enhancements in HMC Version 8
- Hardware Models

1.1 Overview of Hardware Management Console (HMC)

The HMC is an appliance for planning, deploying, and managing IBM Power Systems servers. It can be used to create and modify logical partitions, including dynamically adding and removing resources from a running partition. This section briefly describes some of the concepts and functions of the HMC and introduces the user interface that is used for accessing those functions.

1.1.1 Introduction to the Hardware Management Console

The HMC allows you to configure and manage servers. One HMC can manage multiple servers, and dual HMCs can provide redundant support by managing the same system. To ensure consistent function, each HMC is preinstalled with the HMC Licensed Machine Code.

Note: Virtualization is not supported on the IBM Power System S824L (8247-42L) server.

To provide flexibility and availability, you can implement HMCs in several configurations.

Local HMC

A local HMC is an HMC that is physically located close to the system it manages and is connected by either a private or public network. An HMC in a private network is a DHCP server for the service processors of the systems it manages. An HMC may also manage a system over an open network, where the managed system's service processor IP address has been assigned manually using the Advanced System Management Interface (ASMI).

Physical proximity

Prior to HMC version 7, at least one local HMC was required to be physically located near the managed systems. This is not a requirement with the Version 7 and the HMC's web browser interface.

Remote HMC

A remote HMC is an HMC that is not physically located near its managed systems. This could be in another part of the same room or data center, in another building, or even on another site. Typically, a remote HMC is attached to its managed servers using a public network, but configurations with a remote HMC attached to a private network are also possible. Prior to HMC version 7, at least one local HMC was required. With Version 8, any or all HMCs may be virtual HMC (vHMC).

Redundant HMC

The HMC allows you to configure and manage servers. One HMC can manage multiple servers, and dual HMCs can provide redundant support by managing the same system. To help ensure consistent function, each HMC is preinstalled with the Hardware Management Console Licensed Machine Code.

The IBM Power Systems HMC virtual appliance can be used to manage any of the systems that are supported by the Version 8 HMC, which includes Power Systems servers with IBM POWER6®, POWER7®, and POWER8® processors.

The Power Systems vHMC offers these benefits:

- Provides hardware, service, and basic virtualization management for your Power Systems servers.
- Offers the same functionality as the traditional HMC.
- Runs as a virtual machine on an x86 server virtualized either by VMware ESXi or Red Hat KVM.

When the server is connected to the higher version of the management console, the partition configuration is upgraded to the latest version. After the partition configuration upgrade, lower levels of the management consoles will not be able to interpret the data correctly.

After the server is managed by the higher version of the management console, you must first initialize the server before you can go back to the lower version of the management console. You can restore a backup that is taken at the older level or re-create the partitions.

If the server is not initialized, one of the following outcomes can occur depending on the version of the lower-level HMC:

- HMC Version 8 Release 8.4.0 and later reports a connection error of Version mismatch with reference code Save Area Version Mismatch.
- HMC Version 8 Release 8.3.0 and earlier might report a server state of Incomplete or Recovery. In addition, partition configuration corruption can also occur.

Predefined user IDs and passwords

Predefined user IDs and passwords are included with the HMC. An imperative step to your system's security is that you change the hscroot predefined password immediately. The user IDs and passwords are case-sensitive.

Table 1-1 shows predefined user IDs and passwords that are included with the HMC.

Table 1-1 Predefined HMC user IDs and passwords

User ID	Password	Purpose
hscroot	abc123	The hscroot user ID and password are used to log in to the HMC for the first time.
root	passw0rd	The root user ID and password are used by the service provider to perform maintenance procedures. They cannot be used to log in to the HMC.

1.1.2 What's new in Managing the HMC through the HMC Enhanced+ interface

Read about new or significantly changed information in the topic "What's new in Managing the HMC through the HMC Enhanced+ interface" since the previous update of the topic collection described in this section:

https://www.ibm.com/support/knowledgecenter/8247-22L/p8eh6/p8eh6_whatsnew.htm?cp=8247-22L&lang=en

October 2015

This update added the following topics:

- SR-IOV Firmware Update
- Test Network Connectivity
- View Network Topology
- Update the Hardware Management Console
- OS and VIOS Images
- Adding, Copying, or Modifying User Profiles
- Updated the Templates and OS Images topic

June 2015

This update added the following topics:

- The procedures and functions of the HMC Enhanced + Tech Preview (Pre-GA) interface, which was an option that was provided with HMC Version 8.2.0, are the same as the HMC Enhanced+ interface that is provided with HMC Version 8.3.0. Only the HMC Enhanced+ is referred to in the documentation, but that content also applies to the HMC Enhanced + Tech Preview (Pre-GA) interface.
- The functions of the HMC Enhanced interface, which was an option that was provided with HMC Version 8.1.0, or later, are now available as a part of the HMC Enhanced+ interface that is provided with HMC Version 8.3.0.
- Added the User Properties and Session handling topics.
- Updated the Power Management topic.

November 2014

This update added the following topic:

- Added information about the HMC Enhanced + Tech Preview (Pre-GA) interface for HMC Version 8, Release 2, or later on IBM Power Systems servers that contain the POWER8 processor.

1.1.3 Functionality improvements

The following new and improved functions are made available:

- Improved virtualization user experience starting with HMC V8.2.0.
- Enhanced and simplified HMC management of PowerVM virtualization enables automation and helps simplify the setup and operation of PowerVM.
- Improved no-touch Virtual I/O Server (VIOS) virtualization management enables complete virtualization administration from HMC.
- Delivers one-touch VIOS deployment that enables VIOS images to be deployed from HMC to help simplify the setup of I/O virtualization and PowerVM.
- Has system and partition templates that enable site-specific virtual machine configurations to be consistently deployed and can be used to enforce virtualization best practices for various configurations.
- Includes simplified Remote Restart, removing need for storage area network (SAN/LUNs).
- Contains operating system-level shutdown for IBM i partitions, providing parity with existing support for VIOS, IBM AIX and Linux.
- Has technology preview of the concurrent activation and network install graphical user interface for partition operating system.

- Has technology preview for new User Interface capabilities such as quick search, gallery views, graphical topology, and improved resource views.
- Delivers enhanced manual and automatic First Failure Data Capture (FFDC) on Live Partition Mobility (LPM) abort.
- Includes, with HMC V8.2, IBM POWER8 Enterprise hardware support.

Note: The virtualization improvements implemented by the HMC require HMC V8.2. This function is already available in HMC V8.10 SP1.

PowerKVM V2.1.1 contains additional support for new Linux distributions, additional I/O support, and availability improvements.

Enhancements

Major enhancements include the following items:

- Peripheral Component Interconnect (PCI) pass-through I/O support allows more options for performance.
- Mixed Endian virtual machine support on a single PowerKVM host provides increased flexibility.
- PCI hot plug support provides expanded availability by allowing new devices to be added dynamically.
- Support for SUSE Linux Enterprise Server 12 and Ubuntu 14.10 provides a larger choice of Linux versions.

Hardware

Hardware support was enhanced with the following items:

- x86 64-bit hardware with hardware virtualization assists (Intel VT-x or AMD-V).
- Resources for the HMC virtual appliance VM: four CPUs, eight GB of memory, 160 GB of disk space, and two network interfaces.
- IBM Power Systems HMC virtual appliance is included as part of all Pure Power Primary Manager Node Indicator 8374-01M feature EHKZ orders.

Software

Software support includes the following item:

- Virtualization: Either VMware ESXi V5 or Red Hat Enterprise Linux 6.x with KVM

Unsupported functions

The following items are not supported by the HMC:

- Format media
- Call Home with a modem
- Call Home of HMC hardware failures

Note: HMC Version 8 no longer supports POWER5.

New vHMC functions

The vHMC introduces the following functions:

- Activation engine, which provides configuration on the first boot
- Accept license, locale, network (DHCP not supported), Secure Shell (SSH), and Network Time Protocol (NTP)
- Allow second virtual disk multiple for `/data`

The HMC virtual appliance has several differences from the hardware appliance HMC:

- An activation engine allows unique configuration during initial deployment. Differences exist in the way the license acceptance dialog is presented. Support exists for multiple virtual disks for additional data storage. Format of physical media is not supported, but this is supported through a virtual device attached to the virtual machine (VM).
- Since the hardware and server virtualization is supplied by the client to run the HMC virtual appliance, this infrastructure that actually hosts the HMC virtual appliance is not monitored by IBM. The HMC virtual appliance does continue to monitor the Power Systems hardware just like the HMC hardware appliance. Both HMC form factors provide remote notification of system errors for the managed Power Systems servers.
- Any software maintenance that is required for the HMC virtual appliance is done using the same procedure as is currently performed using fix central with the hardware-based HMC. Further information about the HMC maintenance strategy is at the following web page:

  https://www-304.ibm.com/webapp/set2/sas/f/power5cm/home.html

1.1.4 Major functions of the Hardware Management Console

With the HMC, a system administrator can do logical partitioning functions, service functions, and various system management functions by using either the web-browser-based user interface or the command-line interface (CLI). The HMC uses its connection to one or more systems (referred to in this book as *managed systems*) to do various functions:

- Creating and maintaining logical partitions in a managed system

  The HMC controls logical partitions in managed systems. These tasks are explained in 5.6, “Partition management” on page 370.
- Displaying managed system resources and status

  These tasks are explained in 5.5, “Systems Management for Servers” on page 340.
- Opening a virtual terminal for each partition

  The HMC provides virtual terminal emulation for AIX and Linux logical partitions and virtual 5250 console emulation for IBM i logical partitions.
- Displaying virtual operator panel values for each partition

  You can see the operator panel messages for all partitions within managed systems in HMC.
- Powering the managed systems on and off

  These tasks are explained in Chapter 5, “Operating” on page 291.
- Performing dynamic logical partition (DLPAR) operation

  With the HMC, you can do DLPAR operations that change the resource allocation (such as processor, memory, physical I/O, and virtual I/O) dynamically for the specified partition. These tasks are explained in 5.7, “Dynamic partitioning” on page 376.

- Managing Capacity on Demand operation

  These tasks are explained in 5.11, “Capacity on Demand (CoD)” on page 405.

- Managing virtualization features

  These tasks are explained in “PowerVM” on page 365.

- Managing platform firmware installation and upgrade

  These tasks are explained in 6.9.6, “Managed system firmware updates” on page 467.

- Acting as a service focal point

  You can use the HMC as a service focal point for service representatives to determine an appropriate service strategy and to enable the service agent to call home to IBM. These tasks are explained in 6.3, “Serviceability” on page 425.

HMC Version 8 uses a web-browser-based user interface. This interface uses a tree-style navigation model that provides hierarchical views of system resources and tasks by using drill-down and launch-in-context techniques to enable direct access to hardware resources and task management capabilities. This version provides views of system resources and provides tasks for system administration. For more information about using the web-browser-based user interface, see 5.1.1, “Web-based user interface” on page 292.

1.2 Enhancements in HMC Version 8

This section gives an overview of the new content that can be exercised on this HMC code level:

- An enhancement was added in HMC to provide support for VLAN tag for network boot of IBM i.
- HMC provides complete management of the shared storage pool cluster functionality with the multiple tier and pool mirroring support. Additional features of migrating the shared storage pool volumes across tiers, and resizing the shared storage pool volumes is supported in the HMC V8R8.4.0.
- Added SFTP protocol support to Power firmware update.
- Added update support for SR-IOV devices.
- Migration with Inactive Source Storage VIOS. With this feature, you can migrate logical partitions even if one of the Virtual I/O Servers in a redundant setup is not active. Virtual storage adapter information (virtual SCSI and virtual Fibre Channel) is persisted for all the partitions on each (managing) HMC that is used during migration. A server-level preference (`allow_inactive_source_storage_vios`) is provided to enable this feature.
- Convert Permanent Capacity on Demand Entitlement to Mobile. In the HMC V8 release, a new function is provided that allows the IBM Product Fulfillment to provide a Capacity on Demand configuration file that converts permanent Capacity on Demand entitlements to mobile entitlements so that they can be used by a Power Enterprise Pool.
- Improvement to communication between management console and VIOS to make Live Partition Mobility operation resilient to network disruption and heavy load.

1.2.1 Further enhancements to Enhanced+ user interface

The Enhanced+ User Interface received the following major enhancements:

- Consolidation of Templates and OS Images under one window.
- Addition of Action buttons to tables improves touch-screen accessibility.
- Improvements to New System Experience. Newly added systems will be placed at the top of the table or beginning of the gallery view until the view is refreshed, making them easily accessible for faster configuration.
- Improvements to the integrated HMC help:
  - You can now open the help in a pop-out window to view help content and HMC User Interface at the same time.
  - Search functionality is integrated into a new help pop-out window.
  - The help window now shows a table of contents, previously viewed topics, and also related topics.
- Consolidation of System Properties and Licensed Capabilities. System properties are no longer split between Enhanced+ “look-and-feel” and a separately launched legacy panel. Licensed capabilities are all accounted for under a new PowerVM task.

1.2.2 Virtual storage diagrams

The following virtual storage diagrams are available:

- Partition-level storage diagram. Accessible from the logical partition in the Enhanced+ user interface only, this feature provides a visual representation of the storage tied to the individual partition. Easily illustrates the relationships between different storage entities such as shared storage pools, disks, and adapters.
- System-level storage diagram. Accessible from the managed system in the Enhanced+ user interface only, this feature provides a visual representation of the high-level storage configuration for an individual system.

The HMC can work with the integrated management module 2 (IMM2) remote control feature on an as-is basis. This feature is useful for installation and upgrades in a lights-out data centers and remote debugging. The IMM2 remote control feature needs to be enabled for this enhancement.

1.2.3 NIST support for HMC

Starting with HMC V8.4.0, the HMC supports NIST SP800-131A by implementing the following features:

- Upgrading JVM to a version that contains NIST support.
- Enabling TLS V1.2; prepare to disable protocols less than TLS V1.2.
- Cryptographic keys adhere to a minimum key strength of 112 bits.
- Digital signatures at a minimum use SHA-256.
- Uses approved random number generator (Java only).

Enabling NIST SP800-131A in HMC enables the following tasks:

- Changes the SSL protocol to TLS V1.2.
- HMC now uses the SP 800-131a approved cipher suites.

HMC browser requirements for NIST

Table 1-2 lists the HMC browser requirements after NIST SP800-131A is enabled.

Table 1-2 HMC browser requirements

Browser name	Browser version	NIST (TLS v1.2) supported
Firefox	► 1 - 18 ► ESR 10 and 17 ► 19 - 23	No
	► 24 - 26 ► ESR 24‘	Yes, but disabled by default
	► 27+ ► ESR31 and later	Yes
Internet Explorer	6 and 7	No
	8 and later	Yes, but disabled by default
	11	Yes
Chrome	0 - 29	No
	30 and later	Yes

Checking the HMC security mode

To check the current security mode, run **`lshmc`**. If NIST SP800-131A is disabled, the system returns `legacy` as the output, as shown in Example 1-1.

Example 1-1 HMC without NIST SP800-131A security compliance

```
hscroot@hmc8:~>lshmc -r -Fsecurity
legacy
```

If NIST SP800-131A is enabled, the system returns `nist_sp800_131a` as the output, as shown in Example 1-2.

Example 1-2 HMC with NIST SP800-131A security compliance

```
hscroot@hmc8:~>lshmc -r -Fsecurity
nist_sp800_131a
```

Enabling the NIST SP800-131A security mode

To enable the NIST SP800-131A security mode, run **`chhmc`**, as shown in Example 1-3.

Example 1-3 Enable the NIST SP800-131A security mode

```
hscroot@hmc8:~>chhmc -c security -s modify --mode nist_sp800_131a
The Hardware Management Console will automatically be restarted after the security
mode is changed. Are you sure you want to change the security mode now (0 = no, 1
= yes)?
1

Broadcast message from root@hmc8 (Thu May  8 14:40:43 2014):

The system is shutting down for reboot now.
```

Note: The HMC is rebooted to enable the new security mode.

Disabling the NIST SP800-131A security mode

To disable the NIST SP800-131A security mode, run **chhmc**, as shown in Example 1-4.

Example 1-4 Disable the NIST SP800-131A security mode

```
hscroot@hmc8:~>chhmc -c security -s modify --mode legacy
The Hardware Management Console will automatically be restarted after the security
mode is changed. Are you sure you want to change the security mode now (0 = no, 1
= yes)?
1

Broadcast message from root@hmc8 (Thu May  8 14:53:33 2014):

The system is shutting down for reboot now.
```

Effect of NIST SP800-131A compliance

After NIST SP800-131A is activated, the following tasks are effected:

- All base HMC and Hardware Management Console Representational State Transfer (REST) application program interfaces (APIs) calls allow the TLS V1.2 protocol and approved cipher suite.
- If a dependent component is not configured with the TLS V1.2 protocol or an approved cipher suite, the system generates an SSL handshake error.

1.2.4 HMC Virtual Appliance

The IBM Power Systems HMC virtual appliance can be used to manage any of the systems that are supported by the HMC Version 8, which includes Power Systems servers with IBM POWER6, POWER7, and POWER8 processors.

The Power Systems HMC virtual appliance offers these benefits:

- Provides hardware, service, and basic virtualization management for your Power Systems servers
- Offers the same functionality as the traditional HMC
- Runs as a virtual machine on an x86 server virtualized either by VMware ESXi or Red Hat KVM

With the HMC virtual appliance, a new option gives clients additional flexibility to deploy an HMC to manage IBM Power Systems servers. Clients can use the option to provide the hardware and server virtualization to host the IBM supplied HMC virtual appliance.

Power virtualization allows organizations to deliver services more efficiently by consolidating workloads onto fewer servers. This consolidation optimizes utilization of server and storage resources. Power virtualization offerings include IBM PowerVM and IBM PowerKVM. The management of PowerVM typically requires the IBM HMC.

Power virtualization enhancements include the following improvements for PowerVM, PowerKVM, and HMC:

- PowerVM support for Power Enterprise Systems featuring the IBM POWER8 processor.
- An additional option for one-year software maintenance for PowerVM for IBM PowerLinux™ Edition.
- Starting with HMC V8.2.0, which offers an improved user experience for PowerVM.
- Starting with PowerKVM V2.1.1, which provides support for new Linux distributions, additional I/O support, and availability improvements.

Starting with IBM HMC V8 R8.2.0 enhancements improve the usability of IBM PowerVM and support the new Power Enterprise Systems.

1.2.5 PowerVM NovaLink overview

NovaLink is a new virtualization management paradigm for PowerVM systems and allows for dramatic scale improvements for PowerVM based PowerVC environments. For more information about NovaLink and its benefits, see IBM developerWorks®:

https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Wc1c29d23e0fd_4346_b509_f1c00a2099f0/page/PowerVC%20NovaLink%20Overview

Leveraging the NovaLink architecture, PowerVC is able to significantly increase its scaling for PowerVM based systems. In an existing HMC managed environment, PowerVC can manage up to 30 hosts and up to 3000 virtual machines. In a NovaLink based environment, PowerVC can manage up to 200 hosts and 5000 virtual machines. Do not worry though, you can use PowerVC to manage your new NovaLink systems while still managing your HMC managed systems.

PowerVM NovaLink architecture

IBM PowerVC V1.3.0 is an advanced virtualization management offering for Power Systems servers based on OpenStack technology. This comprehensive virtualization management offering is simple to install and use, and enables virtual machine setup and management.

PowerVC can help achieve the following goals:

- Improve resource usage to reduce capital expense and power consumption.
- Increase agility and execution to quickly respond to changing business requirements.
- Increase IT productivity and responsiveness.
- Simplify Power Systems virtualization management.
- Accelerate repeatable, error-free virtualization deployments.

PowerVC can manage AIX, Linux, and IBM i VMs running under PowerVM virtualization and Linux VMs running under PowerKVM virtualization. This release supports the enterprise Power Systems servers that are built on POWER8 technology.

PowerVC includes the following features and benefits:

- Virtual machine image capture, deployment, resizing, and management
- Policy-based VM placement to help improve usage and reduce complexity
- Policy-based workload optimization using either VM migration or resource movement using mobile capacity on demand
- VM Mobility with placement policies to help reduce the burden on IT staff in a simplified GUI

- A management system that manages existing virtualization deployments
- Integrated management of storage, network, and compute resources, which simplifies administration

PowerVC v1.3.0 is built with OpenStack technology, one of the key components of the set of “host” processes, such as nova-compute, neutron (networking), and ceilometer (statistics). Each host that is managed by PowerVC runs an independent set of these processes. Figure 1-1 shows how PowerVC manages PowerVM Systems through the HMC. The HMC acts as a central management controller for sets of hardware. Because the HMC is a closed appliance, PowerVC must run the various compute processes on the PowerVC system directly. This increases the CPU and memory requirements on the PowerVC system, and limits scalability.

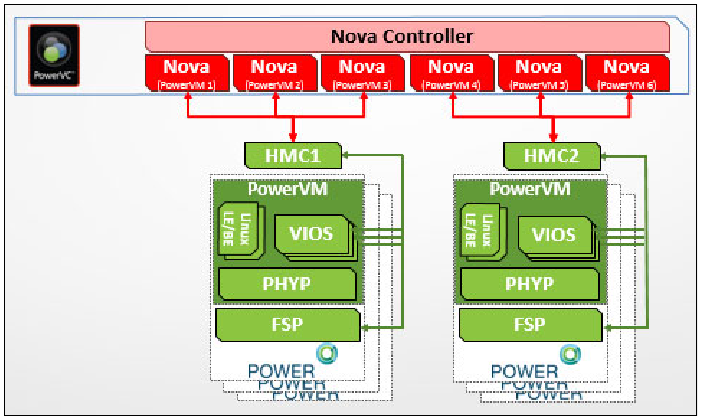


Figure 1-1 PowerVM NovaLink architecture

Another limitation is that when PowerVC manages through an HMC, it can manage only up to 500 virtual machines (logical partitions) per HMC. An HMC that is not in use by PowerVC can scale higher, but due to monitoring and other ongoing processes it is tuned for 500 VMs when managed using PowerVC. That means if you want to take advantage of PowerVC at a higher scale, you need multiple HMCs.

The NovaLink architecture changes the virtualization management point for PowerVC. With NovaLink, a thin “management” virtual machine exists on the system. You can see the thin NovaLink partition denoted in Figure 1-2 as NVL.

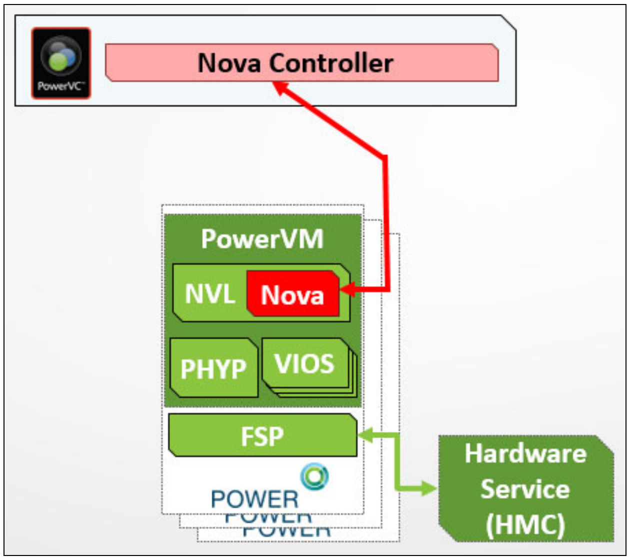


Figure 1-2 NovaLink partition

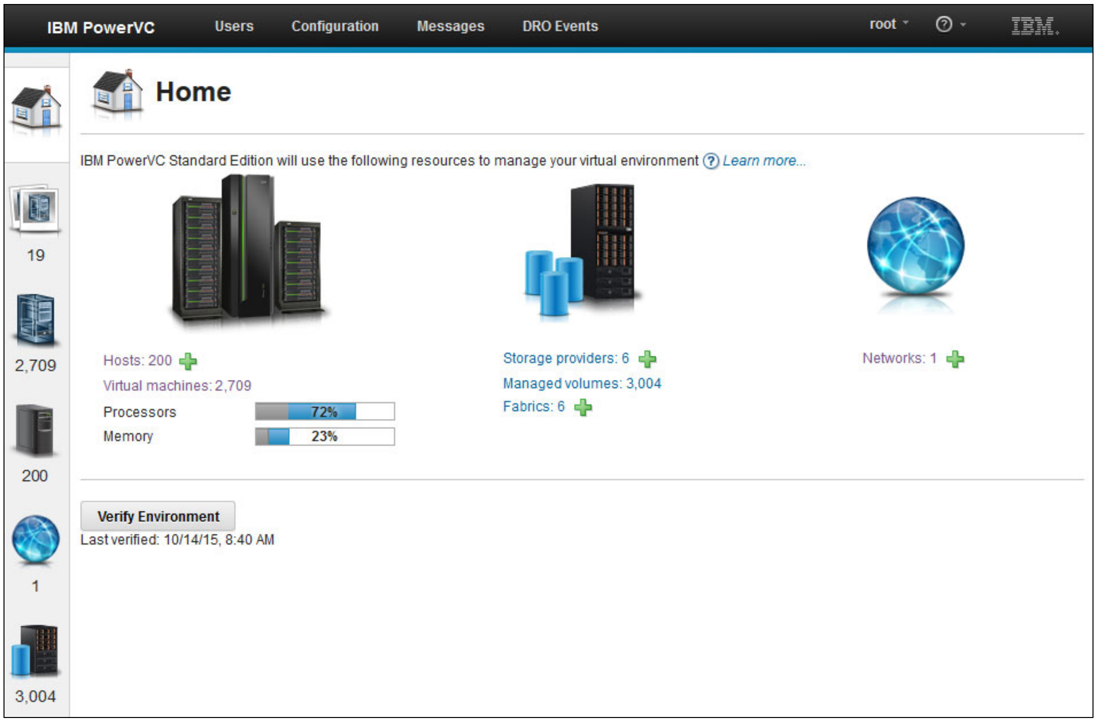
This figure shows that the architecture between PowerVC and a PowerVM system is dramatically simplified. The compute processes now run directly on the NovaLink thin virtual machine. This allows PowerVC to dramatically scale out the number of hosts that it can manage using this one-to-one link. It also reduces the load on an administrator’s HMC, allowing the hosts to connect significantly more systems to a given HMC than they would otherwise.

Also, the NovaLink code is tuned directly for PowerVC and OpenStack use. This increased efficiency allows PowerVC to scale a single system to 1,000 virtual machines, double the current 500 VMs per system limitation that exists today. More important, it is aligned with the capabilities of the PowerVM platform itself.

PowerVM NovaLink user experience

The integration of Novalink is designed to provide a unified PowerVM experience. Whether you choose to have PowerVC manage through NovaLink (to take advantage of the scale and speed) or using the traditional HMC path, PowerVC provides you with a consistent experience.

As shown, the experience within the interface is similar. In Figure 1-3, the home page looks identical, although PowerVC is managing NovaLink systems. However, note the dramatic increase in hosts.



Home

IBM PowerVC Standard Edition will use the following resources to manage your virtual environment ? *Learn more...*

Hosts: 200 +
Virtual machines: 2,709
Processors 72%
Memory 23%

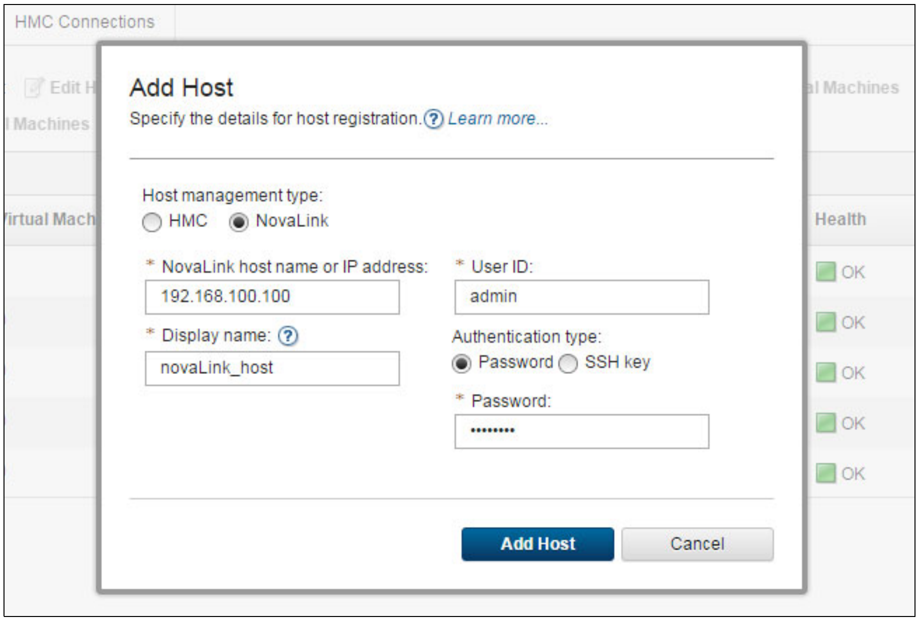
Storage providers: 6 +
Managed volumes: 3,004
Fabrics: 6 +

Networks: 1 +

Last verified: 10/14/15, 8:40 AM

Figure 1-3 PowerVC Standard edition interface

There are some areas where changes are evident in the user interface. The most obvious one is the Host Registration panel. Although host registration for an HMC managed system remains unchanged, there is a new path for NovaLink host registration. Administrators provide the IP Address and credentials of the NovaLink VM, which PowerVC uses to register the system. This panel is similar to the panel used for PowerKVM system registration. Figure 1-4 shows the Host Registration panel.



HMC Connections

Add Host

Specify the details for host registration. ? Learn more...

Host management type:
○ HMC ● NovaLink

* NovaLink host name or IP address: 192.168.100.100

* Display name: ? novaLink_host

* User ID: admin

Authentication type:
● Password ○ SSH key

* Password: ••••••••

Figure 1-4 Host Registration panel

Beyond this, few other differences exist. The Host panel does not show through which HMC the PowerVC is managing (because it manages through NovaLink).

In addition, to ensure a unified experience, a single PowerVC can mix the management types. This means that a single PowerVC can manage some systems through an HMC and others through NovaLink.

Figure 1-5 shows the NovaLink diagrams.

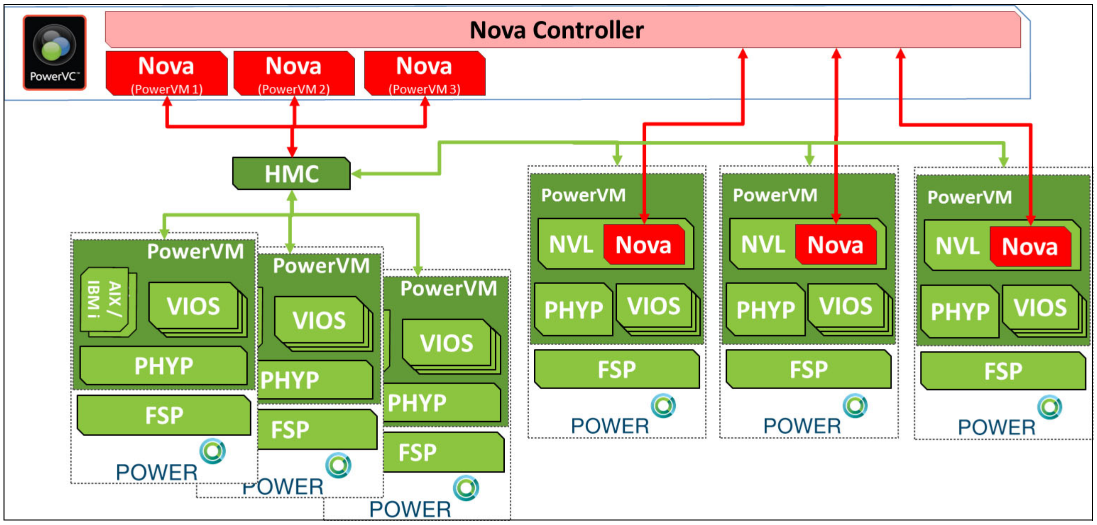


Figure 1-5 NovaLink diagrams

As shown, the same HMC can be used for PowerVC traditional management, or NovaLink management. However, if a system has NovaLink installed, PowerVC must be pointed to the NovaLink on the system. This mixed mode provides a good path for our existing customers that want to start taking advantage of NovaLink without too much disruption.

Key prerequisites

For IBM PowerVC, the key prerequisites are as follows:

- IBM PowerVM Standard Edition (5765-PVS) for basic functions, and IBM PowerVM Enterprise Edition (5765-PVE) or IBM PowerVM PowerLinux Edition (5765-PVL) for full function.
- IBM PowerKVM (5765-KVM).
- Firmware v8.2, or higher, is required for the new Remote Restart function for IBM PowerVM that is managed by IBM PowerVC.

For IBM PowerVM, the key prerequisites are as follows:

- Any IBM system that includes an IBM POWER7, POWER7+™, or POWER8 processor.
- PowerVM NovaLink requires systems with a POWER8 processor and Firmware 840, or later, that is not managed by an HMC.

NovaLink provides significant advantages for PowerVM users who want to scale up their environments. It is highly concurrent and highly scalable, and can reduce infrastructure complexity. At the same time, the existing PowerVC experience is preserved enabling administrators to take advantage of these benefits quickly.

1.2.6 Live Partition Mobility improvements in PowerVM 2.2.4

PowerVM Version 2.2.4 is a major upgrade that includes many new enhancements. One of the major areas of focus has been improvements to Live Partition Mobility (LPM). Live Partition Mobility is at the heart of any cloud solution and provides higher availability for planned outages.

Better NPIV storage validation

PowerVM Version 2.2.4 allows you to select the level of N_Port ID Virtualization (NPIV) storage validation that best fits your environment. By default, the VIOS at PowerVM Version 2.2.4 will continue to do LPM validation at the NPIV port level. This is appropriate if you are confident that the Storage Area Network (SAN) storage is correctly zoned. If you are setting up a new LPM environment or want to assure yourself that SAN zoning errors are caught prior to starting an LPM operation, you will want to enable the new disk plus port level validation. With disk-level validation enabled, the VIOS will validate that individual disk Logical Unit Number (LUNs) assigned to the partition are usable on the target system. This additional checking will increase the amount of time required to perform LPM validation but has the advantage of surfacing zoning issues that could impact VM migration.

To take advantage of NPIV validation at the disk level, both the source and target VIOS partitions must be at version 2.2.4. To enable disk level validation, the src_lun_val attribute in the LPM pseudo-device (vioslpm0) of the VIOS that is hosting the NPIV storage on the source system must be set to a value of on and the dest_lun_val attribute on the VIOS partitions that are hosting NPIV storage on the destination system cannot be set to lpm_off or off. You can find more information about displaying and changing the VIOS NPIV partition migration attributes at the IBM Knowledge Center (NPIV LUN or disk level validation).

Improved performance

Performance of Live Partition Mobility has been a focus area for IBM over the past few releases of PowerVM. This trend has continued in version 2.2.4 with scalability improvements to support higher speed connections. Prior to version 2.2.4, a single LPM operation was only able to saturate a 10 Gb network connection. To support network bandwidth up to 35 Gb, improvements were made in the VIOS and PowerVM hypervisor in version 2.2.4. The connection can be a single connection or redundant connection built using link aggregation. These faster speed connections for a single LPM operation both reduce the time to migrate a partition and can also address application issues that are triggered by slow speed lines.

To drive a high-speed line at its rated speed, you must allocate additional VIOS resources to the LPM operation. You can control the number of resources using the concurrency level setting for the VIOS and the **`migrlpar`** HMC command. The concurrency level can be set specifically for a migration by the **`migrlpar`** HMC command and will override the VIOS default for that migration. The highest level of concurrency (best performance and highest amount of resource consumption) is concurrency level 1. This is preferred if you want to drive LPM operation at network speeds greater than 30 Gb. Concurrency level 4 is the default value and is preferred for line speeds up to 10 Gb.

To take advantage of these performance improvements, both the source and target systems must be at PowerVM version 2.2.4. You can find more information about displaying and changing the VIOS concurrency level attributes at the IBM Knowledge Center.

Virtual switch

Starting in PowerVM 2.2.4 the HMC allows the selection of the virtual switch name on the target system. Prior to PowerVM 2.2.4, there was no option to override the virtual switch name so you were required to have the same named virtual switch on both the source and target system.

Minimum PowerVM levels

To support the capabilities discussed in this section, you will need PowerVM 2.2.4 which consists of these releases:

- VIOS Version 2.2.4
- System Firmware Release 8.4.0
- HMC Release 8 Version 8.4.0

For more details, see IBM developerWorks and the IBM Knowledge Center:

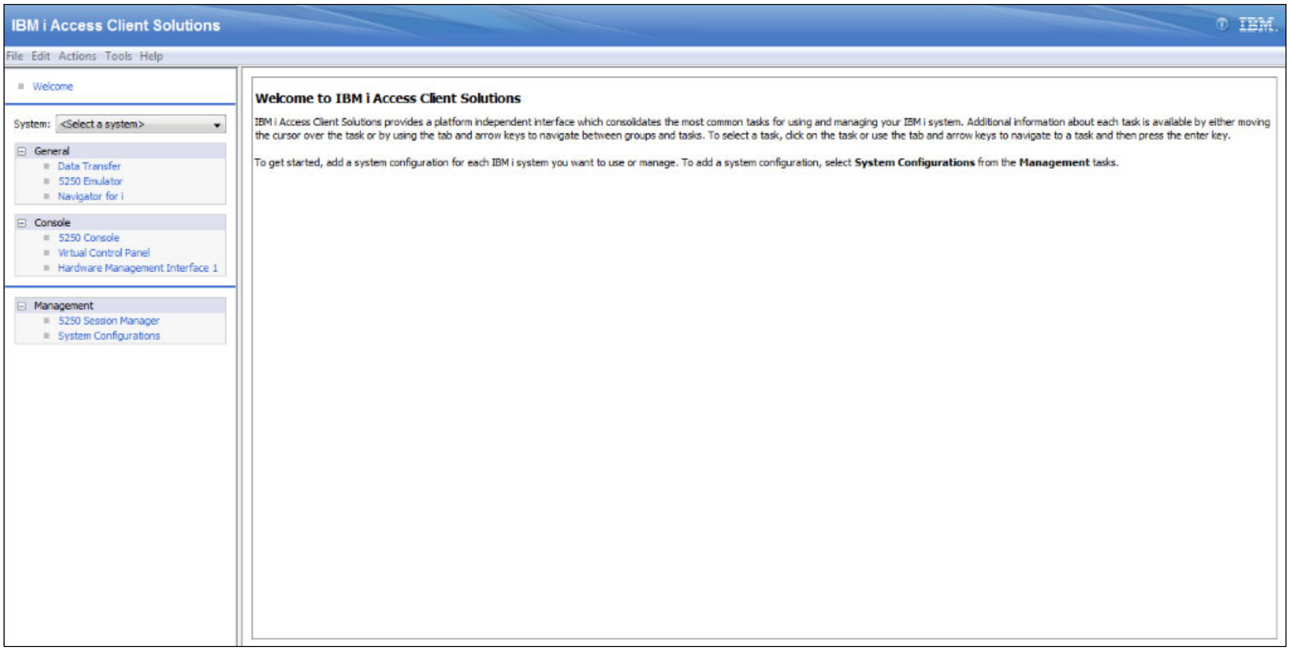
- https://ibm.biz/Bd4jw8
- https://ibm.biz/Bd4jwV

1.2.7 IBM i virtual terminal changes

IBM i Access Client Solutions replaces IBM i Access for Linux Emulation. It provides a Java based, platform-independent interface that runs on operating systems that support Java, including Linux, Mac, and Windows.

IBM i Access Client Solutions consolidates the most commonly used tasks for managing your IBM i into one simplified location.

The main IBM i Access Client Solutions window is shown Figure 1-6.



Welcome to IBM i Access Client Solutions

IBM i Access Client Solutions provides a platform independent interface which consolidates the most common tasks for using and managing your IBM i system. Additional information about each task is available by either moving the cursor over the task or by using the tab and arrow keys to navigate between groups and tasks. To select a task, click on the task or use the tab and arrow keys to navigate to a task and then press the enter key.

To get started, add a system configuration for each IBM i system you want to use or manage. To add a system configuration, select **System Configurations** from the **Management** tasks.

Figure 1-6 IBM i Access Client Solutions

For more information, see the IBM POWER8 systems information at these web pages:

- `http://www.ibm.com/systems/power/software/i/access/index.html`
- `https://ibm.biz/Bd4jkc`

1.2.8 Single root I/O virtualization support

Single root I/O virtualization (SR-IOV) is a PCI standard architecture that enables a PCI Express (PCIe) adapter to become self-virtualizing. It enables adapter consolidation, through sharing, much like logical partitioning enables server consolidation. With an adapter capable of SR-IOV, you can assign virtual *slices* of a single physical adapter to multiple partitions through logical ports; all of this is done without the need for a VIOS.

Initial SR-IOV deployment supports up to 48 logical ports per adapter, depending on the adapter. You can provide additional fan-out for more partitions by assigning a logical port to a VIOS, and then using that logical port as the physical device for a Shared Ethernet Adapter (SEA). VIOS clients can then use that SEA through a traditional virtual Ethernet configuration. Overall, SR-IOV provides integrated virtualization without VIOS and with greater server efficiency as more of the virtualization work is done in the hardware and less in the software.

Initial support for SR-IOV was included in HMC V7.7.9.0. Starting with the release of HMC V8.8.1.0, support for the following adapters is included:

- PCIe2 4-port (10 Gb FCoE and 1 GbE) SR&RJ45 Adapter
- PCIe2 4-port (10 Gb FCoE and 1 GbE) SFP+Copper and RJ4 Adapter
- Integrated Multifunction Card with 10 GbE RJ45 and Copper Twinax
- Integrated Multifunction Card with 10 GbE RJ45 and SR Optical

For more details about SR-IOV, see the following sources of information:

- *IBM Power Systems SR-IOV: Technical Overview and Introduction*, REDP-5065
- The “Single root I/O virtualization” topic in the IBM Knowledge Center:

  https://www.ibm.com/support/knowledgecenter/POWER7/p7hb1/iphb1_vios_concepts_network_sriov.htm

1.2.9 vNIC: Introducing PowerVM Virtual Networking Technology

Virtual Network Interface Controller (vNIC) is a new PowerVM virtual networking technology that delivers enterprise capabilities and simplifies network management. It is a high performance, efficient technology that when combined with SR-IOV NIC provides bandwidth control quality of service (QoS) capabilities at the virtual NIC level. vNIC significantly reduces virtualization overhead resulting in lower latencies and less server resources (CPU, memory) required for network virtualization.

Figure 1-7 shows the vNIC backed by SR-IOV adapter.

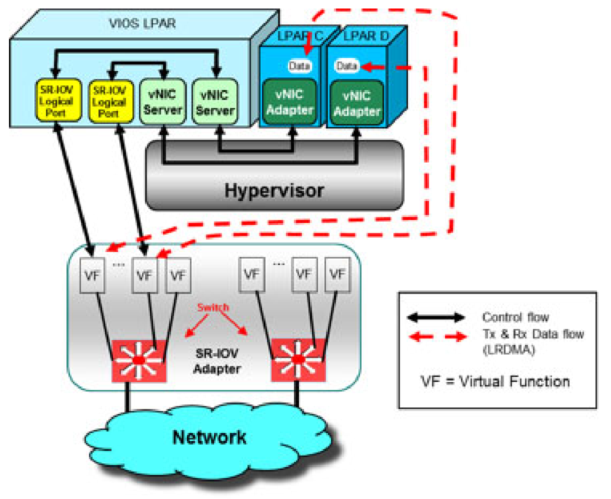


Figure 1-7 vNIC backed by SR-IOV adapter

Until now, PowerVM network virtualization has mostly relied on Shared Ethernet Adapter (SEA) in VIOS and virtual switch in the PowerVM Hypervisor to bridge the Virtual Ethernet Adapters (VEA) with the physical network infrastructure. While this approach provides great flexibility in enabling network connectivity for client logical partitions, the SEA-based virtual networking solution incurs layered software overhead and multiple data copies from the time a packet is committed for transmission on VEA to the time the packet is queued on the physical NIC for transmission (same issues apply for receive packets). In the meantime, the PCI industry has developed the SR-IOV (Single Root I/O Virtualization and Sharing) standard for hardware-based virtualization technology. An SR-IOV adapter allows creation of multiple virtual replicas of a PCI function, called a Virtual Function (VF), and each VF can be assigned to a logical partition independently. The SR-IOV VF operates with little software intervention providing superior performance with little CPU overhead. The Host Ethernet Adapter (HEA) introduced with POWER6 based systems was an early implementation of such hardware virtualization solution.

In 2014, support was added for SR-IOV adapters for selected models of POWER7+ systems and more recently for POWER8 based systems. While a dedicated SR-IOV VF provides great performance advantage, this configuration does not allow Live Partition Mobility, which can be a major drawback. With this new technology, LPM is supported for SR-IOV VFs, which are assigned to vNICs. This is made possible because the SR-IOV VF is assigned to the VIOS directly and is used by the client logical partition. Since the SR-IOV VF or logical port resides in the VIOS instead of the client logical partition, the logical partition is LPM capable.

Figure 1-7 on page 19 shows the key elements in the vNIC model. There is a one-to-one mapping or connection between vNIC adapter in the client logical partition and the backing logical port in the VIOS. Through a proven PowerVM technology known as logically redirected DMA (LRDMA), packet data for transmission (similarly for receive) is moved from the client logical partition memory to the SR-IOV adapter directly without being copied to the VIOS memory.

The benefits of bypassing VIOS on the data path are two-fold:

- Reduction in the overhead of memory copy (for example, lower latency)
- Reduction in the CPU and VIOS memory consumption (for example, efficiency)

Besides the optimized data path, the vNIC device supports multiple transmit and receive queues, like many high performance NIC adapters. These design points enable vNIC to achieve performance that is comparable to direct attached logical port, even for workloads dominated with packets of small sizes. Figure 1-8 is the control and data flow differences between the current virtual Ethernet and the new vNIC support.

Figure 1-8 shows the comparison of virtual Ethernet and vNIC control and flows.

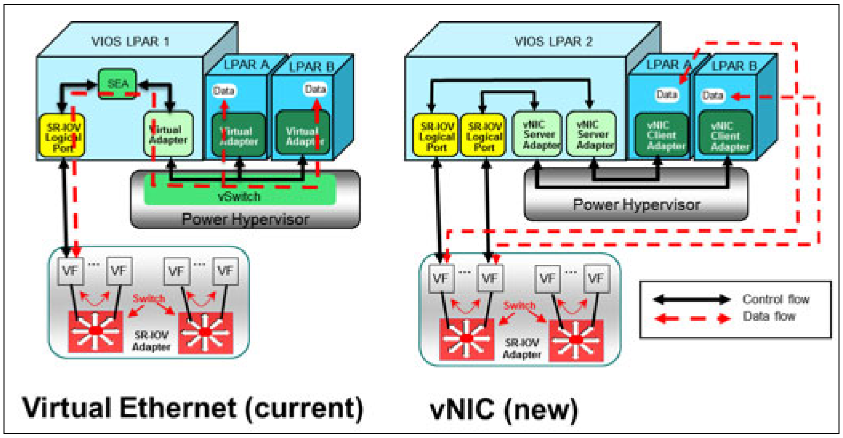


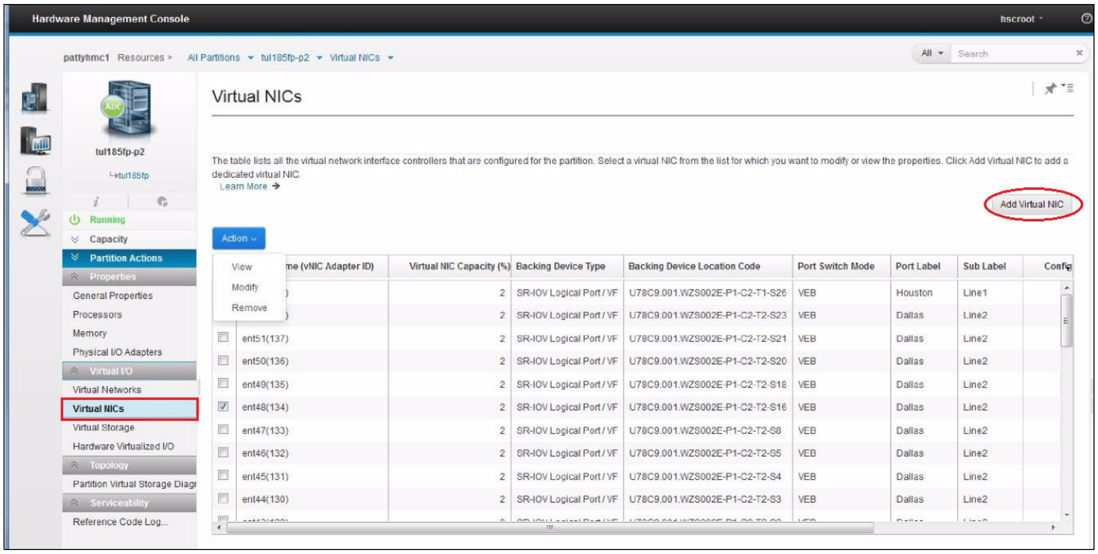
Figure 1-8 Comparison of Virtual Ethernet & vNIC control and flows

In addition to the improved virtual networking performance, the client vNIC can take full advantage of the quality of service (QoS) capability of the SR-IOV adapters supported on Power Systems. Essentially, the QoS feature ensures that each logical port receives its share of adapter resources, which includes its share of the physical port bandwidth. A vNIC combined with SR-IOV adapters provides the best of both quality of service and flexibility.

Link aggregation technologies such as IEEE 802.3ad/802.1ax Link Aggregation Control Protocol (LACP) and active-back approaches (for example, AIX Network Interface Backup (NIB), IBM i VIPA, or Linux Active-Backup bonding mode) are supported for failover with some limitations. In the case of LACP, the backing logical port must be the only VF on the physical port. This restriction is not specific to vNIC; it applies to the direct attached VF also. When using one of the active-backup approaches, a capability to detect a failover condition must be configured, such as an IP address to ping for AIX NIB. The vNIC and the VEA backed by SEA can coexist in the same logical partition. At this time SEA failover is not supported but similar capability is planned for the future.

vNIC support can be added to a partition by adding a vNIC client virtual adapter to the partition using the HMC. When adding a vNIC client, the user selects the backing SR-IOV adapter, the physical port, and the VIOS hosting the server devices, defines capacity, and other parameters, Port VLAN ID, VLAN access list, and others. Default settings are used if the user does not specify the parameter. The HMC creates all the necessary devices in the client logical partition and also VIOS. The HMC supports configuration and control of vNIC configurations in the GUI, command line, or Hardware Management Console Representational State Transfer (REST) application program interfaces (REST APIs). Note that most of the vNIC GUI support is available only using the HMC Enhanced GUI (not in the Classic view). Figure 1-9 shows a snapshot of vNIC device listing in a logical partition using the HMC Enhanced GUI view. For vNIC removal, HMC does the cleanup in both logical partition and in VIOS. So, from a user's perspective, the user deals with only the client vNIC adapter and does not have to be concerned with backing devices in normal cases because they are managed automatically by the HMC.

Figure 1-9 shows the HMC Enhanced GUI Listing of vNIC devices.



The table lists all the virtual network interface controllers that are configured for the partition. Select a virtual NIC from the list for which you want to modify or view the properties. Click Add Virtual NIC to add a dedicated virtual NIC.

	me (vNIC Adapter ID)	Virtual NIC Capacity (%)	Backing Device Type	Backing Device Location Code	Port Switch Mode	Port Label	Sub Label	Config
	)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T1-S26	VEB	Houston	Line1	
	)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S23	VEB	Dallas	Line2	
□	ent51(137)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S21	VEB	Dallas	Line2	
□	ent50(136)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S20	VEB	Dallas	Line2	
□	ent49(135)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S18	VEB	Dallas	Line2	
☑	ent48(134)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S16	VEB	Dallas	Line2	
□	ent47(133)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S8	VEB	Dallas	Line2	
□	ent46(132)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S5	VEB	Dallas	Line2	
□	ent45(131)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S4	VEB	Dallas	Line2	
□	ent44(130)	2	SR-IOV Logical Port / VF	U78C9.001.WZS002E-P1-C2-T2-S3	VEB	Dallas	Line2	

Figure 1-9 HMC Enhanced GUI: Listing of vNIC devices

During LPM or Remote Restart operations, the HMC handles the creation of the vNIC server and backing devices on the target system and cleanup of devices on the source system when LPM completes. The HMC also provides auto-mapping of devices (namely selecting suitable VIOS and SR-IOV adapter port to back each vNIC device). The SR-IOV port label, available capacity, and VIOS redundancy are some of the items used by the HMC for auto mapping. Optionally users have the choice of specifying their own mapping manually.

The minimum PowerVM and OS levels required to support vNIC are as follows:

- PowerVM 2.2.2
- VIOS Version 2.2.4
- System Firmware Release 8.4.0
- HMC Release 8 Version 8.4.0

The required operating systems levels are as follows:

- AIX 7.1 TL4 or AIX 7.2
- IBM i 7.1 TR10 or IBM i 7.2 TR3

Note: Linux support to follow at a future date.

1.2.10 Dynamic Partition Remote Restart

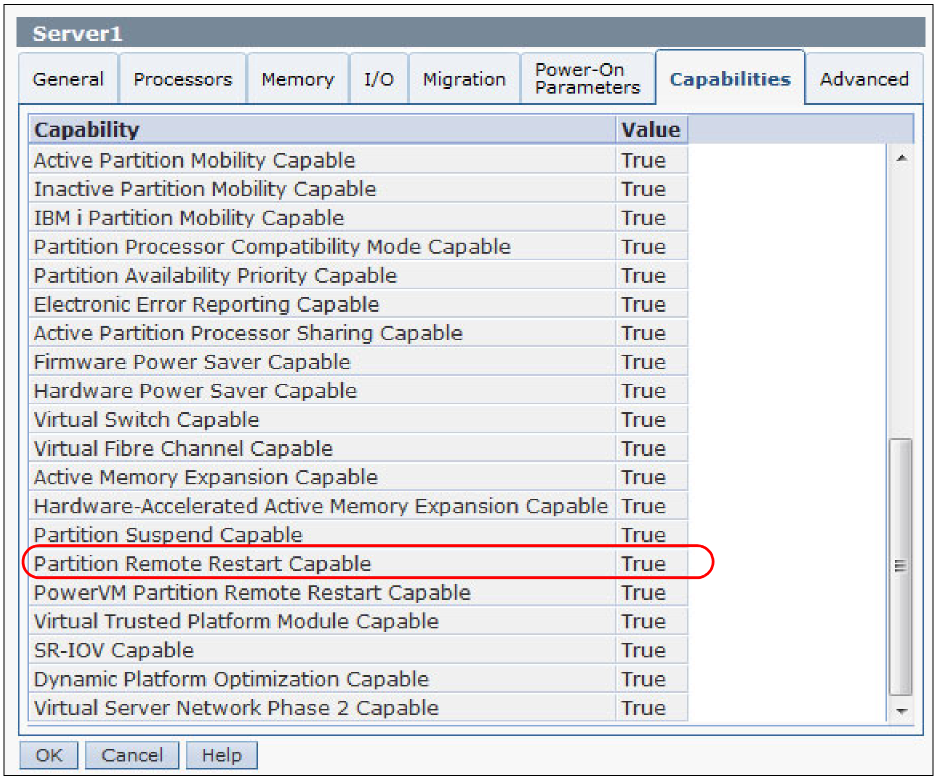
Partition Remote Restart is a function that is designed to enhance the availability of a partition on another server when its original host server fails. This is a high availability (HA) function of PowerVM Enterprise Edition.

Starting with HMC V8 R8.1.0, the requirement of enabling Remote Restart of a logical partition only at creation time is removed. Dynamic Partition Remote Restart allows for the dynamic toggle of Remote Restart capability when a logical partition is deactivated. To verify that your managed system can support this capability, enter the command that is shown in Example 1-5. The highlighted text indicates that the managed system can remotely restart a partition.

Example 1-5 PowerVM Remote Restart Capable

```
hscroot@slcb27a:~>lssyscfg -r sys -m Server1 -F capabilities
"active_lpar_mobility_capable,inactive_lpar_mobility_capable,os400_lpar_mobility_c
apable,active_lpar_share_idle_procs_capable,active_mem_dedup_capable,active_mem_ex
pansion_capable,hardware_active_mem_expansion_capable,active_mem_mirroring_hypervi
sor_capable,active_mem_sharing_capable,autorecovery_power_on_capable,bsr_capable,c
od_mem_capable,cod_proc_capable,custom_mac_addr_capable,dynamic_platform_optimizat
ion_capable,dynamic_platform_optimization_lpar_score_capable,electronic_err_report
ing_capable,firmware_power_saver_capable,hardware_power_saver_capable,hardware_dis
covery_capable,hardware_encryption_capable,hca_capable,huge_page_mem_capable,lpar_
affinity_group_capable,lpar_avail_priority_capable,lpar_proc_compat_mode_capable,l
par_remote_restart_capable,powervm_lpar_remote_restart_capable,lpar_suspend_capabl
e,os400_lpar_suspend_capable,micro_lpar_capable,os400_capable,5250_application_cap
able,os400_net_install_capable,os400_restricted_io_mode_capable,redundant_err_path
_reporting_capable,shared_eth_auto_control_channel_capable,shared_eth_failover_cap
able,sp_failover_capable,sriov_capable,vet_activation_capable,virtual_eth_disable_
capable,virtual_eth_dlpar_capable,virtual_eth_qos_capable,virtual_fc_capable,virtu
al_io_server_capable,virtual_switch_capable,vlan_stat_capable,vtpm_capable,vsi_on_
veth_capable,vsn_phase2_capable"
```

From the HMC, click **Managed System Properties** and then the **Capabilities** tab to show all the managed system capabilities (Figure 1-10).



Capability	Value
Active Partition Mobility Capable	True
Inactive Partition Mobility Capable	True
IBM i Partition Mobility Capable	True
Partition Processor Compatibility Mode Capable	True
Partition Availability Priority Capable	True
Electronic Error Reporting Capable	True
Active Partition Processor Sharing Capable	True
Firmware Power Saver Capable	True
Hardware Power Saver Capable	True
Virtual Switch Capable	True
Virtual Fibre Channel Capable	True
Active Memory Expansion Capable	True
Hardware-Accelerated Active Memory Expansion Capable	True
Partition Suspend Capable	True
Partition Remote Restart Capable	True
PowerVM Partition Remote Restart Capable	True
Virtual Trusted Platform Module Capable	True
SR-IOV Capable	True
Dynamic Platform Optimization Capable	True
Virtual Server Network Phase 2 Capable	True

Figure 1-10 PowerVM Partition Remote Restart Capable

The capability is displayed only if the managed system supports it.

Power Systems servers running Firmware code 760 or later support the Dynamic Partition Remote Restart feature.

To activate a partition on a supported system to support Dynamic Partition Remote Restart, run the following command:

```
chsyscfg -r lpar -m <ManagedSystemName> -i
"name=<PartitionName>,remote_restart_capable=1"
```

To use the Remote Restart feature, the following conditions must be met:

- The managed system must support the *toggle partition remote capability*.
- The partition must be in the inactive state.
- The partition type must be AIX, IBM i, or Linux.
- The reserved storage device pool exists.
- The partition should not own any of the following resources or have these settings:
  - The barrier-synchronization register (BSR)
  - Time Reference Partition
  - Service Partition
  - OptiConnect
  - High speed link (HSL)
  - Physical I/O
  - HEA
  - Error Reporting Partition
  - Part of IBM Enterprise Workload Manager™ (EWLM)

– Huge Page Allocation
– Owns Virtual Serial Adapters
– Belongs to I/O Fail Over Pool
– SR-IOV non-adjunct

For more information, including the usage of Partition Remote Restart, see the following web page:

http://www.ibm.com/support/knowledgecenter/POWER8/p8hat/p8hat_enadisremres.htm

1.2.11 Absolute value for the partition command-line interface

HMC V8.8.4.0 adds additional functionality to the dynamic logical partitioning (DLPAR) commands. The functionality enables the absolute value to be set for processor and memory DLPAR operations.

With previous versions of HMC, adding or removing only the delta between the current and target values for processor or memory during DLPAR operations was possible.

Important: This function is supported for both *Active* and *Inactive* partitions.

There is a single command to set this value. It might vary depending on the attribute to be set.

DLPAR command to set the absolute value for a partition processor

The **chhwres** command to set processor absolute value has the following syntax:

```
chhwres -r proc -m <managed_system_name> --id <lpar_id> -o s [--procs quantity]
[--procunits quantity][--5250cpwpercent percentage] [-w wait-time] [-d
detail-level] [--force] [--help]
```

The following parameters are required when setting the absolute value for partition processor:

```
chhwres -r proc -m ManagedSys_A --id 1 --procs 3 -o s
```

Note: The **-o s** flag sets the absolute processor value to a partition using DLPAR.

DLPAR CLI command to set the absolute value for a partition memory

The **chhwres** command to set memory absolute value has the following syntax:

```
chhwres -r mem -m <managed_system_name> --id <lpar_id> -o s [-q quantity] [-w
wait-time] [-d detail-level] [--force] [--entitled value] [--help]
```

The following parameters are required when setting the absolute value for partition memory:

```
chhwres -r mem -m ManagedSys_A -o s --id 1 -q 256
```

Note: The **-o s** flag sets the absolute value for a partition using DLPAR.

Using the `lshwres` command, verifying that the resource value is properly set is possible.

Example 1-6 shows the adjustment of partition memory by using previous method where the *delta* of the change was specified, and then you used the absolute value setting in the **chhwres** command. The partition had 2048 MB memory allocated. This allocation was changed with 256 MB to 2304 MB by using the delta change method. The partition then had its memory changed to 3072 MB through the new absolute value parameter.

Example 1-6 Addition of memory to a partition by using the delta and absolute value settings

```
hscroot@hmc8:~>lshwres -r mem -m 9117-MMA*101F170  --level lpar --filter
"lpar_names=VIOS2" -F curr_mem
2048
hscroot@hmc8:~>chhwres -r mem -m 9117-MMA*101F170 -o a -p VIOS2 -q 256
hscroot@hmc8:~>lshwres -r mem -m 9117-MMA*101F170  --level lpar --filter
"lpar_names=VIOS2" -F curr_mem
2304
hscroot@hmc8:~>chhwres -r mem -m 9117-MMA*101F170 -o s -p VIOS2 -q 3072
hscroot@hmc8:~>lshwres -r mem -m 9117-MMA*101F170  --level lpar --filter
"lpar_names=VIOS2" -F curr_mem
3072
```

Supported setup combination

This absolute value DLPAR function is supported by the following partition setup combinations:

- Dedicated memory and dedicated processor
- Shared processor and shared memory
- Shared processor and dedicated memory

Active Memory Sharing

The absolute value also can be set on an Input/Output Entitled Memory for IBM Active Memory™ Sharing (AMS) configured partition.

The **chhwres** command in the following example sets the absolute value when using Active Memory Sharing:

```
chhwres -r mem -m firebird4 --id 3 -o s --entitled 80 -q 5376
```

1.2.12 POWER8 processor-based systems support

Starting with HMC V8.8.1.0, the HMC v8 is updated for the POWER8 processor. The details of the updates and how they affect various HMC functions are described in this section.

Processor modes

The following two processor modes are available on the POWER8 processor-based systems:

- Configured/Desired Mode

  A mode that is configured by an administrator creating or modifying a partition profile or when creating a partition.

- Effective/Current Mode

  A mode that is negotiated between the PHYP and the OS running on the partition when the partition is activated or whenever the IPL happens.

The configurable processor modes that are available on the POWER8 processor-based systems are shown in Table 1-3.

Table 1-3 Processor modes that are available on POWER8 systems

Mode	Systems
Configurable modes	Default, IBM POWER6, IBM POWER6+™, IBM POWER7, and POWER8
Effective modes	POWER6, POWER6+, POWER7, and POWER8
Default mode	POWER8

Command-line support for the new processor modes

The following commands are affected by the addition of POWER8 support. The syntax of the commands has not changed, but the output from the commands is updated with support for POWER8.

- To show the supported modes for a system, run the following command:

  ```
  lssyscfg –r sys –F lpar_proc_compat_modes
  ```

  The output is either Default, POWER6, POWER6+, POWER7, or POWER8.

- To show the desired and current mode of a partition, run the following command:

  ```
  lssyscfg -r lpar –F desired_lpar_proc_compat_mode, curr_lpar_proc_compat_mode
  ```

  POWER8 is a new possible value for these two attributes.

- To show the mode at the profile level, run the following command:

  ```
  lssyscfg -r prof –F lpar_proc_compat_mode
  ```

  POWER8 is a new possible value for this attribute.

- To specify a mode when creating a logical partition or a profile, run the following command:

  ```
  mksyscfg -r prof/lpar –m <cec_name> -I “lpar_proc_compat_mode =POWER8”
  ```

- To change the mode for a profile, run the following command:

  ```
  chsyscfg -r prof –m <cec_name> -I “lpar_proc_compat_mode =POWER8”
  ```

Processor modes for Live Partition Mobility

The following list indicates the methods of Live Partition Mobility and the supported processor modes:

- Active partition mobility

  Both desired and current processor compatibility modes of logical partition must be supported by the destination server.

- Inactive partition mobility

  Only desired processor compatibility mode of the logical partition must be supported by the destination server.

- Suspended partition mobility

  This is the same as active partition mobility.

The processor compatibility matrix for migration is updated to include POWER8 processor-based systems, as shown in Table 1-4.

Table 1-4 Processor compatibility modes matrix for POWER8 to POWER8 migration

Source environment POWER8 based system		**Destination environment POWER8 based system**			
		Active migration		Inactive migration	
Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode
Default	POWER8	Default	POWER8	Default	POWER8
POWER8	POWER8	POWER8	POWER8	POWER8	POWER8
POWER8	POWER7	POWER8	POWER7	POWER8	POWER7
POWER7	POWER7	POWER7	POWER7	POWER7	POWER7
Default	POWER7	Default	POWER7	Default	POWER7
POWER6	POWER6	POWER6	POWER6	POWER6	POWER6
POWER6+	POWER6+	POWER6+	POWER6+	POWER6+	POWER6+
Default	POWER6	61V and 71N onwards are the OS levels supporting POWER8 hardware. POWER6 mode is not possible for the default as desired mode.			

The compatibility matrix for POWER7 processor-based servers is updated to include migration from POWER8 processor-based system, as shown in Table 1-5.

Table 1-5 Processor compatibility modes matrix for POWER8 to POWER7 migration

Source environment POWER8 based system		**Destination environment POWER7 based system**			
		Active migration		Inactive migration	
Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode
POWER8	POWER8	Fails because the desired processor mode on POWER8 is not supported on the destination environment.		Fails because the desired processor mode on POWER8 is not supported on the destination environment.	
POWER8	POWER7				
Default	POWER8	Fails because the current processor mode is not supported on the destination environment.		Default	POWER7
POWER7	POWER7	POWER7	POWER7	POWER7	POWER7
Default	POWER7	Default	POWER7	Default	POWER7
POWER6	POWER6	POWER6	POWER6	POWER6	POWER6
POWER6+	POWER6+	POWER6+	POWER6+	POWER6+	POWER6+

The compatibility matrix for POWER6 processor-based systems is updated to include migration from POWER8 processor-based systems, as shown in Table 1-6.

Table 1-6 Processor compatibility modes matrix for POWER8 to POWER6 migration

Source Environment **POWER8 processor-based system**		**Destination environment** **POWER6 processor-based system**			
		Active migration		Inactive migration	
Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode
POWER6	POWER6	POWER6	POWER6	POWER6	POWER6
Default	POWER7	Fails because the current processor mode is not supported on the destination environment.		Default	POWER6
Default	POWER8			Default	POWER6
POWER8	POWER8	Fails because the current processor mode is not supported on the destination environment.		Fails because the current processor mode is not supported on the destination environment.	
POWER8	POWER7				
POWER7	POWER7				
POWER6+	POWER6+				

The compatibility matrix for POWER7 processor-based systems is updated to include migration to POWER8 processor-based systems, as shown in Table 1-7.

Table 1-7 Processor compatibility modes matrix for POWER7 to POWER8 migration

Source environment **POWER7 processor-based system**		**Destination environment** **POWER8 processor-based system**			
		Active migration		Inactive migration	
Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode
POWER7	POWER7	POWER7	POWER7	POWER7	POWER7
Default	POWER7	Default	POWER7 (If OS supports POWER8, it will be POWER8 after restarting the logical partition.)	Default	POWER8 or POWER7 (Depends on the operating system version)
POWER6	POWER6	POWER6	POWER6	POWER6	POWER6
POWER6+	POWER6+	POWER6+	POWER6+	POWER6+	POWER6+

The compatibility matrix for POWER6/6+ processor-based systems is updated to include migration to POWER8 processor-based systems, as shown in Table 1-8.

Table 1-8 Processor compatibility modes matrix for POWER6/6+ to POWER8 migration

Source environment POWER6/6+ processor-based system		**Destination environment POWER8 processor-based system**			
		Active migration		Inactive migration	
Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode	Desired processor compatibility mode	Current processor compatibility mode
Default	POWER6/6+	Default	Power6/6+ (It will be POWER7 or POWER8 depending on the operating system version upon restarting the partition.)	Default	POWER8 or POWER7 (Depends on the operating system version)
POWER6/6+	POWER6/6+	POWER6/6+	POWER6/6+	POWER6/6+	POWER6/6+

1.2.13 Performance usage metrics

Usage attributes, described here, are added for POWER8 processor-based systems and other Power Systems servers.

New logical partition level performance usage attributes

The following attributes are introduced starting with HMC V8.8.1.0 and are available for POWER8 processor-based systems:

- `total_instructions`

  The number of instructions that are performed by the partition since the managed system was started. It is independent of whether the partition is in its idle loop or running real work; the instruction count increments as instructions are completed.

- `total_instructions_execution_time`

  The number of time instruction counts were collected since the managed system was started. The time value also is not gated by the run latch and is a measure of the time the partition was running on a physical processor.

Unavailable logical partition level performance usage attributes

The following attributes are not available for POWER8 processor-based systems:

- `run_latch_cycles`

  The number of non-idle cycles that are used by the partition when the run latch was set and since the managed system was started.

- `run_latch_instructions`

  The number of non-idle instructions that are performed by the partition when the run latch was set and since the managed system was started.

Use of performance usage attributes

Example 1-7 shows the output of the **lslparutil** command when run against a POWER8 processor-based system and how the metrics can be used to aid in performance-related problem determination.

Example 1-7 The lslparutil output for a partition on a POWER8 processor-based system

```
lslparutil -r lpar -m <P8_sys> --filters lpar_ids=<lpar Id> -n 2
time=02/05/2014 19:34:00,event_type=sample,resource_type=lpar,sys_time=07/22/2026
14:06:54,time_cycles=855743101199861,lpar_name=tul179c1,lpar_id=6,curr_proc_mode=d
ed,curr_procs=1,curr_sharing_mode=share_idle_procs,curr_5250_cpw_percent=0.0,mem_m
ode=ded,curr_mem=2048,entitled_cycles=576965682013944,capped_cycles=57696568201394
4,uncapped_cycles=0,shared_cycles_while_active=0,idle_cycles=573779118316816,total
_instructions=29173046763191,total_instructions_execution_time=576964317138087
```

The two new metrics can be used to diagnose performance issues at a high level by looking at the amount of time each instruction is taking to complete.

Average time per instruction is calculated as follows:

```
total_instructions_execution_time / total_instructions
```

1.2.14 Power Integrated Facility for Linux (Power IFL)

Power IFL is an optional, lower-cost per processor core activation feature for only Linux workloads on IBM Power Systems servers. Processor cores that are activated for general-purpose workloads can run any supported operating system. If you want to activate Power IFL processor cores, the systems must be in compliance with the license terms.

What is new in Power IFL

Since the previous update of Power IFL, changes were introduced in HMC V8.8.1 to assist with managing the compliance of Power IFL processors:

- Enabled Power IFL processors can be viewed from the HMC GUI.
- Updated command-line interface (CLI) commands.
- An updated compliance monitoring assistance feature.

Command-line and graphical interface updates

Power IFL was introduced in HMC 7.9.0 and had only command-line tools for monitoring the activated processor allocation and activation.

In HMC V8.8.4.0, the Capacity on Demand (CoD) Processor Capacity Settings and managed system properties in the GUI are updated to show the activations and enable the monitoring of Power IFL processor allocation and activation.

The CLI commands also were updated to show IFL activations and available IFL processor cores.

Capacity on Demand CLI and graphical interface changes

The `lscode` command shows the permanent Linux only and all operating system processors. Example 1-8 shows the syntax of the `lscod` command and its output.

Example 1-8 Syntax of the lscod command syntax and its output

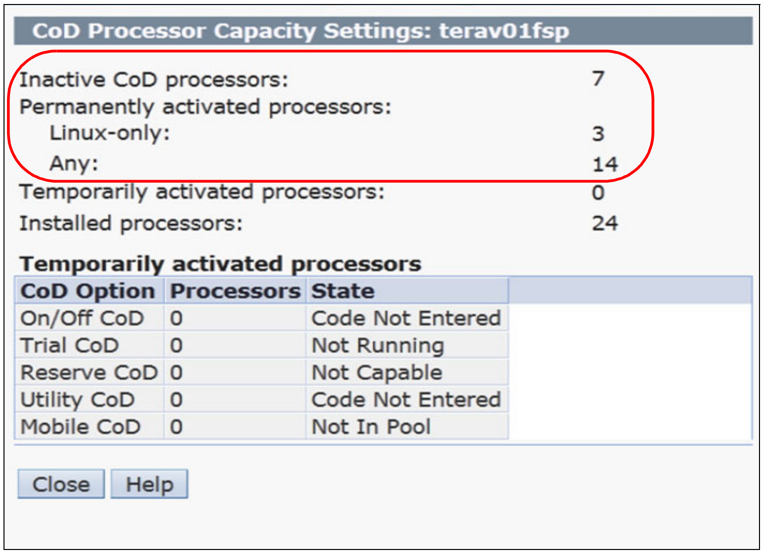
```
lscod -t cap -c cuod -r proc -m <managed system>
perm_procs=10,perm_procs_linux=3,perm_procs_all_os=7
```

The `perm_procs_linux=3` parameter indicates that three processor cores are licensed for Linux only workloads.

Notes:

- An additional `-F` flag is required if those values are not displayed in the output.
- If `perm_procs_linux` is 0, it is not shown in the default output. It is shown only when `-F` is specified.
- If `perm_procs_all_os = perm_procs, perm_procs_all_os` is not shown in the default output, it is shown only when `-F` is specified.
- If the *managed system* does not support Power IFL compliance monitoring, these attributes are not shown.

Support for Power IFL is added in HMC V8.8.1.0 to show information about CoD Capacity Processor Settings, as shown in Figure 1-11.



CoD Processor Capacity Settings: terav01fsp

Inactive CoD processors: 7
Permanently activated processors:
Linux-only: 3
Any: 14
Temporarily activated processors: 0
Installed processors: 24

Temporarily activated processors

CoD Option	Processors	State
On/Off CoD	0	Code Not Entered
Trial CoD	0	Not Running
Reserve CoD	0	Not Capable
Utility CoD	0	Code Not Entered
Mobile CoD	0	Not In Pool

Figure 1-11 CoD Processor Capacity Settings showing activated IFL processors

The **lshwres** command is updated to show the number of processor units that are configurable for either Linux only or all operating system workloads (Example 1-9).

Example 1-9 Syntax of the lshwres command and its output

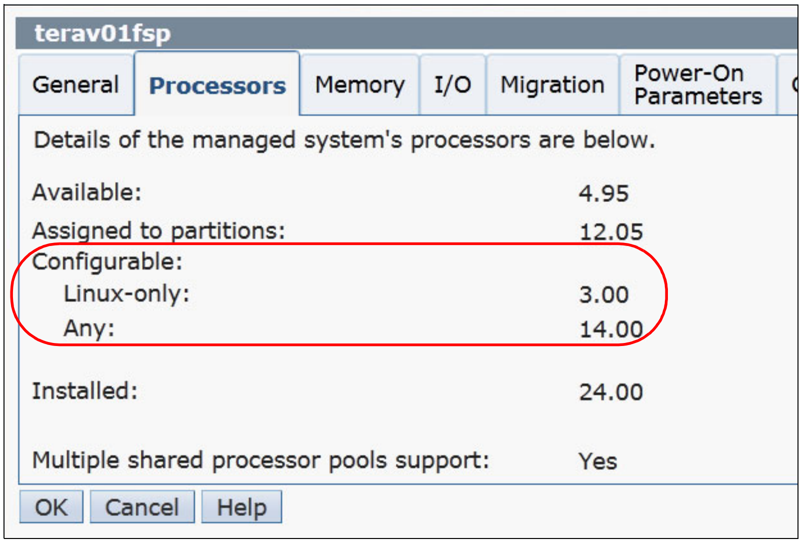
```
lshwres -m <managed system> -r proc --level sys
configurable_sys_proc_units=10.0,curr_avail_sys_proc_units=1.0,pend_avail_sys_proc_units=0.
0,installed_sys_proc_units=16.0,deconfig_sys_proc_units=0,min_proc_units_per_virtual_proc=0
.05,max_virtual_procs_per_lpar=256,max_procs_per_lpar=256,max_curr_virtual_procs_per_aixlin
ux_lpar=64,max_curr_virtual_procs_per_vios_lpar=64,max_curr_virtual_procs_per_os400_lpar=64
,max_curr_procs_per_aixlinux_lpar=64,max_curr_procs_per_vios_lpar=64,max_curr_procs_per_os4
00_lpar=64,max_shared_proc_pools=64,configurable_sys_proc_units_all_os=7.0,configurable_sys
_proc_units_linux=3.0
```

The **configurable_sys_proc_units_linux=3.0** parameter indicates that 3.0 processor cores are configured for Linux only workloads.

Notes:

- An additional **-F** flag is required if the expected values are not shown in the output.
- If **configurable_sys_proc_units_linux** is 0, it is not shown in the default output. It is shown only when **-F** is specified.
- If **configurable_sys_proc_units_all_os = configurable_sys_proc_units**, **configurable_sys_proc_units_all_os** is not shown in the default output, it is shown only when **-F** is specified.
- If the *managed system* does not support Power IFL compliance monitoring, these attributes are invalid.

The updated managed system properties tab now shows the number of Linux only and any operating system processors that are licensed in the system (Figure 1-12).



terav01fsp

Details of the managed system's processors are below.

Available: 4.95

Assigned to partitions: 12.05

Configurable:

Linux-only: 3.00

Any: 14.00

Installed: 24.00

Multiple shared processor pools support: Yes

Figure 1-12 GUI window output to show the Linux only and all OS processors

Compliance monitoring assistance

For certain models of IBM Power Systems servers, the HMC shows a message if the managed system is not in compliance with the Power IFL license terms.

Compliance monitoring assistance is available on the following models with firmware version 7.8.1 or later:

- 9119-FHB
- 9117-MMD
- 9179-MHD

System firmware on supported models periodically computes the actual processor core consumption.

> **Note:** If a determination is made that your system is out of compliance with the processor core license terms, the HMC displays a message every hour. You must be logged in to the HMC GUI to see these messages; otherwise, they are discarded.

On HMC V8.8.1.0 or later, you can see the license configuration for a managed server with Power IFL activations in the HMC server properties Processors tab.

Two categories are listed in the Configurable section:

- Processors that are listed as *Linux only* represent the number of Power IFL processor cores.
- Processors that are listed as *Any* can be used for any (general purpose) workload.

This same information is available in the CoD Processor Capacity Settings window.

Compliance conditions

The system records an entry in the CoD history log when an *out of compliance* condition is first detected.

When the number of out of compliance processor units changes, an A7004735 system reference code (SRC) is logged.

If a system is out of compliance for 24 continuous hours, an A7004736 SRC is logged as a serviceable event.

If you determine that your system is out of compliance, you must correct the problem. Reduce the processor usage of one or more of the running AIX, IBM i, or VIOS partitions on the managed system, reduce processor usage through dynamic partitioning, or shut down or suspend a partition.

1.2.15 Save Area improvements

Starting with HMC V8.8.1.0, many improvements were made in the ability to recover the data in the configuration Save Area. With this improvement, recovery of the Save Area data is possible when corruption occurs on the HMC and service processor and there are no good backups from which to restore.

In previous HMC versions, the recovery consisted of multiple commands, which were available only to Product Engineers, to recover the Save Area configuration. These commands are now combined into the **`mkprofdata`** command.

The **mkprofdata** command also can convert the Save Area data in to an XML file to enable verification of the data before using it for a recovery or restore operation. Previously, this task could be done only by restoring the Save Area data.

The authorization to run the **mkprofdata** command is added to the *hmcpe* and *hmcsuperadmin* task roles.

> **Note:** Use the **mkprofdata** command only when there are no other options and normal operations of recovery is not working.

Re-creating Save Area data configuration from the POWER Hypervisor

If the Save Area data must be re-created, run **mkprofdata** to re-create the Save Area configuration with the following syntax:

```
mkprofdata -r sys - m <System Name> - o recreate -s sys -v
```

> **Note:** This command can be run only when the managed system is in a standby or operating state.

If the Save Area data must be recovered, run **mkprofdata**. The output of a successful recovery is shown in Example 1-10.

Example 1-10 Successful mkprofdata output

```
hscroot@hmc8:~> mkprofdata -r sys -m SystemB -o recreate -s sys -v
 Service processor and management console data backups taken and saved with the
names FSP_1399485387564 , MC_1399485387564
Verification of save area directory objects is complete
Initialization of save area is complete
Execution of recover operation is complete
Update of partition attributes, profiles, and associations is complete
```

Example 1-11 shows where **mkprofdata** recovers only partial data. The output shows that **mkprofdata** successfully recovered only logical partition IDs 1, 2, and 3.

Example 1-11 Partial successful mkprofdata output

```
hscroot@hmc8:~> mkprofdata -r sys -m SystemB -o recreate -s sys -v
 Service processor and management console data backups taken and saved with the
names FSP_1399485387564 , MC_1399485387564
Verification of save area directory objects is complete
Initialization of save area is complete
Execution of recover operation is complete
PartitionId of partially updated Partitions attributes, profiles and associations
are { 1,2,3 }
```

Converting Save Area configuration data from a binary file to XML

The Save Area data is in binary format, and it is difficult to check whether there are consistency issues with the data.The **mkprofdata** command can convert the Save Area data to XML format so that the data that is contained in the Save Area is checked before it is used for a recovery or restore operation. It also checks the consistency of the data because the command generates an error if the data is inconsistent.

To convert the Save Area data to an XML format, run **mkprofdata** with the following syntax:

```
mkprofdata -r sys -o createxml -m <system name> -x <xmlfile name>
```

Example 1-12 shows the conversion of Save Area data to XML format that is saved to the user home directory.

Example 1-12 Convert Save Area data to XML format by using mkprofdata

```
hscroot@hmc8:~>mkprofdata -r sys -o createxml -m SystemA -x 08052014data
hscroot@hmc8:~>ls
08052014data.xml  08052014data_dir.xml  tmp
hscroot@hmc8:~>
```

> **Note:** The **mkprofdata** command also can be run in Power Off condition, regardless of the server connection.

1.2.16 Dynamic Platform Optimizer

The Dynamic Platform Optimizer (DPO) is a PowerVM virtualization feature that is designed to improve partition memory and processor placement (affinity) on Power Servers. The server must be running firmware level 760 or later. DPO determines an optimal resource placement strategy for the server based on partition configuration and hardware topology on the system. It performs memory and processor relocations to transform the existing server layout to the optimal layout. This process occurs dynamically while the partitions are running.

Starting with HMC V8.8.1.0, the HMC v8 added the ability to schedule DPO from the HMC GUI. In earlier HMC versions, DPO was available only on the CLI and had to be run manually.

> **Note:** For a complete explanation about DPO and how to perform DPO from the CLI, see Chapter 15, “Dynamic Platform Optimizer”, of *IBM PowerVM Virtualization Managing and Monitoring*, SG24-7590.

Scheduling DPO from the HMC Enhanced+ Interface

To schedule a DPO task to either start monitoring or to perform DPO from the HMC GUI, complete the following steps:

1. In the navigation pane, click the **Resources** icon, select **All Systems**, select the server and click **Actions** → **Schedule Operations**, as shown in Figure 1-13.

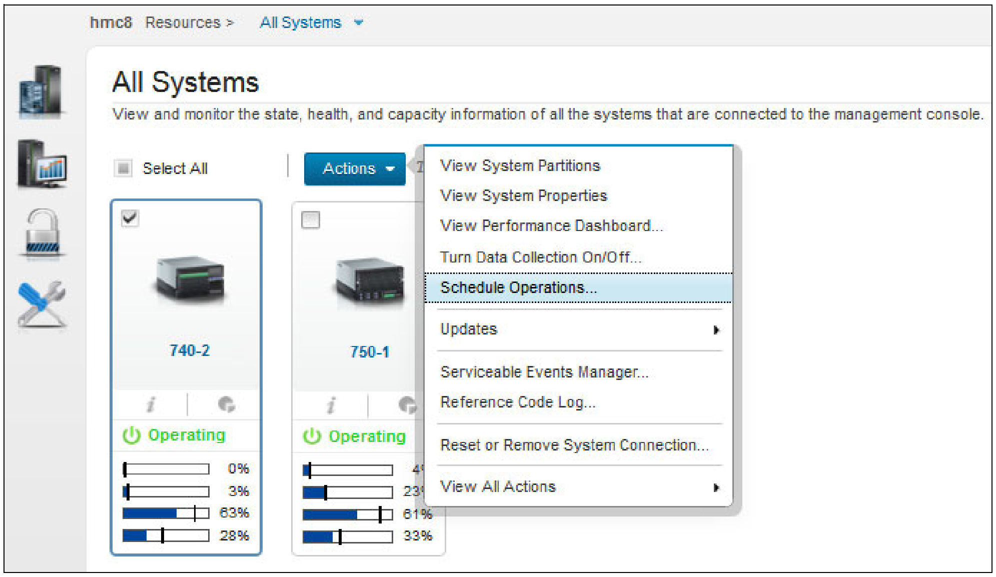

hmc8 Resources > All Systems
All Systems
View and monitor the state, health, and capacity information of all the systems that are connected to the management console.
Select All
Actions
View System Partitions
View System Properties
View Performance Dashboard...
Turn Data Collection On/Off...
Schedule Operations...
Updates
Serviceable Events Manager...
Reference Code Log...
Reset or Remove System Connection...
View All Actions
740-2
750-1
Operating
Operating
0%
3%
63%
28%
61%
33%

Figure 1-13 Schedule operations from the HMC Actions menu

2. Create a schedule in the Customize Scheduled Operations window by clicking **Options** → **New**, as shown in Figure 1-14.

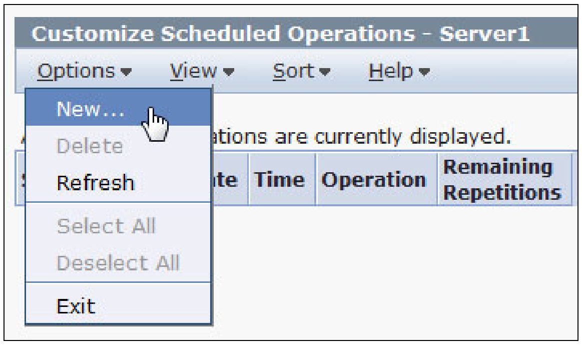
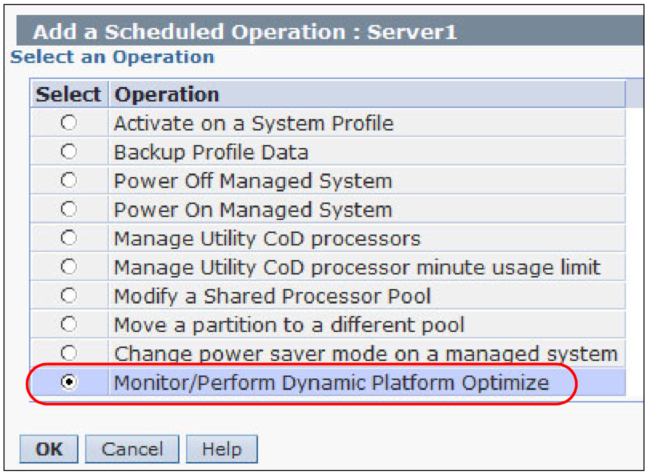


Figure 1-14 Customize Schedule Operations window

3. If the system can perform DPO, a new task, named **Monitor/Perform Dynamic Platform Optimize**, is shown (Figure 1-15). Select that task and then click **OK**.



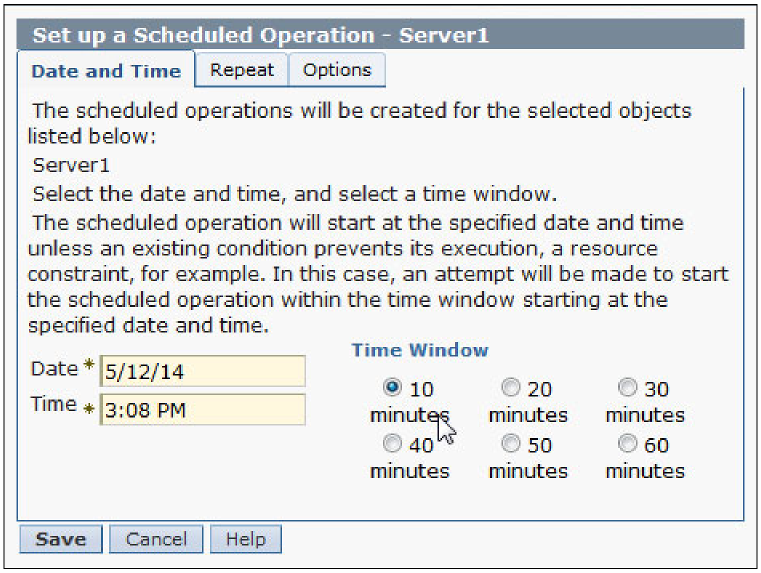
Add a Scheduled Operation : Server1

Select an Operation

Select	Operation
○	Activate on a System Profile
○	Backup Profile Data
○	Power Off Managed System
○	Power On Managed System
○	Manage Utility CoD processors
○	Manage Utility CoD processor minute usage limit
○	Modify a Shared Processor Pool
○	Move a partition to a different pool
○	Change power saver mode on a managed system
●	Monitor/Perform Dynamic Platform Optimize

Figure 1-15 Add a Scheduled Operation window

From the Set up a Scheduled Operation window, you can set up the task (Figure 1-16).



Set up a Scheduled Operation - Server1

The scheduled operations will be created for the selected objects listed below:

Server1

Select the date and time, and select a time window.

The scheduled operation will start at the specified date and time unless an existing condition prevents its execution, a resource constraint, for example. In this case, an attempt will be made to start the scheduled operation within the time window starting at the specified date and time.

Date * 5/12/14

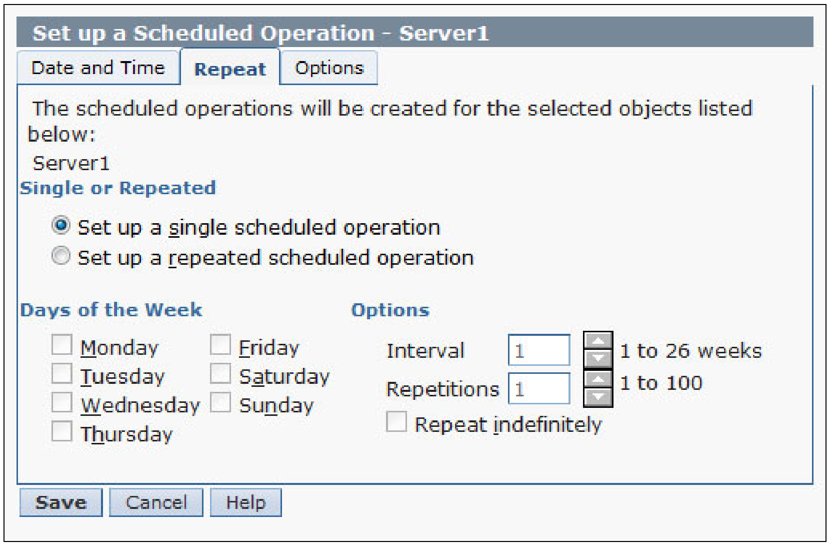
Time * 3:08 PM

Time Window

● 10 minutes ○ 20 minutes ○ 30 minutes
○ 40 minutes ○ 50 minutes ○ 60 minutes

Figure 1-16 Set up a Scheduled Operation task: Date and Time tab

On the Repeat tab (Figure 1-17), you can set repeating operations.



The scheduled operations will be created for the selected objects listed below:

Server1

Single or Repeated

● Set up a single scheduled operation
○ Set up a repeated scheduled operation

Days of the Week

□ Monday	□ Friday
□ Tuesday	□ Saturday
□ Wednesday	□ Sunday
□ Thursday	

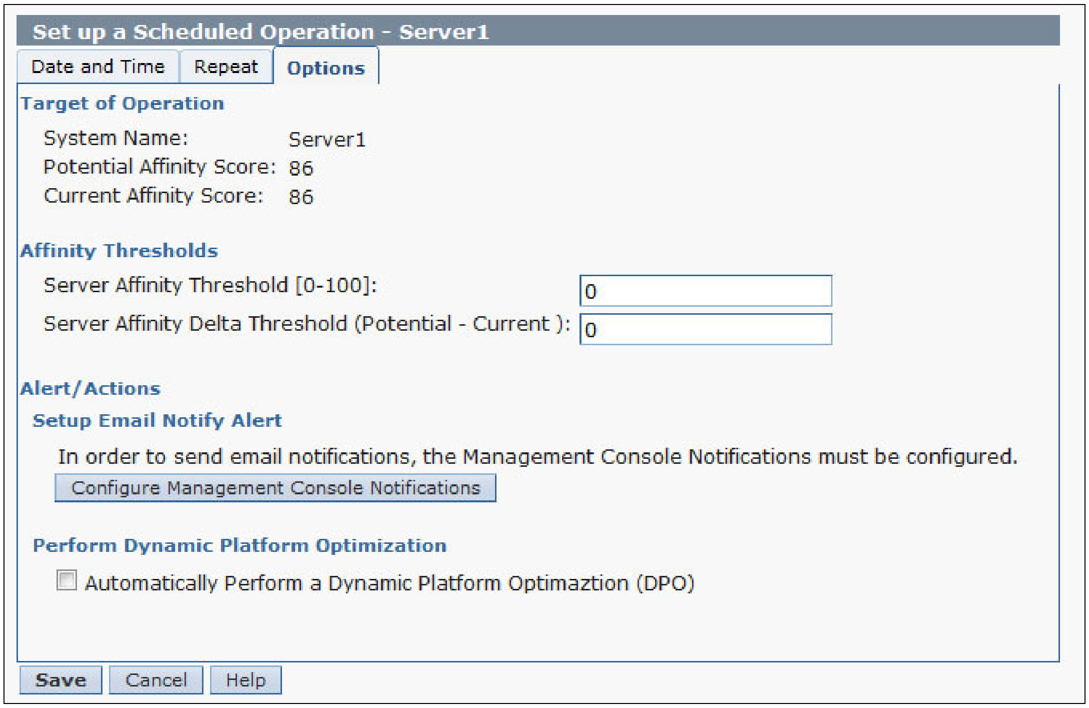
Options

Interval	1	1 to 26 weeks
Repetitions	1	1 to 100

□ Repeat indefinitely

Figure 1-17 Set up a Scheduled Operation task: Repeat tab

On the Operations tab (Figure 1-18), you can configure DPO thresholds, alerts, and actions.


Set up a Scheduled Operation - Server1
Date and Time
Repeat
Options
Configure Management Console Notifications
Save
Cancel
Help

Target of Operation

System Name:	Server1
Potential Affinity Score:	86
Current Affinity Score:	86

Affinity Thresholds

Server Affinity Threshold [0-100]:	0
Server Affinity Delta Threshold (Potential - Current):	0

Alert/Actions

Setup Email Notify Alert

In order to send email notifications, the Management Console Notifications must be configured.

Perform Dynamic Platform Optimization

□ Automatically Perform a Dynamic Platform Optimaztion (DPO)

Figure 1-18 Set up a Scheduled Operation task: Options tab

The Options tab has these sections:

- Target of Operation

  Shows the System name, Potential Affinity Score, and Current Affinity Score.

- Affinity Threshold

  Sets the Server Affinity Threshold and Server Affinity Delta Threshold (Potential-Current).

- Alert/Actions

  Configures a system alert email when the server reaches a certain condition.

- Perform Dynamic Platform Optimization

  Select **Automatically Perform a Dynamic Platform Optimization (DPO)** to perform DPO automatically when Server Affinity Threshold is less than Current Affinity Score, and the server Affinity Delta (Potential Affinity Score minus Current Affinity Score) is greater than the Server Affinity Delta Threshold.

1.2.17 Power Enterprise Pools and the HMC

Each Power Enterprise Pool is managed by a single master HMC. The HMC that is used to create a Power Enterprise Pool is set as the master HMC of that pool. After a Power Enterprise Pool is created, a redundant HMC can be configured as a backup. All Power Enterprise Pool resource assignments must be performed by the master HMC. When powering on or restarting a server, ensure that the server is connected to the master HMC, which ensures that the required Mobile Capacity on Demand resources are assigned to the server.

The maximum number of systems in a Power Enterprise Pool is 32 high-end or 48 mid-range systems. An HMC can manage multiple Power enterprise pools, but is limited to 1000 total partitions. The HMC can also manage systems that are not part of the Power Enterprise Pool. Powering down an HMC does not limit the assigned resources of participating systems in a pool, but does limit the ability to perform pool change operations.

After a Power Enterprise Pool is created, the HMC can be used to do the following functions:

- Mobile Capacity on Demand processor and memory resources can be assigned to systems with inactive resources. Mobile Capacity on Demand resources remain on the system to which they are assigned until they are removed from the system.
- New systems can be added to the pool and existing systems can be removed from the pool.
- New resources can be added to the pool or existing resources can be removed from the pool.
- Pool information can be viewed, including pool resource assignments, compliance, and history logs.

Power Enterprise Pools qualifying machines

To qualify for use of the Power Enterprise Pool offering, a participating system must be one of the following systems:

- IBM Power E880 with POWER8 processors, designated as 9119-MHE
- IBM Power E870 with POWER8 processors, designated as 9119-MME
- IBM Power 795 with POWER7 processors, designated as 9119-FHB
- IBM Power 780 with POWER7+ processors, designated as 9179-MHD
- IBM Power 770 with POWER7+ processors, designated as 9117-MMD

Each system must have installed Machine Code release level 7.8.0, or later, and be configured with at least the minimum amount of permanently active processor cores (listed next). Processor and memory activations that are enabled for movement within the pool will be in addition to these base minimum configurations.

Power Enterprise Pool configuration requirements

The two types of pools are as follows:

- The Power 770 and E870 pools
- The Power 780, 795, and E880 pools

Static requirements are as follows:

- The Power 770 and 780 systems require a minimum of 4 static processor activations.
- The Power 870 and 880 require a minimum of 8 static processor activations.
- The Power 795 requires a minimum of 24 static processor activations.
- For all systems, 50% of memory must be active, and a minimum of 25% of the active memory must be static memory.

All the systems in a pool must be managed by the same HMC or by the same pair of redundant HMCs. If redundant HMCs are used, the HMCs must be connected to a network so that they can communicate with each other. The HMCs must have at least 2 GB of memory.

An HMC can manage multiple Power Enterprise Pool and can also manage systems that are not part of a Power Enterprise Pool. The maximum number of systems an HMC can manage is 32 high-end systems, 48 mid-range, or 48 low-end systems. An HMC can manage a maximum of 1000 total partitions. Systems can belong to only one Power enterprise pool at a time.

Note: Power Enterprise Pools are not available on the IBM Flex System® Manager.

For more details about Power Enterprise Pools, see the following web page:

`https://www.ibm.com/support/knowledgecenter/POWER8/p8ha2/systempool_cod.htm`

For configuration of Power Enterprise Pools, see 5.11.5, “Managing Power Enterprise Pools” on page 418.

1.2.18 The myHMC application

With the myHMC Android or iOS application, you can connect to and monitor managed objects of your HMC. For more information, see Appendix A, “myHMC” on page 553.

1.3 Hardware Models

This section describes the hardware models available for the HMC Version 8.

The HMC Version 8 supports the following HMC machine types:

- 7042-C08
- 7042-CR5
- 7042-CR6
- 7042-CR7
- 7042-CR8
- 7042-CR9

The following illustrations identify each of the machine type 7042 models and show the cable connections located on the back of each HMC model.

Figure 1-19 shows the front view of HMC mode 7042-C08.

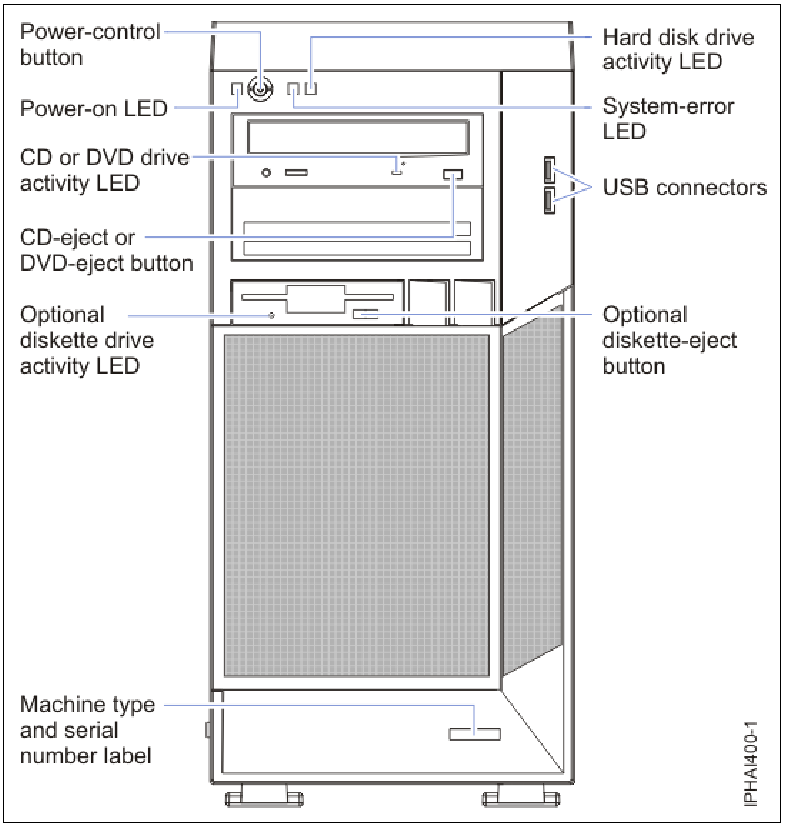

Power-control button
Power-on LED
CD or DVD drive activity LED
CD-eject or DVD-eject button
Optional diskette drive activity LED
Machine type and serial number label
Hard disk drive activity LED
System-error LED
USB connectors
Optional diskette-eject button
IPHAI400-1

Figure 1-19 Model 7042-C08 (front view)

Figure 1-20 shows the front view of Model 7042-CR5.

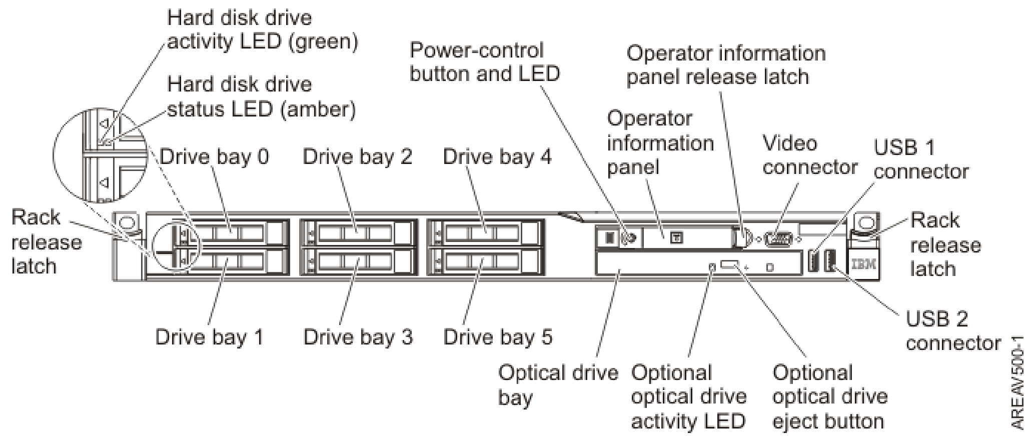

Hard disk drive activity LED (green)
Hard disk drive status LED (amber)
Power-control button and LED
Operator information panel release latch
Operator information panel
Video connector
USB 1 connector
Drive bay 0
Drive bay 2
Drive bay 4
Rack release latch
Rack release latch
Drive bay 1
Drive bay 3
Drive bay 5
USB 2 connector
Optical drive bay
Optional optical drive activity LED
Optional optical drive eject button
AREAV500-1

Figure 1-20 Model 7042-CR5 (front view)

Figure 1-21 shows the front view of Model 7042-CR6.

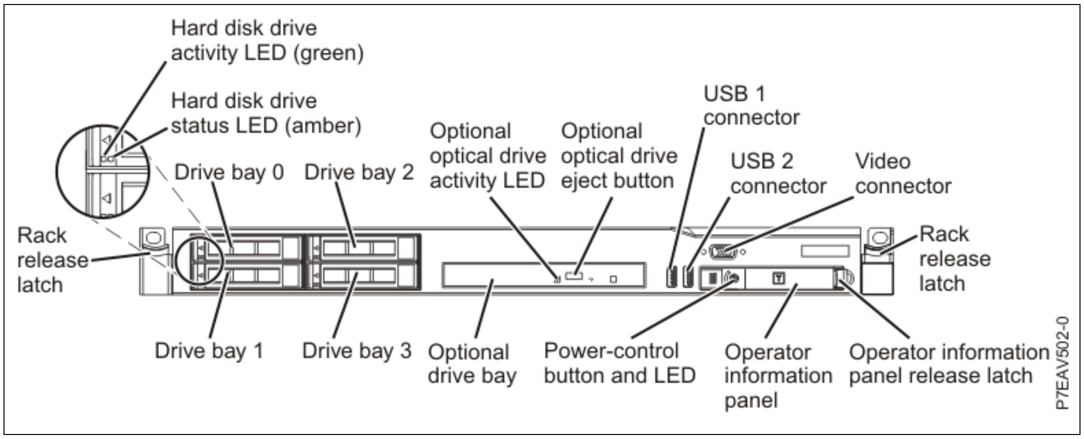

Hard disk drive activity LED (green)
Hard disk drive status LED (amber)
Drive bay 0
Drive bay 2
Optional optical drive activity LED
Optional optical drive eject button
USB 1 connector
USB 2 connector
Video connector
Rack release latch
Rack release latch
Drive bay 1
Drive bay 3
Optional drive bay
Power-control button and LED
Operator information panel
Operator information panel release latch
P7EAV502-0

Figure 1-21 Model 7042-CR6 (front view)

Figure 1-22 shows the front view of Model 7042-CR7 or 7042-CR8 (front view of the server model with a 2.5-inch hard disk drive).

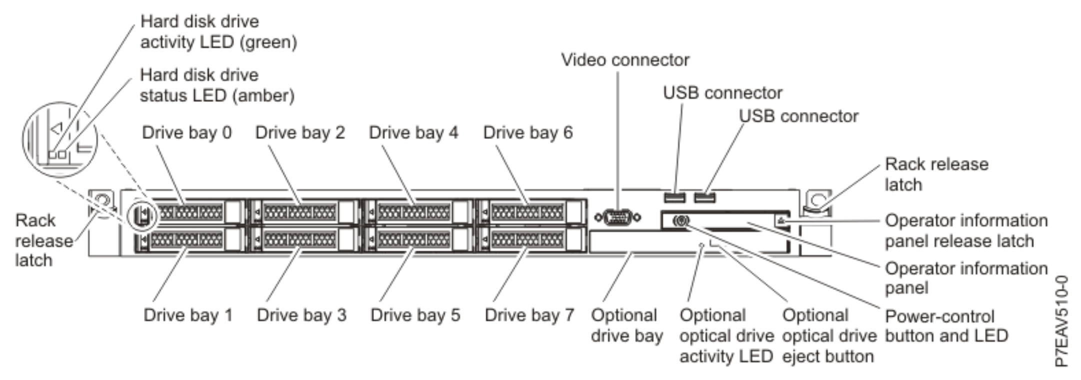

Hard disk drive activity LED (green)
Hard disk drive status LED (amber)
Video connector
USB connector
USB connector
Drive bay 0
Drive bay 2
Drive bay 4
Drive bay 6
Rack release latch
Rack release latch
Operator information panel release latch
Operator information panel
Drive bay 1
Drive bay 3
Drive bay 5
Drive bay 7
Optional drive bay
Optional optical drive activity LED
Optional optical drive eject button
Power-control button and LED
P7EAV510-0

Figure 1-22 Model 7042-CR7 or 7042-CR8 (front view with a 2.5-inch hard disk drive)

Figure 1-23 shows Model 7042-CR7 or 7042-CR8 (front view of the server model with a 3.5-inch hard disk drive).

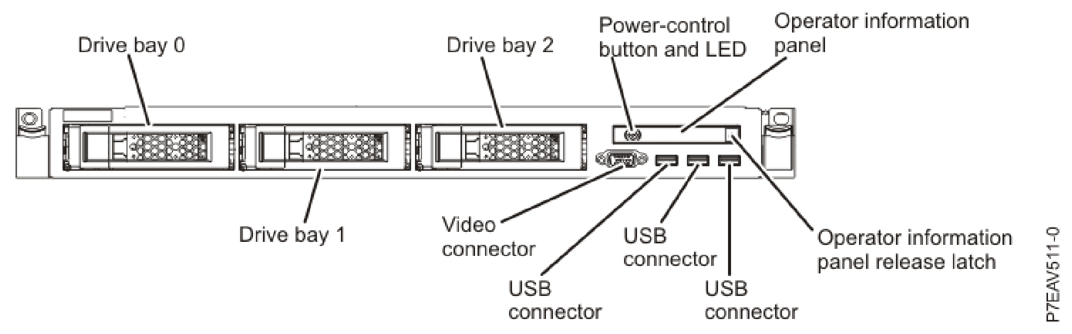


Figure 1-23 Model 7042-CR7 or 7042-CR8 (front view with a 3.5-inch hard disk drive)

Figure 1-24 shows the rear view of Model 7042-CR7 or 7042-CR8.

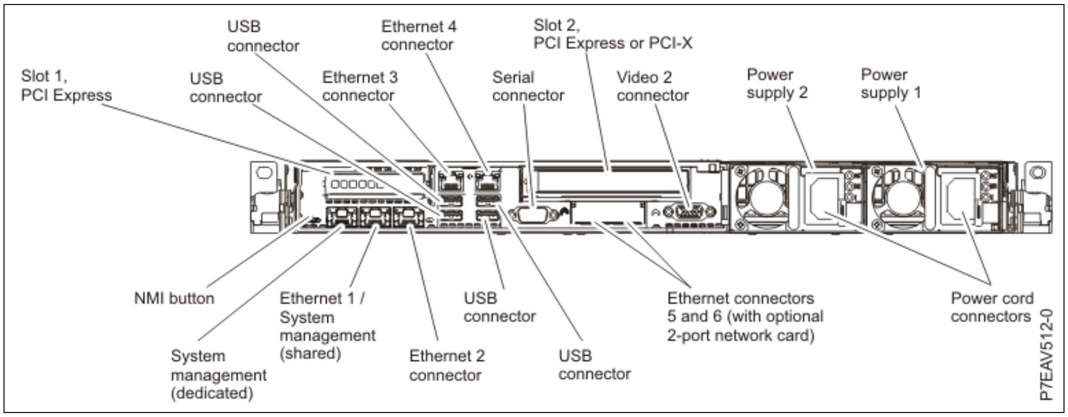


Figure 1-24 Model 7042-CR7 or 7042-CR8 (rear View)

Figure 1-25 shows Model 7042-CR9 (front view of the server model with 2.5-inch hard disk drives).

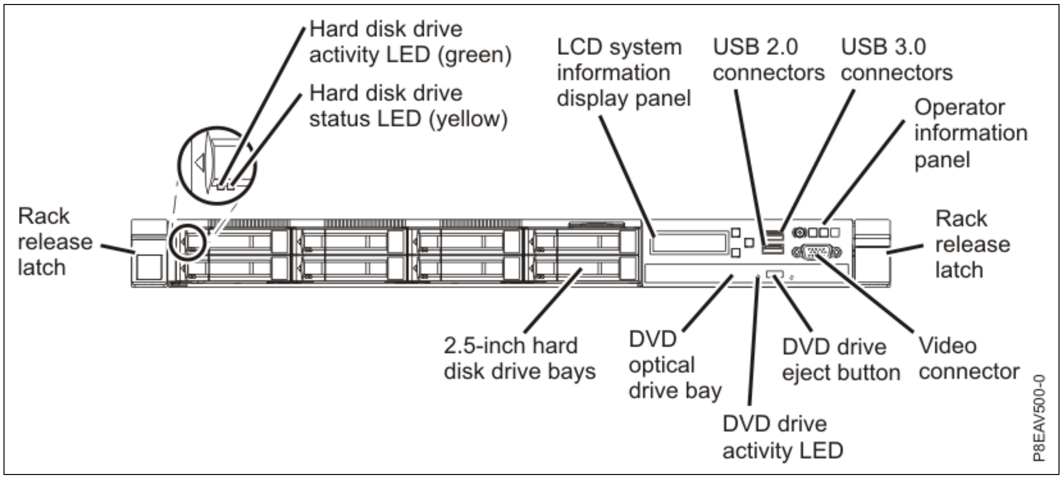

Hard disk drive activity LED (green)
Hard disk drive status LED (yellow)
LCD system information display panel
USB 2.0 connectors
USB 3.0 connectors
Operator information panel
Rack release latch
Rack release latch
2.5-inch hard disk drive bays
DVD optical drive bay
DVD drive eject button
Video connector
DVD drive activity LED
P8EAV500-0

Figure 1-25 Model 7042-CR9 (front view of the server model with 2.5-inch hard disk drives)

Figure 1-26 shows the rear view of Model 7042-CR9.

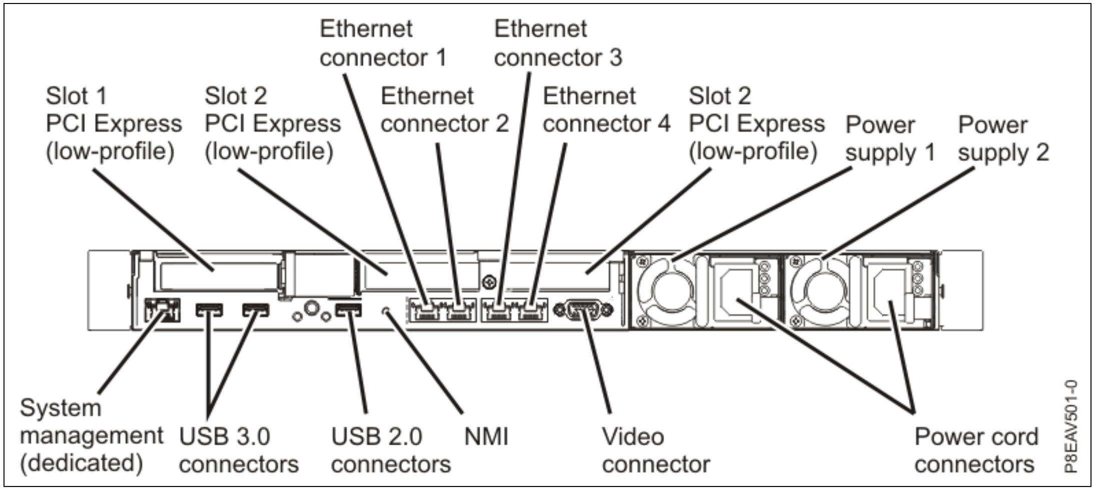


Figure 1-26 Model 7042-CR9 (rear view)

For more details about the Model 7042-CR9, see the following web page:

http://www.ibm.com/common/ssi/printableversion.wss?docURL=/common/ssi/rep_ca/7/897/ENUS115-127/index.html

2

Planning

You can use the Hardware Management Console (HMC) to create import, export, view, create, remove, and deploy system plans and templates. The HMC provides a set of graphical user interfaces (GUIs) for these logical partition (LPAR) management functions. This chapter also describes reliability, availability, and serviceability (RAS) features of the HMC.

This chapter describes the following topics:

- System plans
- What is new in system plans
- System planning tool
- System plans deployment
- System and partition templates
- Partition templates
- Virtualization introduction
- Reliability, availability, and serviceability (RAS) on the HMC

2.1 System plans

A system plan is a specification of the hardware and the logical partitions contained in one or more systems. You can use system plans in various ways that are useful for managing your system. For example, you can use a system plan to create a record of hardware and logical partition configuration data for a system, to create a set of system specifications for ordering a system, or to deploy logical partitions to a system. A system plan is stored in a *systemplan* file, which has a file suffix of sysplan. A systemplan file can contain more than one system plan, although multiple plans in a single file are not common. After you create a system plan, you can also view, delete, and export the system plan.

System plans have a number of valuable uses. For example, you can use system plans to accomplish the following goals:

- Create a system plan as a means of capturing up-to-date system documentation. The system plan provides a record of the hardware and logical partition configuration of the managed system at a given time.
- Use a system plan that you create for system documentation as part of your disaster recovery planning. On the HMC, you can export the systemplan file to an off-site location or to removable media for off-site storage so that you have the system documentation that you need available if you must recover a managed system.

  > **Note:** Although the system plan contains a large amount of system configuration information, it does not contain all the configuration information for a system. Therefore, the system plan is not intended to provide complete system documentation.

- Use system plans as audit records to track system hardware resources for accounting and accountability purposes by exporting the information in them to a spreadsheet.
- Use system plans to help you plan new workloads that require additional system and hardware resources. You can use a system plan, along with appropriate capacity planning information, to make decisions about whether your current system can handle a new workload.
- Create a system plan based on one managed system and deploy the system plan on another system to more quickly and easily create logical partitions on that system.
- Use the System Planning Tool (SPT) to design a managed system based on workload data from your current systems, based on new workloads that you want the managed system to support, based on sample systems that are provided with the utility, or based on your own custom specifications. You can then use the system plan to order a system based on the specifications that the system plan contains. Also, you can use the HMC to deploy the system plan to configure an existing system when the target system meets the requirements for deployment.

Use one of the following methods to create a system plan:

- IBM System Planning Tool (SPT)

  You can create a system plan to capture the configuration of a system or systems that you want to order. A systemplan file created in the SPT can contain more than one system plan, although multiple plans in a single file are not common.

- HMC

  You can create a system plan that documents the configuration of a system that is managed by the HMC.

2.2 What is new in system plans

Read about new or significantly changed information for system plans since the previous update of this topic collection in the following sections.

The system plans topic collection contains information about using the System Planning Tool (SPT) to work with system plans that you create with the HMC.

October 2015

The following updates were made to the content:

- Added references to POWER8 processor-based servers in various topics.
- Removed or updated obsolete information in various topics.

June 2015

The following updates were made to the content:

- Added references to POWER8 processor-based servers in various topics.
- Removed or updated obsolete information in various topics.

November 2014

The following updates were made to the content:

- Removed references to IBM Systems Director Management Console (SDMC).
- Removed or updated obsolete information in various topics.

2.3 System planning tool

The System Planning Tool (SPT) helps you design a managed system that can support a specified set of workloads.

You can design a managed system based on workload data from your current systems, based on new workloads that you want the managed system to support, based on sample systems that are provided with the utility, or based on your own custom specifications. The SPT helps you design a system to fit your needs, whether you want to design a logically partitioned system or want to design an un-partitioned system. SPT incorporates the function from Workload Estimator to help you create an overall system plan. The SPT opens the Workload Estimator to help you gather and integrate workload data, and provides advanced users with the option of creating a system plan without the help of additional tools.

> **Note:** The SPT currently does not help you plan for high availability on logical partitions or Redundant Array of Independent Disks (RAID) solutions.

Several options are available to help you get started with using the SPT:

- You can use the sample system plans that the SPT provides as a starting point for planning your system.
- You can create a system plan based on existing performance data.
- You can create a system plan based on new or anticipated workloads.
- You can create a system plan by using the HMC. You can then use the SPT to convert the system plan to SPT format, and modify the system plan for use in system ordering or system deployment.

- You can copy logical partitions from a system in one system plan to either another system in the same system plan or to a different system in another system plan. For example, you can build up system plans that contain your own sample logical partitions, and then copy one or more of these sample logical partitions into a new system plan that you are creating. You also can copy a logical partition within the same system plan. For example, you can define the attributes of a partition within a system plan and then make seven copies of that partition within the same plan.
- You can export a system plan as a `.cfr` file and import it into the marketing configurator (eConfig) tool to use for ordering a system. When you import the `.cfr` file into the eConfig tool, the tool populates your order with the information from the `.cfr` file. However, the `.cfr` file does not contain all the information that the eConfig tool requires. You will need to enter all required information before you can submit your order.

If you make any changes to the hardware assignments or placement in the system, the SPT validates the changes to ensure that the resulting system fulfills the minimum hardware requirements and hardware placement requirements for the logical partitions.

After you finish making changes to the system, you can save your work as a system plan. You can import this file into your HMC. You then can deploy the system plan to a managed system that the HMC manages. When you deploy the system plan, the HMC creates the logical partitions from the system plan on the managed system that is the target of the deployment.

To download the SPT, see the IBM System Planning Tool website:

http://www.ibm.com/systems/support/tools/systemplanningtool/

2.3.1 System plan conversion

You can convert a systemplan file that you have created by using the HMC into the format that the System Planning Tool (SPT) uses.

Converting a system plan so that you can work with it in the SPT has several benefits:

- You can reconfigure your existing system and validate the changes in SPT before deploying them on your server. For example, you can try adding or moving some parts, or changing the layout of the partitions.
- You can plan an upgrade to a new system. For example, you can move from an IBM Power 570 Model MMA (9117-MMA) POWER6 processor-based server to an IBM Power 770 Model MMB (9117-MMB) POWER7 processor-based server.
- You can move workloads from one system to another. You can even move a partition configuration from one system to another and ensure that the configuration works with the existing hardware.
- You can validate that the configuration on the system is what you want it to be.

To convert a system plan that you created by using the HMC into the SPT format successfully, ensure that you optimize the data that you collect when you create the plan. You must also gather some information to prepare for the conversion and to understand the limitations of the conversion process.

After you complete the conversion process, you can edit the system plan for redeployment of newly added partitions.

For example, assume that you converted an HMC system plan that contains two client logical partitions. You can use the SPT to add another logical partition and specify virtual Ethernet adapters and virtual Small Computer System Interface (vSCSI) adapters for the new partition.

You can then use the HMC to redeploy the changed system plan to configure the new logical partition.

Note: Although you can add partitions, you cannot use SPT to change existing items and redeploy the system plan to the original managed system.

After creating or converting a system plan on the SPT, you can use the HMC to deploy the system plan. However, the SPT must validate this system plan successfully before you can deploy it. The HMC supports deployment only of system plans on which you have created logical partitions and logical partition profiles. It does not support deployment of system plans on which you have modified attributes of existing logical partitions and logical partition profiles. For example, if you use the SPT to add a logical partition and assign unassigned resources to the logical partition, you can deploy the system plan by using the HMC. However, if you use the SPT to move resources from an existing logical partition to a new logical partition, you cannot deploy the system plan by using the HMC.

See 2.4.1, “Deployment validation process” on page 63 for the HMC to learn more about the validation considerations that can affect deployment of the system plan.

2.3.2 Preparing for system plan conversion

Before you convert the system plan to the format that the System Planning Tool (SPT) uses for system plans, you must collect some information to use during the conversion process.

Your original systemplan file remains intact after the conversion. You will not lose any of your data. When you convert your system plan to the format that the SPT uses for system plans, the SPT gives the converted plan a new name and saves it as a new system plan.

Before converting a system plan to the format that the SPT uses for system plans, you must collect some information to use during the conversion process. Some of this information can help with potential conversion limitations. You must gather the following information:

- System attributes

  You must provide the processor, server, and edition features for the system that you want to convert. The SPT Conversion Wizard narrows the options to those options that are valid for the system you are converting, but you must select the correct values from the list of valid options.

- Additional system units

  If your processor feature has multiple system units that support different processor features, select the correct processor feature for each system unit from a list of valid options.

- Backplane

  If the system in the plan that you are converting supports more than one type of backplane, select the backplane that your system uses from a list of valid options.

- Logical partitions

  When you convert your systemplan file to the SPT format, select the logical partitions that you want to include in the converted plan. Thus, you can pick just the logical partitions that you want to work within the SPT. For example, if you are considering moving a particular workload to a new system, you can select just those logical partitions that are used to run that workload and include them in the plan that is converted to the SPT format.

After you know the logical partitions that you want to include, select the profile to associate with each logical partition in the converted plan. The SPT can only associate one profile with a logical partition. For this reason, you might be required to convert your original system plan more than once to work with different views of the data. For example, if you have logical partitions that use one profile during the day and another profile at night, select the logical partitions and profiles that are used at the same time to ensure that your converted system plan has an accurate view of how your system is used.

You also might be required to select the operating system of the logical partition, if that information is unavailable in your original system plan.

- Expansion units

  You must match the enclosures at the top and bottom of any double-high expansion units that are attached to your system. To perform this task, procure the serial numbers of the enclosures at the top and bottom of the double-high expansion unit when you use the wizard.

- Adapters

  You must identify the adapters in each physical location on your system. Based on the vital product data that the system plan contains, the SPT identifies as many adapters as possible. For those adapters that the SPT is unable to identify, the SPT can provide a few possibilities for you to select from. However, if those possibilities are not correct, or if the SPT cannot identify any possibilities, you might be required to provide the Field Replaceable Unit (FRU), Custom Card Identification Number (CCIN), part number, or feature number of the correct adapter. Table 2-1 can help you find the number; look at the physical system or use the operating system commands listed to query and obtain the correct number.

Table 2-1 Operating system commands for identifying adapters

Operating environment	Command	When to use the command
IBM i	DSPHDWRSC	If you have a number of adapters to look up because the command writes the results for multiple adapters to a single output file.
	STRSST	To access the Hardware Resource Manager. By using this command, you can look up information about individual adapters. Use this command if you only have a few numbers to look up.
AIX and Linux	lsslot	If you are trying to obtain information about an adapter in a hot-plug slot. By using this command, you can view all the adapters and integrated hardware for the hot-plug slot so that you can determine the adapter for which you need the number.
	lscfg	If you are trying to obtain information about an adapter that is not in a hot-plug slot, or if you have already used the lsslot command to obtain adapter information for a hot-plug slot.

You can find additional details about how to use these commands in the online help for the SPT Conversion Wizard.

After you finish preparing for the conversion process, export the system plan that you want to convert from the HMC.

2.3.3 Limitations of system plan conversion

You can convert a system plan that you created on the HMC for use in the System Planning Tool (SPT). However, there are some limitations in the data that the SPT can convert.

By setting up your system to optimize the hardware information that you capture when you create a system plan by using the HMC, you can ensure that your system plan provides you with the most valuable information possible. You can also ensure that you have the most usable configuration information possible when you convert the system plan for use in the SPT.

There are some limitations in the data that the SPT can convert at this time. The system plans that you create by using the HMC contain information about the hardware parts that are on your system. To convert one of these plans, the SPT maps the information about the parts back to the features that represent those parts.

In some cases, the HMC systemplans do not contain enough information for the SPT to do the necessary mapping conclusively. For hardware parts with inconclusive mapping information, the SPT performs one of the following actions to resolve the inconclusive mapping:

- When possible, the SPT Conversion Wizard prompts you for additional information about the parts during the conversion process. For example, in the case of PCI cards, the wizard prompts you to provide a part identifier for the card or to select the card from a list.
- The wizard identifies the part based on what it knows from the HMC system plan, even if the information is not conclusive.
- The wizard disregards the part if the level of information in the plan is insufficient to do any kind of identification.

Table 2-2 shows several examples of parts or configurations that are more difficult to convert and what SPT does when it encounters them.

Table 2-2 Conversion examples

Part or configuration	SPT action during conversion
Logical partitions with more than one partition profile	SPT can only convert one profile per logical partition. SPT prompts you to select the profile you want to use for that partition during the conversion process.
Cards that are referred to by more than one partition profile	SPT assigns the card to the first profile it encounters that references the card and discards all other references to the card.
CD, DVD, or optical storage	SPT does not convert these devices.
Disk drives in a Redundant Array of Independent Disks (RAID) array	SPT does not convert any information about these drives.

Table 2-3 on page 52 lists the type of hardware information that you can expect to see in a system plan that you convert to SPT format. The type of information that you can expect is based on the management tool that you use to create the plan and the types of logical partitions in the system plan.

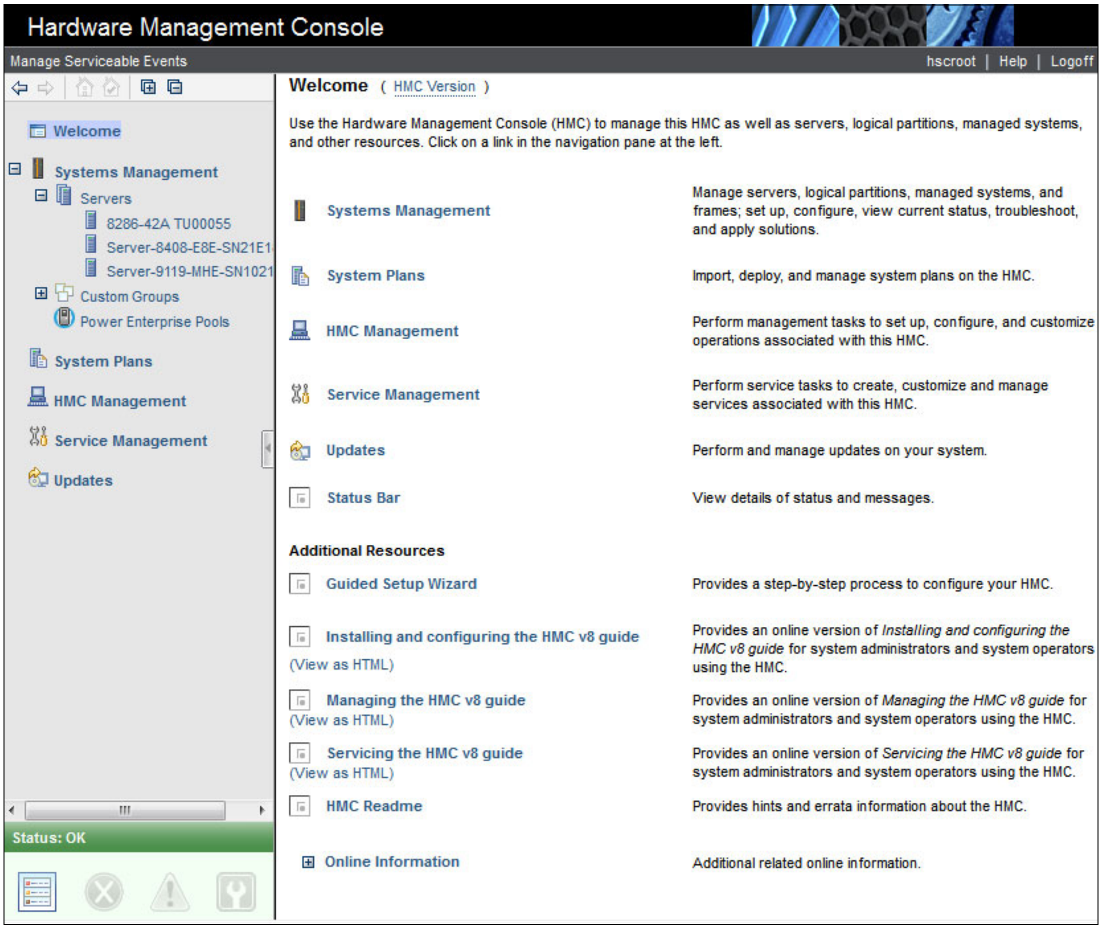
Table 2-3 Hardware information captured in SPT based on management tool and LPARs

Management tool	**POWER8 processors**	
	IBM i	**All other operating environments**
HMC Version 8 Release 8.4.0 (when you optimize data collection for the system plan)	Most cards. All disk drives.	Most cards. Most disk drives.

2.3.4 Work with system plans in the HMC

In the HMC workplace window, *System Plans* is where you can access the graphical interfaces that you use to manage system plans on the servers directly from the HMC or remotely by using the web-browser based client connecting to the HMC (Figure 2-1).

Note: This task is only available on the HMC by using the HMC Classic graphical user interface (GUI).



Welcome (HMC Version)

Use the Hardware Management Console (HMC) to manage this HMC as well as servers, logical partitions, managed systems, and other resources. Click on a link in the navigation pane at the left.

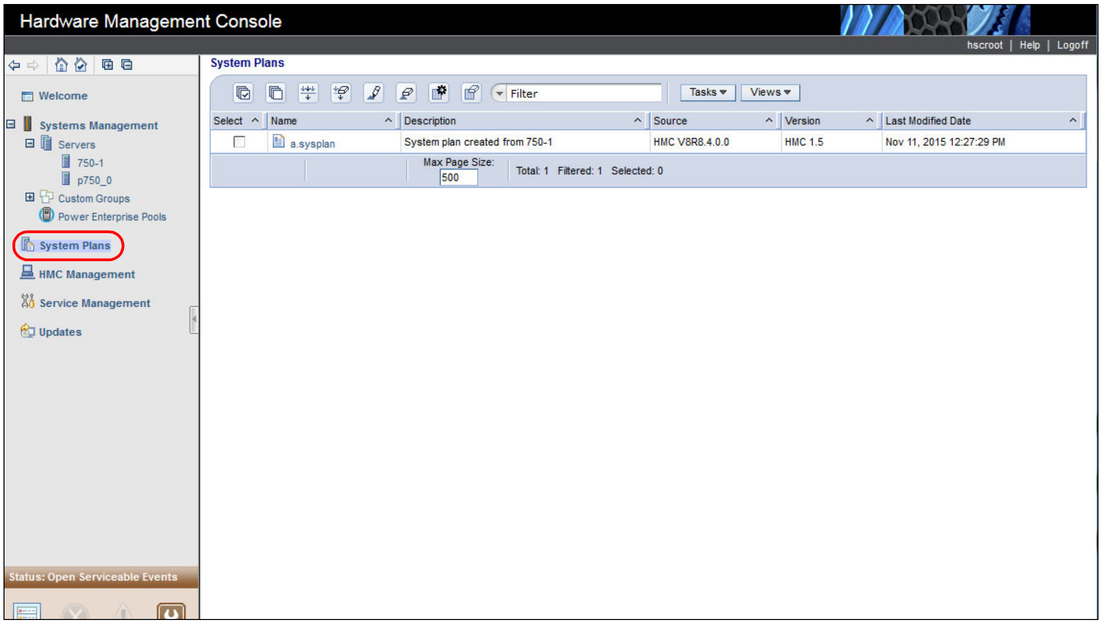
Systems Management	Manage servers, logical partitions, managed systems, and frames; set up, configure, view current status, troubleshoot, and apply solutions.
System Plans	Import, deploy, and manage system plans on the HMC.
HMC Management	Perform management tasks to set up, configure, and customize operations associated with this HMC.
Service Management	Perform service tasks to create, customize and manage services associated with this HMC.
Updates	Perform and manage updates on your system.
Status Bar	View details of status and messages.

Additional Resources

Guided Setup Wizard	Provides a step-by-step process to configure your HMC.
Installing and configuring the HMC v8 guide (View as HTML)	Provides an online version of *Installing and configuring the HMC v8 guide* for system administrators and system operators using the HMC.
Managing the HMC v8 guide (View as HTML)	Provides an online version of *Managing the HMC v8 guide* for system administrators and system operators using the HMC.
Servicing the HMC v8 guide (View as HTML)	Provides an online version of *Servicing the HMC v8 guide* for system administrators and system operators using the HMC.
HMC Readme	Provides hints and errata information about the HMC.
⊞ Online Information	Additional related online information.

Figure 2-1 The HMC Welcome page: System Plans

To display the system plans management tasks window, click **System Plans** (Figure 2-2). The upper section of this window lists all the system plans currently on the HMC. Use the icons above the list to select and clear, sort, filter, and manage the columns of the display table, and perform tasks on selected system plans. The task options are repeated in the lower *tasks* section of the main system plans management window. With no system plan selected, the only options are to import a system plan or to create a system plan.



Select	Name	Description	Source	Version	Last Modified Date
□	a.sysplan	System plan created from 750-1	HMC V8R8.4.0.0	HMC 1.5	Nov 11, 2015 12:27:29 PM

Max Page Size: 500   Total: 1 Filtered: 1 Selected: 0

Figure 2-2 The main system plan management page

Using the HMC, you can do the following actions:

- Create a system plan
- View a system plan
- Deploy a system plan
- Export a system plan
- Import a system plan
- Remove a system plan

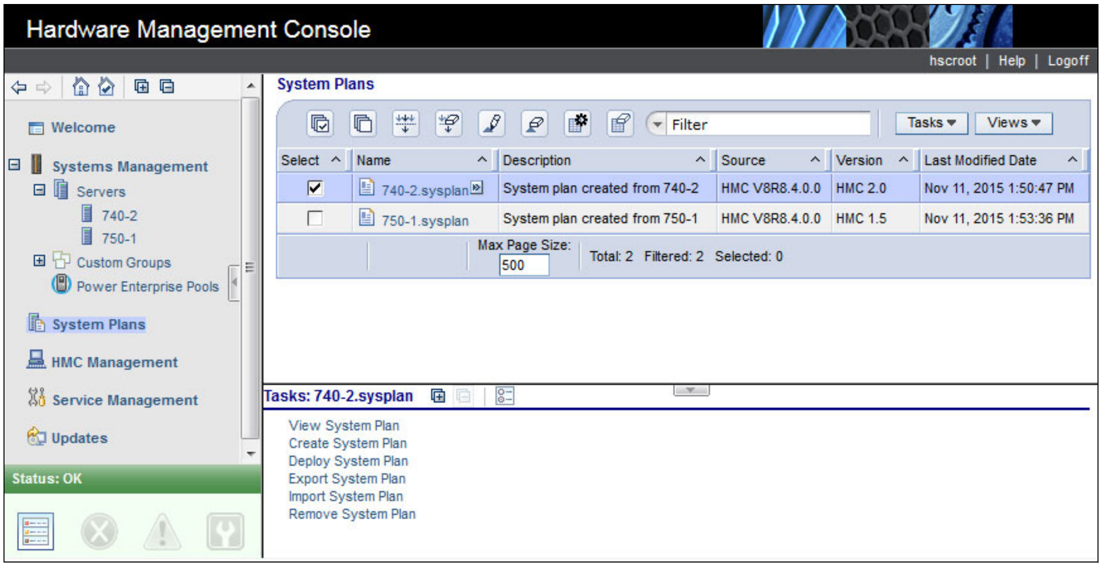
You can save a system plan that is created by using the HMC interface as a record of the hardware and partition configuration of the managed system at a specified time.

You can deploy an existing system plan to other systems that this HMC manages that have hardware that is identical to the hardware in the system plan.

You can export a system plan to another HMC (which imports the plan). You can then use it to deploy the system plan to other systems that the target HMC manages that have hardware that is identical to the hardware in the system plan.

You can view, create, deploy, export, import, or remove a system plan. These tasks can be selected in either the Tasks menu or the Tasks links in the lower part of the right frame. The following sections provide more details for each option.

Figure 2-3 shows a common starting point for each example. In the first example, a system plan named `740-2.sysplan` is selected.



System Plans

Select	Name	Description	Source	Version	Last Modified Date
☑	740-2.sysplan	System plan created from 740-2	HMC V8R8.4.0.0	HMC 2.0	Nov 11, 2015 1:50:47 PM
□	750-1.sysplan	System plan created from 750-1	HMC V8R8.4.0.0	HMC 1.5	Nov 11, 2015 1:53:36 PM

Max Page Size: 500   Total: 2 Filtered: 2 Selected: 0

Tasks: 740-2.sysplan

- View System Plan
- Create System Plan
- Deploy System Plan
- Export System Plan
- Import System Plan
- Remove System Plan

Figure 2-3 The system plan management page with a system plan selected

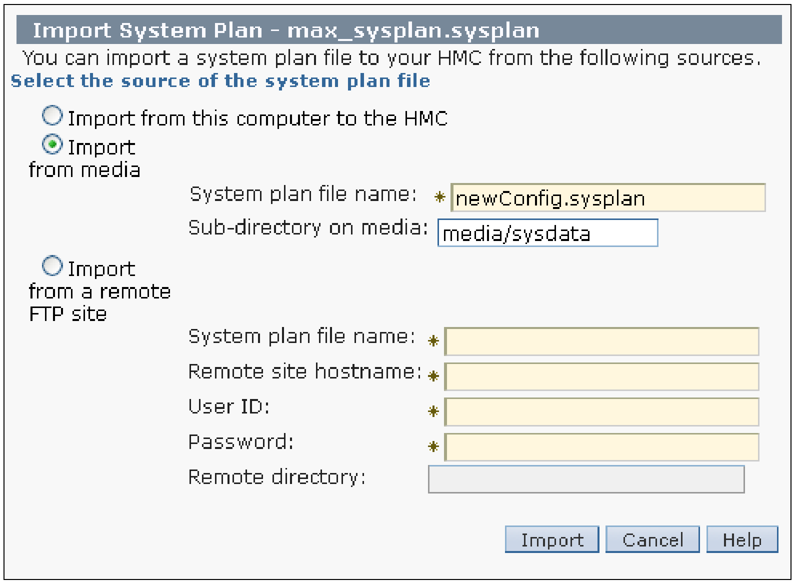
2.3.5 Importing a system plan to the HMC

You can load a system plan that was created by using the SPT or created on another HMC by using the import operation. You can import the system plan from one of the supported media types. Types include CD, DVD, or a USB device such as a memory card, a remote FTP site, or a PC connected to the HMC through a browser connection.

When you import a system plan, you first must prepare the media, if needed. Then, you import the sysplan file.

From the System Plans task menu, select **Import System Plan**, which opens the Import System Plan prompt window. Identify the system plan file name and whether you are importing it from media, an FTP server, or, if you are accessing the HMC through a PC-based web browser, the sysplan file can be on that PC.

In the example (Figure 2-4), the system plan file is stored on a USB flash drive. The name of the file is `newConfig.sysplan`, and the file was initially created by using SPT and saved to the flash drive. The directory path to access the file on the flash drive is `/media/sysdata`.



Import System Plan - max_sysplan.sysplan

You can import a system plan file to your HMC from the following sources.

Select the source of the system plan file

○ Import from this computer to the HMC

● Import from media

System plan file name: * newConfig.sysplan

Sub-directory on media: media/sysdata

○ Import from a remote FTP site

System plan file name: *

Remote site hostname: *

User ID: *

Password: *

Remote directory:

Figure 2-4 Import System Plan window

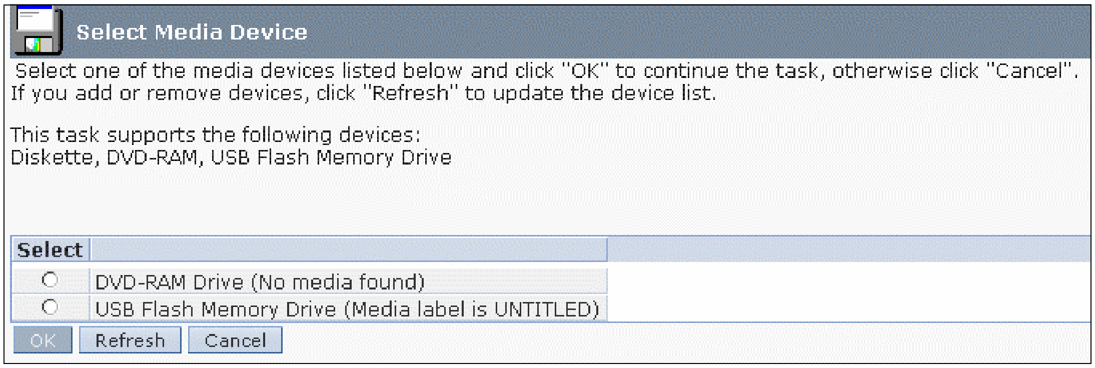
2.3.6 Exporting a system plan from the HMC

You can export system plans that are on the HMC to media, an FTP server, or, if you are using a PC to access the HMC through a browser, to a directory on the PC. The process is much like the importing of a sysplan file. If you are exporting to media, you must format that media for use with the HMC.

Preparing the media

To export to external media, that media must be in a format that is available to the HMC. The easiest method is to use the Format Removable Media task:

1. Select **HMC Management** from the left navigation frame.
2. Select **Format Media** in the right window to open the media selection box (Figure 2-5).



Select Media Device

Select one of the media devices listed below and click "OK" to continue the task, otherwise click "Cancel". If you add or remove devices, click "Refresh" to update the device list.

This task supports the following devices:
Diskette, DVD-RAM, USB Flash Memory Drive

Select	
○	DVD-RAM Drive (No media found)
○	USB Flash Memory Drive (Media label is UNTITLED)

Figure 2-5 Format media

If you have a USB memory key, insert it in a USB slot on the HMC.

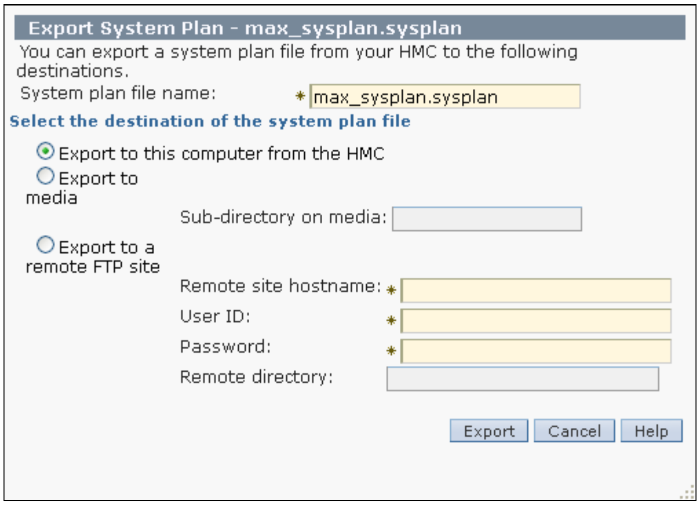
If you have a diskette or CD that must be formatted, insert it into the disk or CD drive.

3. Select the correct device to format and click **OK**. The memory format process starts and completes.
4. Insert the media into the PC and load the system plan file by using the save function in SPT or by browsing to the file and copying the sysplan file to the media.

Exporting the system plan

To export a system plan, complete the following steps:

1. Select a system plan to export.
2. Click **Export System Plan** either from the Tasks menu or the content Tasks link in the lower portion of the window. A dialog box opens asking where you want to export the system plan (Figure 2-6). In our example, the name of the sysplan file is `max_sysplan.sysplan` and the target is to `local computer` directory.



Export System Plan - max_sysplan.sysplan

You can export a system plan file from your HMC to the following destinations.

System plan file name: * max_sysplan.sysplan

Select the destination of the system plan file

● Export to this computer from the HMC

○ Export to media

Sub-directory on media:

○ Export to a remote FTP site

Remote site hostname: *

User ID: *

Password: *

Remote directory:

Figure 2-6 Export System Plan window

3. Click **Export** to initiate the export process. A results window with a success indication or an error message indicates the result of the export.

2.3.7 Creating a system plan on the HMC

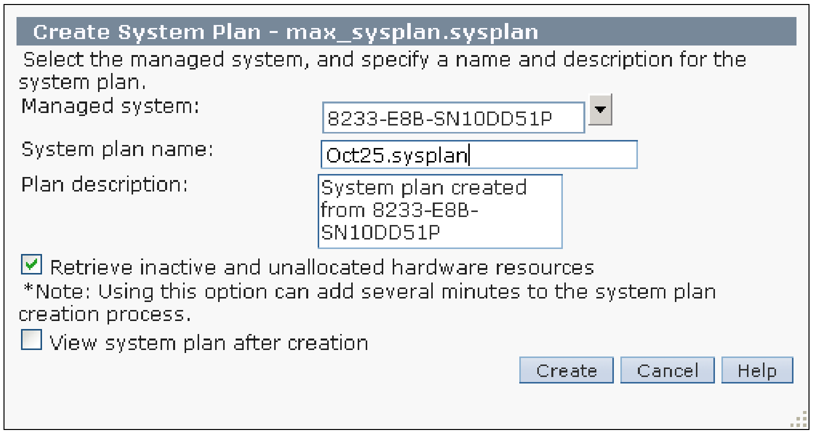
You can create a system plan for a system that is controlled by the HMC. The system plan has information about the current partition definitions and hardware allocations. Processor, memory, and PCI cards are identified in the system plan, even if they are not owned by a partition.

Notes:

- Hardware that is controlled through an input/output adapter controller (IOA), such as disk units and external media devices, is not represented in the system plan unless the owning partition is running.
- You cannot import the sysplan file that the HMC creates into the SPT to edit it. The sysplan file can be only deployed and viewed either on the HMC on which the file was created or an HMC to which the file was moved.

From the starting point, shown in Figure 2-3, follow these steps:

1. Select **Create System Plan**.
2. The Create System Plan window prompts you for the system name, sysplan file name, a description, and a choice to view the system plan after creation, as shown in Figure 2-7.



Create System Plan - max_sysplan.sysplan

Select the managed system, and specify a name and description for the system plan.

Managed system: 8233-E8B-SN10DD51P

System plan name: Oct25.sysplan

Plan description: System plan created from 8233-E8B-SN10DD51P

☑ Retrieve inactive and unallocated hardware resources

*Note: Using this option can add several minutes to the system plan creation process.

☐ View system plan after creation

Figure 2-7 Create System Plan window

3. After you enter the requested information, click **Create**.
4. Following the successful creation of a system plan, a message displays and the system plan is now in the list of plans on the HMC. Click **OK**.

Enabling hardware inventory collection from active partitions

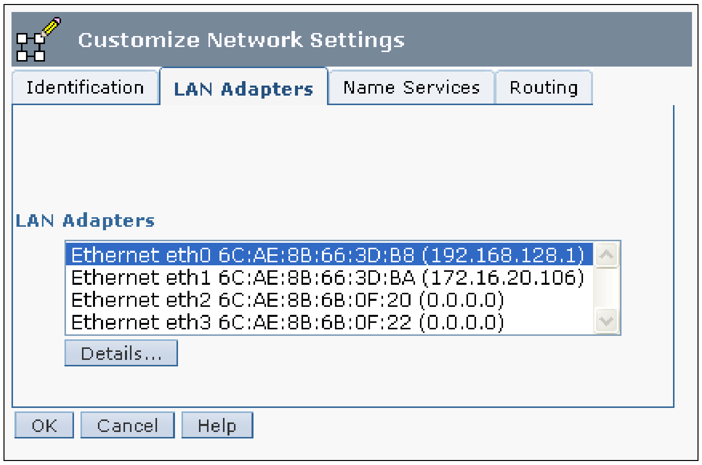
When you use the HMC to create a system plan for a managed system, you can capture partition configuration information and a base set of associated hardware configuration information. If you have partitions already active, you can maximize the information that the HMC can obtain about the hardware.

To maximize the information that the HMC can obtain from the managed system, turn on the managed system and activate the logical partitions on the managed system, assuming that they exist, before you create the system plan.

Additionally, you must set up Resource Monitoring and Control (RMC) on the HMC before you create a system plan to capture the most detailed information. Although using the RMC can take several more minutes to finish processing, you can capture disk drive and tape drive configuration information for a managed system in the system plan. You can view this more detailed hardware information by using the View System Plan task.

To enable the HMC's internal inventory collection tool (`invscout`) to be able to do its most detailed hardware inventory retrieval operations, follow these steps:

1. In the HMC workplace window, select the HMC Management task.
2. Select **Change Network Settings**, and in the Customize Network Settings window, select the LAN Adapters tab, as shown in Figure 2-8.

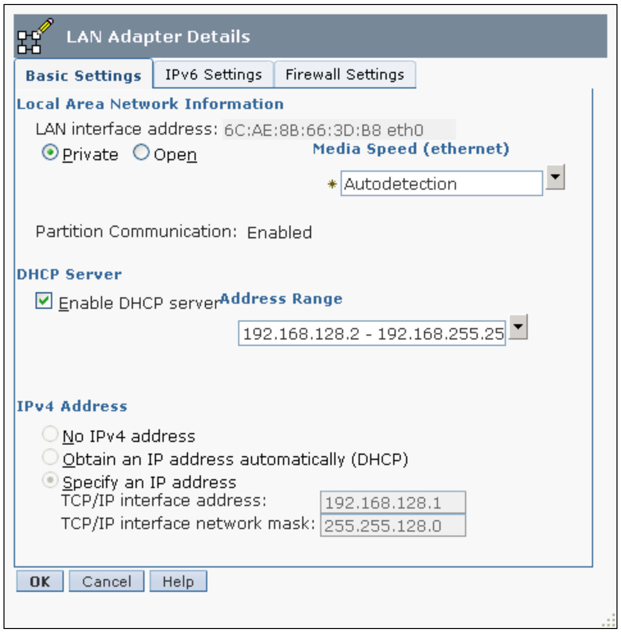


LAN Adapters

```
Ethernet eth0 6C:AE:8B:66:3D:B8 (192.168.128.1)
Ethernet eth1 6C:AE:8B:66:3D:BA (172.16.20.106)
Ethernet eth2 6C:AE:8B:6B:0F:20 (0.0.0.0)
Ethernet eth3 6C:AE:8B:6B:0F:22 (0.0.0.0)
```

Figure 2-8 Customize Network Setting: LAN Adapters tab

3. In the LAN Adapters window, select the **eth0** LAN Adapter and click **Details**.
4. In the LAN Adapter Details window (Figure 2-9) on the LAN Adapter tab, select **Open** within the local area network information area to enable the check box for Partition Communication. Then, select **Partition communication**.



Local Area Network Information

LAN interface address: 6C:AE:8B:66:3D:B8 eth0

● Private ○ Open

Media Speed (ethernet)

Autodetection

Partition Communication: Enabled

DHCP Server

☑ Enable DHCP server

Address Range

192.168.128.2 - 192.168.255.25

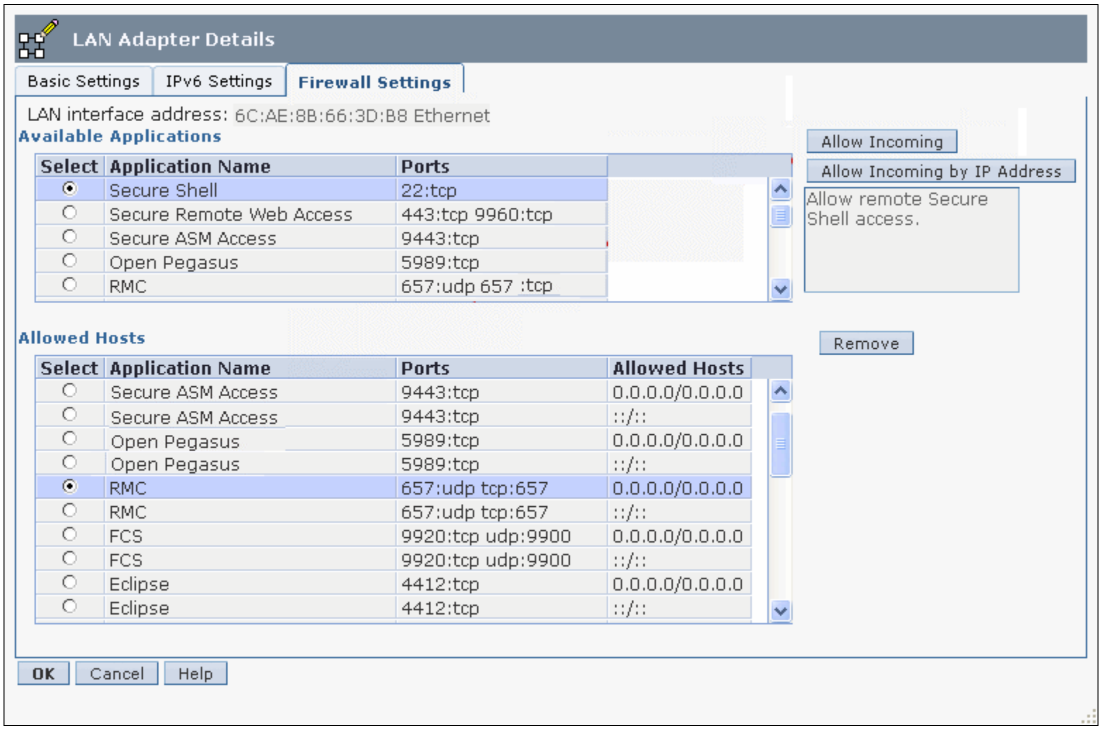
IPv4 Address

○ No IPv4 address
○ Obtain an IP address automatically (DHCP)
● Specify an IP address

TCP/IP interface address: 192.168.128.1
TCP/IP interface network mask: 255.255.128.0

Figure 2-9 Customize Network Setting for LAN Adapters: Partition communication

5. Click the **Firewall Settings** tab (Figure 2-10), scroll to the Available Applications area to see whether RMC is already specified as available. The assumption for this example is that RMC is not yet available. Therefore, select **RMC** in the Allowed Hosts pane and click **Allow Incoming**. This action moves RMC into the Available Applications pane.



LAN interface address: 6C:AE:8B:66:3D:B8 Ethernet

Available Applications

Select	Application Name	Ports
●	Secure Shell	22:tcp
○	Secure Remote Web Access	443:tcp 9960:tcp
○	Secure ASM Access	9443:tcp
○	Open Pegasus	5989:tcp
○	RMC	657:udp 657 :tcp

Allow remote Secure Shell access.

Allowed Hosts

Select	Application Name	Ports	Allowed Hosts
○	Secure ASM Access	9443:tcp	0.0.0.0/0.0.0.0
○	Secure ASM Access	9443:tcp	::/::
○	Open Pegasus	5989:tcp	0.0.0.0/0.0.0.0
○	Open Pegasus	5989:tcp	::/::
●	RMC	657:udp tcp:657	0.0.0.0/0.0.0.0
○	RMC	657:udp tcp:657	::/::
○	FCS	9920:tcp udp:9900	0.0.0.0/0.0.0.0
○	FCS	9920:tcp udp:9900	::/::
○	Eclipse	4412:tcp	0.0.0.0/0.0.0.0
○	Eclipse	4412:tcp	::/::

Figure 2-10 Customize Network Setting for LAN Adapters: RMC application

6. Click **OK** twice to open a window that states that the Network Settings Changes are applied at the next HMC.
7. Click **OK**. You are now back to the HMC workplace window with just the HMC Management pane on the right.

You can verify that you enabled RMC successfully by using the **`lspartition`** command on the HMC CLI.

The list partition command has this syntax:

```
lspartition -c
```

This is an example:

```
hmc:> lspartition -c 9117_MTM-10FZZD
```

The example managed system has the following results:

```
<#0> Partition:<4, partn1.business.com, 1.2.3.444>
   Active:<0>, OS<, >
```

If this command does not return any partitions, the system might not be set up for RMC. Depending on whether the system is a Power Systems server, IBM System i®, or System p, the steps for RMC are different.

IBM Systems Hardware Information Center includes more information about RMC. For background information about RMC, also see *A Practical Guide for Resource Monitoring and Control (RMC)*, SG24-6615. The content of this publication is based on IBM AIX 5L™ V5.1.

If the Create System plan from the GUI fails and if there is a need to create a system plan, use the underlying **mksysplan** CLI at the HMC command prompt, with the **noprobe** option. The **noprobe** option bypasses the default inventory collection of active partitions. Therefore, the resulting sysplan might not have IOA or IOP controlled disk units or media enclosures.

Here is an example:

```
hmc:> mksysplan -m machineName -f filename.sysplan -v -o noprobe
```

When creating a sysplan, if a failure occurs because of a Virtual I/O Server (VIOS) error, you can try the **noprobe** option from the CLI.

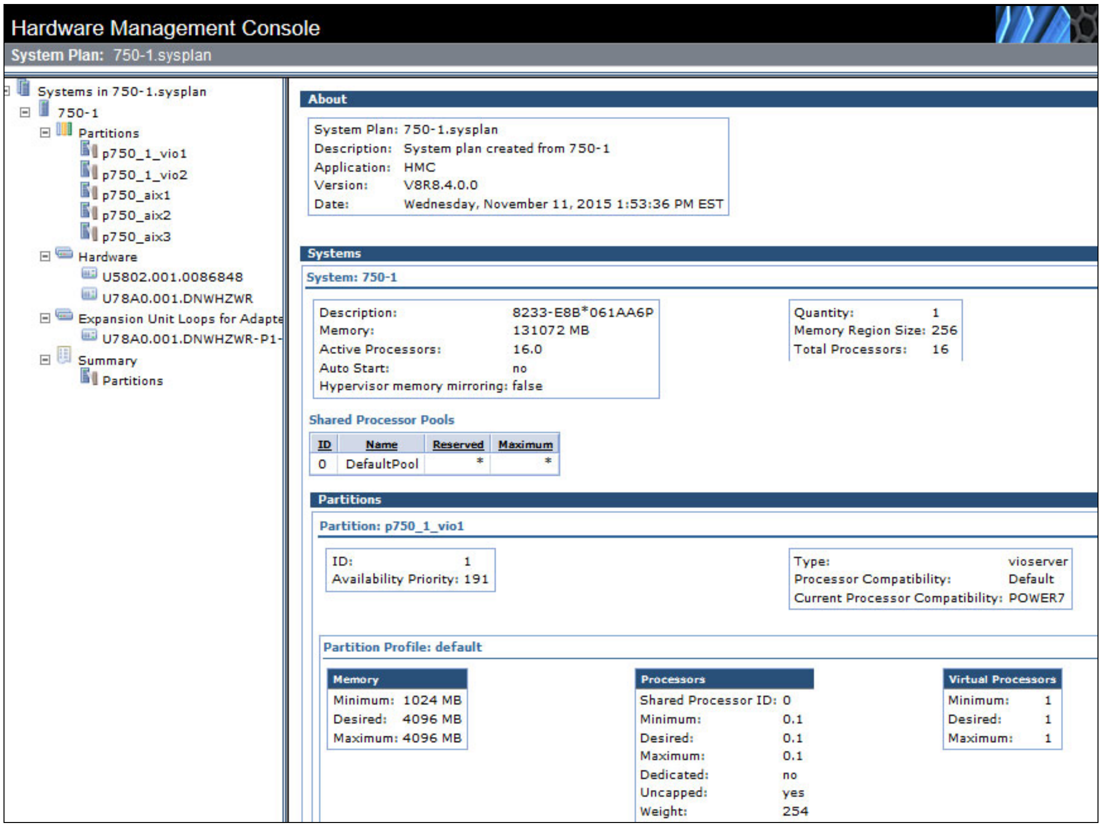
2.3.8 Viewing a system plan on the HMC

The HMC has a system plan viewer similar to the viewer in the System Planning Tool. The viewer offers a non-editable presentation of the partitions and hardware of the system. Using Figure 2-3 on page 54 as a starting point, select the a plan in the main system plan management window. Click **View System Plan**.

When accessing the HMC remotely, you are presented with a View System Plan sign-on window the first time that you start the System Plan Viewer. This additional login protects unauthorized users from viewing the configuration of the system. It also prevents starting the viewer from bookmarks without providing an appropriate user name and password.

Figure 2-11 on page 61 shows the system plan. The left navigation frame shows a single partition or the entire system. You can also choose just specific enclosures under the Hardware section. The file history is also viewable. The viewer also has a Print option and Show Comments / Hide Comments toggle, which is at the bottom of the viewer window.

If you access the HMC from a PC browser, the print function is through the attached network printers of the PC. If you are using the HMC terminal, the print function is through printers that are connected to the HMC or network printers to which the HMC has access.



```
Systems in 750-1.sysplan
  750-1
    Partitions
      p750_1_vio1
      p750_1_vio2
      p750_aix1
      p750_aix2
      p750_aix3
    Hardware
      U5802.001.0086848
      U78A0.001.DNWHZWR
    Expansion Unit Loops for Adapte
      U78A0.001.DNWHZWR-P1-
    Summary
      Partitions
```

About

System Plan: 750-1.sysplan
Description: System plan created from 750-1
Application: HMC
Version: V8R8.4.0.0
Date: Wednesday, November 11, 2015 1:53:36 PM EST

Systems

System: 750-1

Description: 8233-E8B*061AA6P
Memory: 131072 MB
Active Processors: 16.0
Auto Start: no
Hypervisor memory mirroring: false

Quantity: 1
Memory Region Size: 256
Total Processors: 16

Shared Processor Pools

ID	Name	Reserved	Maximum
0	DefaultPool	*	*

Partitions

Partition: p750_1_vio1

ID: 1
Availability Priority: 191

Type: vioserver
Processor Compatibility: Default
Current Processor Compatibility: POWER7

Partition Profile: default

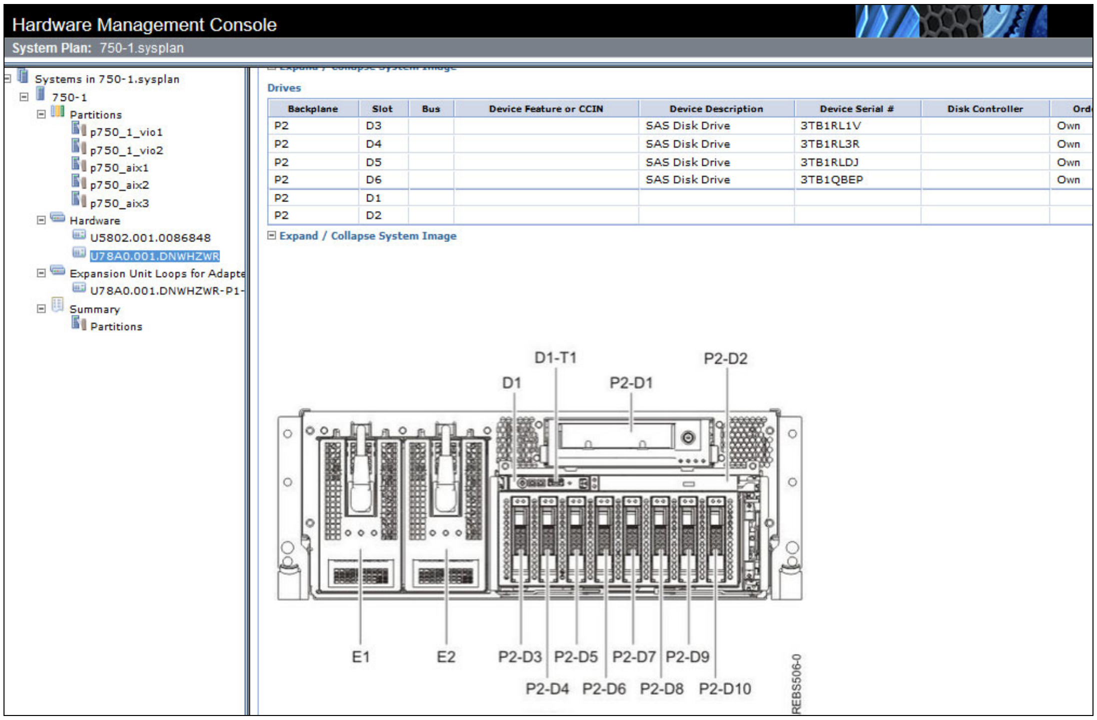
Memory
Minimum: 1024 MB
Desired: 4096 MB
Maximum: 4096 MB

Processors
Shared Processor ID: 0
Minimum: 0.1
Desired: 0.1
Maximum: 0.1
Dedicated: no
Uncapped: yes
Weight: 254

Virtual Processors
Minimum: 1
Desired: 1
Maximum: 1

Figure 2-11 Viewing a system plan

The system plan section in Figure 2-12 shows the system's disk units. The controller for the disk unit displays in the table. This detail is obtained only if the IBM i5/OS™ operating system that is controlling the disk units is running. Linux and IBM AIX operating systems do not display disk controller information or location information.



Hardware Management Console

System Plan: 750-1.sysplan

- Systems in 750-1.sysplan
  - 750-1
    - Partitions
      - p750_1_vio1
      - p750_1_vio2
      - p750_aix1
      - p750_aix2
      - p750_aix3
    - Hardware
      - U5802.001.0086848
      - U78A0.001.DNWHZWR
    - Expansion Unit Loops for Adapte
      - U78A0.001.DNWHZWR-P1-
    - Summary
      - Partitions

Drives

Backplane	Slot	Bus	Device Feature or CCIN	Device Description	Device Serial #	Disk Controller	Ord
P2	D3			SAS Disk Drive	3TB1RL1V		Own
P2	D4			SAS Disk Drive	3TB1RL3R		Own
P2	D5			SAS Disk Drive	3TB1RLDJ		Own
P2	D6			SAS Disk Drive	3TB1QBEP		Own
P2	D1						
P2	D2						

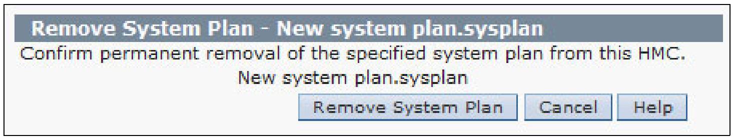
⊟ Expand / Collapse System Image

Figure 2-12 Viewing a system plan

2.3.9 Removing a system plan on the HMC

When you no longer need a system plan, you can remove the sysplan file easily from the HMC. Using Figure 2-3 on page 54 as a starting point, follow these steps:

1. Select a plan in the main system plan management window.
2. Click **Remove System Plan** either from the Tasks menu or the content Tasks link in the lower portion of the window. A confirmation message displays asking if you are sure that you want to delete the file (Figure 2-13).



Remove System Plan - New system plan.sysplan

Confirm permanent removal of the specified system plan from this HMC.

New system plan.sysplan

Figure 2-13 Confirm removal of system plan window

3. Click **Remove System Plan** to remove the selected sysplan file from the HMC.

2.4 System plans deployment

Since the publication of *LPAR Simplification Tools Handbook*, SG24-7231, from a general perspective, the deployment process has not changed much. Because of the updates of System Planning Tool Version 2 and HMC software, the details are not the same. The major improvements of the process are related to Virtual I/O Server implementation.

A summary of the deployment validation process is now described. We cover the new deployment wizard by using examples and provide details of the updates to the restricted shell CLI.

2.4.1 Deployment validation process

Before you deploy any system plan, it must be validated. There are two steps in this validation process. First, the hardware is validated and then, if that validation is successful, the partition is validated.

This process is detailed in *LPAR Simplification Tools Handbook*, SG24-7231. However, because fully understanding how the validation process works is fundamental, these concepts are summarized in the following sections.

Hardware validation

When you run hardware validation, the HMC checks that any planned hardware exists on the managed server and that all the I/O processors and adapters are located physically in the planned slots. Hardware validation does not necessarily mean that an exact match should occur between the planned and the existing hardware. For example, you can plan on using fewer processors or memory than physically installed, or you can plan on not using all the physically installed I/O units.

> **Important:** The HMC is not aware of the devices that are connected to the IOA. Therefore, there is no validation at a lower level than the IOA. When you use the System Plan Tool, specify devices such as disk drives, CD and DVD drives, and tape drives. The validation process *cannot* do any validation about these devices.

The validation includes all the following items:

- Server type, model, and processor feature: An exact match is required.
- Number of processors: At least the planned number should exist.
- Memory: At least the planned amount should exist.
- Expansion units: All the expansion units in the plan should exist.
- Slots: All the I/O processors and adapters in the plan should exist in a correct expansion or in the central electronics complex and should be at the same location.
- Any serial number: An exact match is required.

At this point, it is important to take actions to *avoid any ambiguity* about the expansion units or the processor enclosures central electronics complexes. You can have multiple central electronics complexes, for example on a 16-way model MMB. In that case, you can have four central electronics complexes.

This ambiguity takes place when two or more installed expansion units or central electronics complexes have the same type and contain the same I/O processors and adapters in the same slot. You might plan a partition to use specific expansion units due, for example, to their physical location in the racks or on the floor or to specific disks drives that the HMC cannot see. The validation process allows such a system plan, but there is no guarantee for the deployment to allocate the right expansion to the partition.

The best way to eliminate expansion units or central electronics complexes ambiguity is to specify, in the system plan, their serial number.

Eliminate any hardware validation error, for the partition validation to start.

Partition validation

When you run partition validation, the HMC checks that any *existing* partition on the server exactly matches with one of the planned partitions.

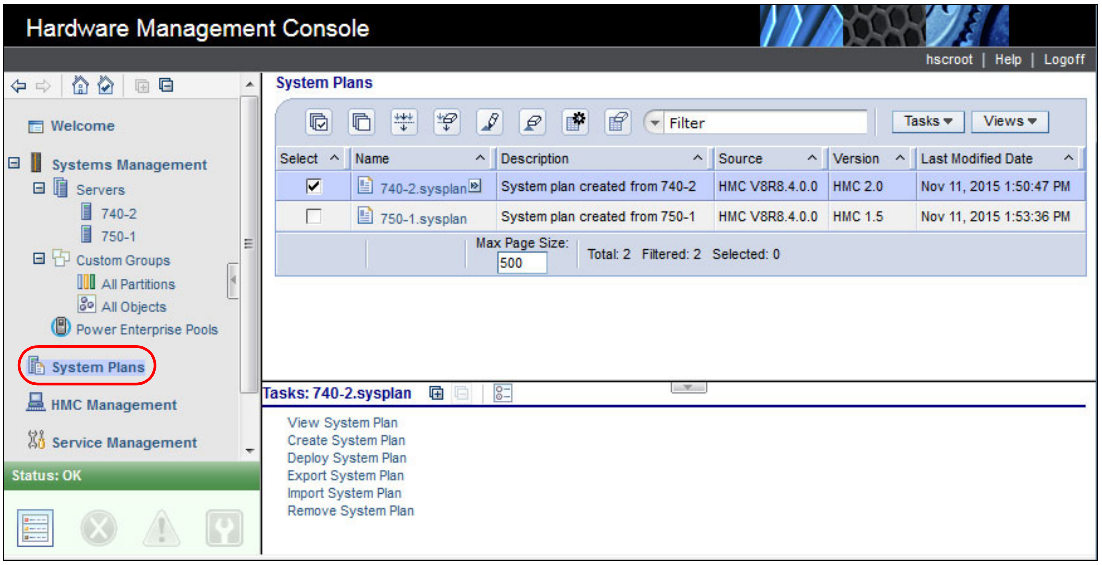
The validation includes all the following items:

- Partition name
- Partition ID
- Name of the default profile
- Processing resources in the system plan
- Memory resources in the system plan
- Physical hardware in the system plan
- Virtual adapters, including slot ID and maximum adapters, in the system plan

If any of these items fail, the partition validation is unsuccessful, and the deployment fails. Some of the corrections to allow the deployment should be applied on the server. This process is the case for the name of the default profile, which cannot be changed in the System Planning Tool and is the same as the partition name. This process is also the case for some hardware features like the USB controller or the IDE CD controller that the HMC allows you to assign to an i5/OS partition (although it cannot use them), but the SPT does not.

2.4.2 Deploy a system plan by using the graphical wizard

You can initiate deployment when you are using any right pane of the HMC by clicking **System Plans** on the left pane, as shown in Figure 2-14.



Select	Name	Description	Source	Version	Last Modified Date
☑	740-2.sysplan	System plan created from 740-2	HMC V8R8.4.0.0	HMC 2.0	Nov 11, 2015 1:50:47 PM
□	750-1.sysplan	System plan created from 750-1	HMC V8R8.4.0.0	HMC 1.5	Nov 11, 2015 1:53:36 PM

Max Page Size: 500 Total: 2 Filtered: 2 Selected: 0

Figure 2-14 Launch deployment

To deploy a system, follow these steps:

1. On the list of the system plans, select the one that you want to deploy by clicking the check box to the left of the system plan.

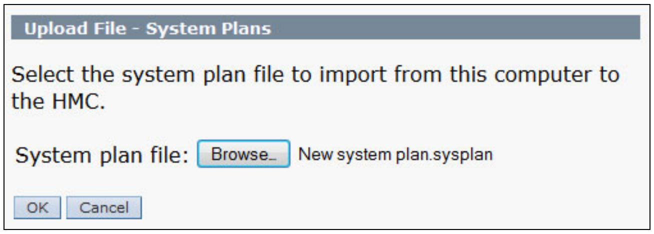
   The three ways to start the deployment of the selected system plan are as follows:

   – Click the contextual menu immediately to the right of the system plan name and select **Deploy System Plan**.

   – Click **Deploy System Plan** in the bottom Tasks panel.

   – Click **Tasks** at the top of the System Plans list panel and select **Deploy System Plan**.

2. After the wizard starts, its Welcome page (Figure 2-15) requests that you confirm the system plan to deploy and choose the managed server to be the target of the procedure. When your choices are made, click **Next** to continue.



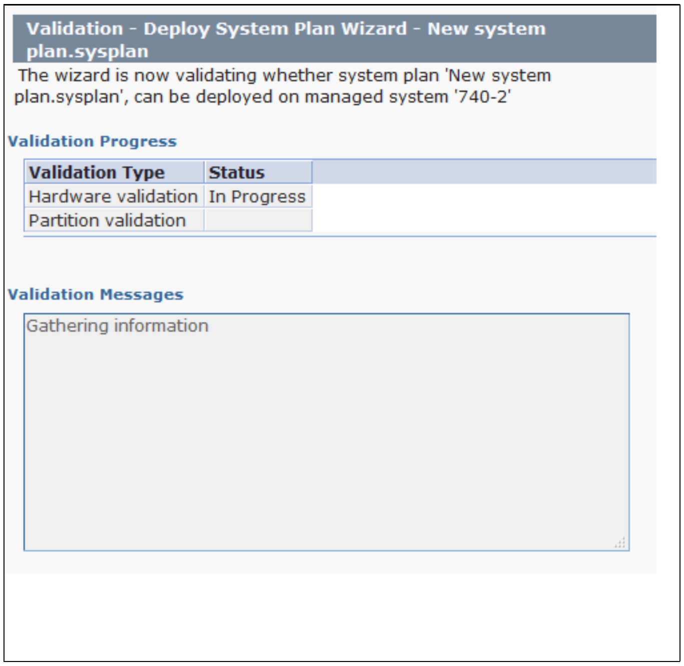
Upload File - System Plans

Select the system plan file to import from this computer to the HMC.

System plan file: Browse... New system plan.sysplan

Figure 2-15 Confirm the deployment startup

The validation progress is displayed (Figure 2-16).



Validation - Deploy System Plan Wizard - New system plan.sysplan

The wizard is now validating whether system plan 'New system plan.sysplan', can be deployed on managed system '740-2'

Validation Progress

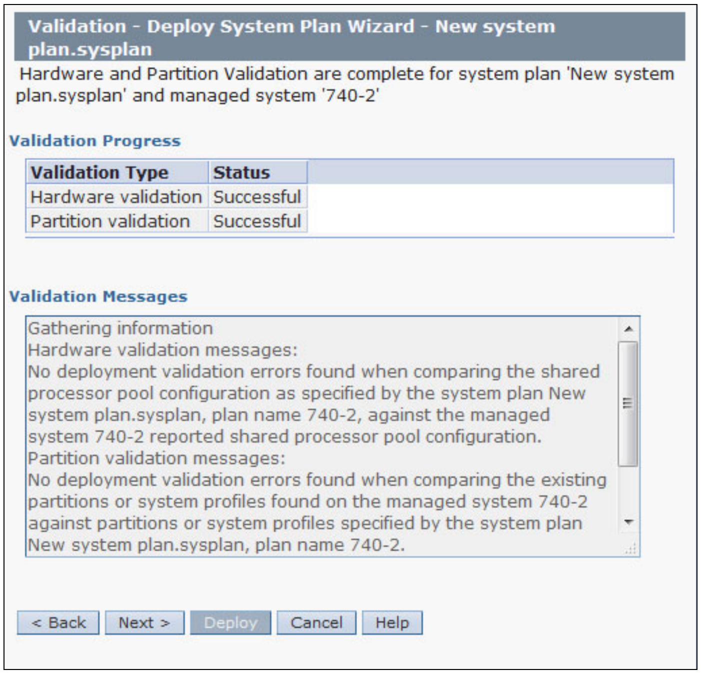
Validation Type	Status
Hardware validation	In Progress
Partition validation	

Validation Messages

Gathering information

Figure 2-16 Validation of system plan deployment in progress

3. When validation completes (Figure 2-17), you can examine all the related messages. You can view the messages that are successful and the messages that are unsuccessful.



Validation - Deploy System Plan Wizard - New system plan.sysplan

Hardware and Partition Validation are complete for system plan 'New system plan.sysplan' and managed system '740-2'

Validation Progress

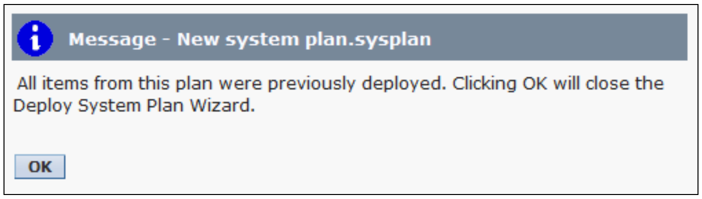
Validation Type	Status
Hardware validation	Successful
Partition validation	Successful

Validation Messages

```
Gathering information
Hardware validation messages:
No deployment validation errors found when comparing the shared
processor pool configuration as specified by the system plan New
system plan.sysplan, plan name 740-2, against the managed
system 740-2 reported shared processor pool configuration.
Partition validation messages:
No deployment validation errors found when comparing the existing
partitions or system profiles found on the managed system 740-2
against partitions or system profiles specified by the system plan
New system plan.sysplan, plan name 740-2.
```

Figure 2-17 Example of successful validation

Figure 2-18 shows an example of a successful validation.



Message - New system plan.sysplan

All items from this plan were previously deployed. Clicking OK will close the Deploy System Plan Wizard.

Figure 2-18 System plan deployment successful

4. On the Summary page, review the system deployment step order and click **Finish**. The HMC uses the system plan to create the specified logical partitions. This process can take several minutes.

Troubleshooting system plan deployment for an HMC

Use the following information to help resolve problems that you might encounter when deploying a system plan with the HMC Version 8, and later.

The system plan deployment process writes any messages, including error messages to the `/var/hsc/log/iqzdtrac.trm` file or to the `/var/hsc/log/deploy_validation.log` file if there are validation errors.

When you deploy a system plan, the validation process checks the information in the system plan with the configuration of the managed system. Some differences between the plan and the system can result in either hardware or partition validation errors. To deploy the system plan successfully, you must either change the system plan or change the target managed system.

2.5 System and partition templates

As the capabilities of PowerVM expand with the introduction of new technologies, the ability to provision virtual machines (VMs) quickly and efficiently becomes a key requirement.

The initial setup and configuration of Power Systems can be a complex process, and starting with the introduction of templates in IBM HMC V8.8.1.0.1, the provisioning of new Power Host systems and VMs has been simplified.

The Templates function allows the deployment of standard or customized templates for both systems and partitions.

Virtualization environment setup

A template is a collection of configuration preferences that can be quickly applied to multiple or single target IBM Power Systems. Templates can be used to set up your virtualization environment, and with preconfiguring of virtual resources, a highly customized template can be created to reduce the repetition of tasks when creating VMs.

Templates simplify the deployment process because templates contain many of the settings that previously were configured by using the HMC command-line interface (CLI) or the HMC graphical user interface (GUI) of previous versions. You can reuse a single template many times and modify templates to suit changes in environment requirements.

2.5.1 Template types

The two types of templates are as follows:

- System template

  System templates are used to define system configuration settings that include general system properties and virtual environment settings.

- Partition template

  Partition templates are used to define logical partition (LPAR) and VM settings, which include general partition properties, processor and memory configuration, virtual networks and virtual storage configuration, logical Host Ethernet Adapters (HEAs), and logical Single Root I/O Virtualization (SR-IOV) port settings.

The SR-IOV logical port settings allow virtualization of the physical ports of an adapter so that the ports can be shared by multiple partitions that are running simultaneously.

Templates do not contain target-specific information, so templates can be used to configure any system or partition in your environment. Partition templates can be used to deploy AIX, IBM i, and Linux logical partitions.

2.5.2 Predefined and custom templates

Templates can be further classified as predefined templates or custom templates.

Predefined templates contain configuration details for typical environment scenarios. Predefined templates are available for immediate use in the Templates and OS Images window. You cannot alter the predefined templates; however, you can copy and modify them for various needs.

Custom templates are templates that you create. Custom templates contain configuration details that are specific to your environment. You can create a custom template by using any of the following methods:

- Copy an existing template and modify the new template according to the requirements of your environment.
- Capture the configuration details of a currently running server or partition and save the details in to a new template.

2.5.3 Template overview

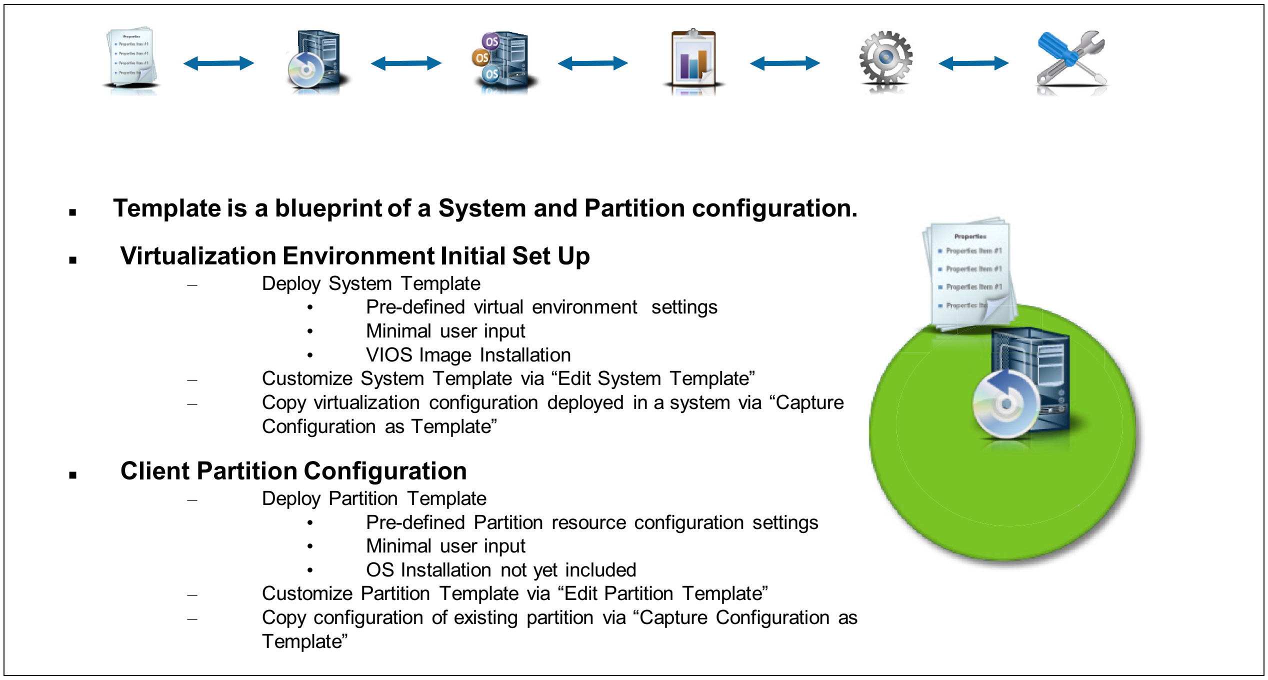
The deployment of logical partitions using the template function requires that you understand your physical infrastructure and how the infrastructure is virtualized. You also are required to ensure that the template can be used multiple times without changing it constantly.

Successful deployment of logical partitions from a template requires the careful planning, appropriate sizing, and configuration of your virtualization environment. The complexity of your environment might include some or all of the following components:

- Type of storage that is attached and how it is attached and presented to your environment. For example, allocated storage requires virtual SCSI or virtual fiber connections.
- Type of peripheral devices and how they are attached to your environment, For example, tape resources possibly require virtual fiber connections.
- Type of adapters that are installed in your Power Systems, for example, SR-IOV capable adapters.
- Type of Ethernet connectivity that is required and associated LAN or VLAN considerations.
- Type of VIOS implementation, for example, dual or single VIOS installations.

You need careful planning and configuring so that a template deployment of a system or partition can be an effective usage of the virtualized environment.

The successful deployment of templates requires simple steps, shown in Figure 2-19.



- **Template is a blueprint of a System and Partition configuration.**
- **Virtualization Environment Initial Set Up**
  - – Deploy System Template
    - Pre-defined virtual environment settings
    - Minimal user input
    - VIOS Image Installation
  - – Customize System Template via “Edit System Template”
  - – Copy virtualization configuration deployed in a system via “Capture Configuration as Template”
- **Client Partition Configuration**
  - – Deploy Partition Template
    - Pre-defined Partition resource configuration settings
    - Minimal user input
    - OS Installation not yet included
  - – Customize Partition Template via “Edit Partition Template”
  - – Copy configuration of existing partition via “Capture Configuration as Template”

Figure 2-19 Template overview

2.5.4 Template workflow

Regardless of the template type, a system or partition template can be viewed, edited, copied, deleted, deployed, and exported. An understanding of the workflow for a template and how it can be customized to suit your environment allows the creation of templates that efficiently deploy systems or partitions from a template.

An understanding of this workflow shows how templates can be created and how they can be edited to enhance their effectiveness when creating systems or logical partitions from a template, as shown in Figure 2-20 on page 70.

The figure shows that a template that is deployed to a target system can be derived from a starter template or a custom template.

- For a *starter template*, the preferred practice is not to edit the *original* template to suit your environment, but to copy the starter template and edit the *copied* template to suit your current environment. You can use these practices to keep the original template in its original state if you want to create an additional template that is based on the starter template to incorporate a new or different infrastructure.
- A *custom system template* can be derived by capturing the configuration details of a system in a running state. This custom template includes information about the VIOS, virtual network, virtual storage, and system settings. You can capture and save these details as a custom system template by using the HMC.

  A *custom partition template* can be derived by capturing the configuration details of a running partition or a partition that is not activated. Save the configuration details as a custom template to enable the creation of multiple partitions with the same configuration.

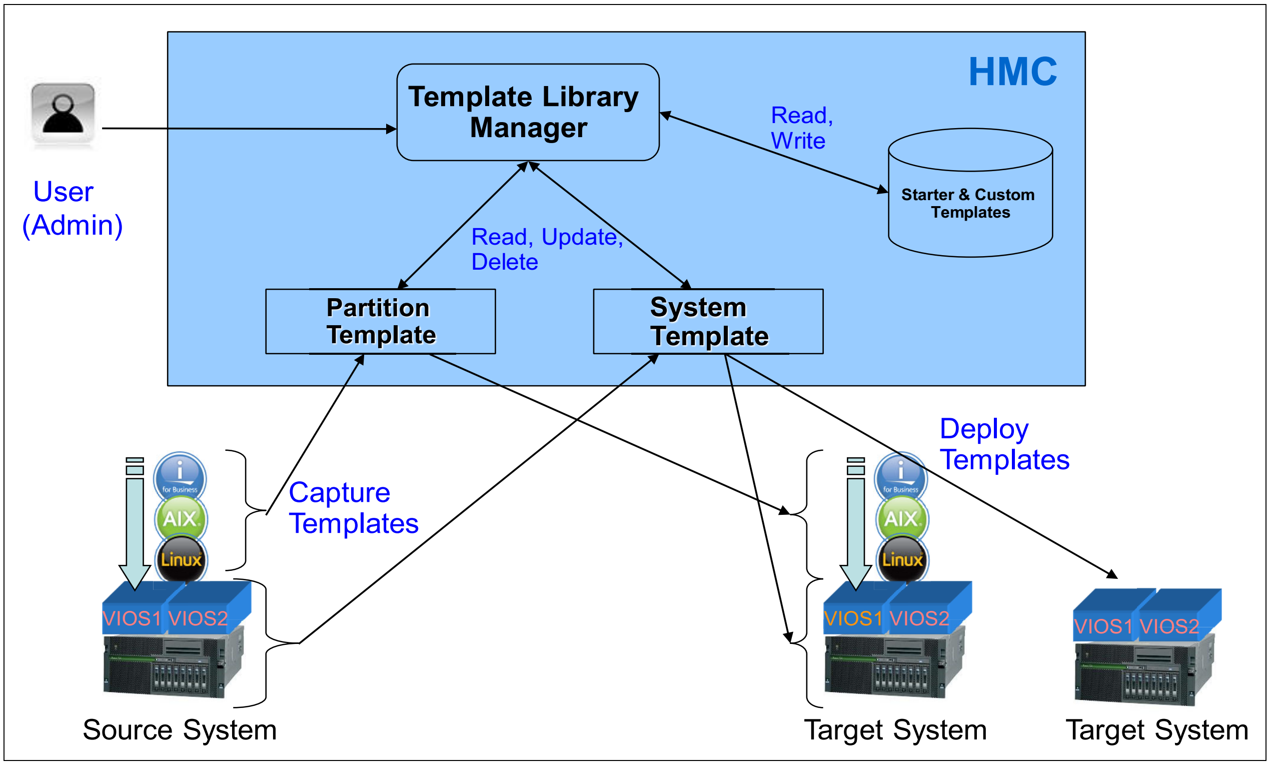
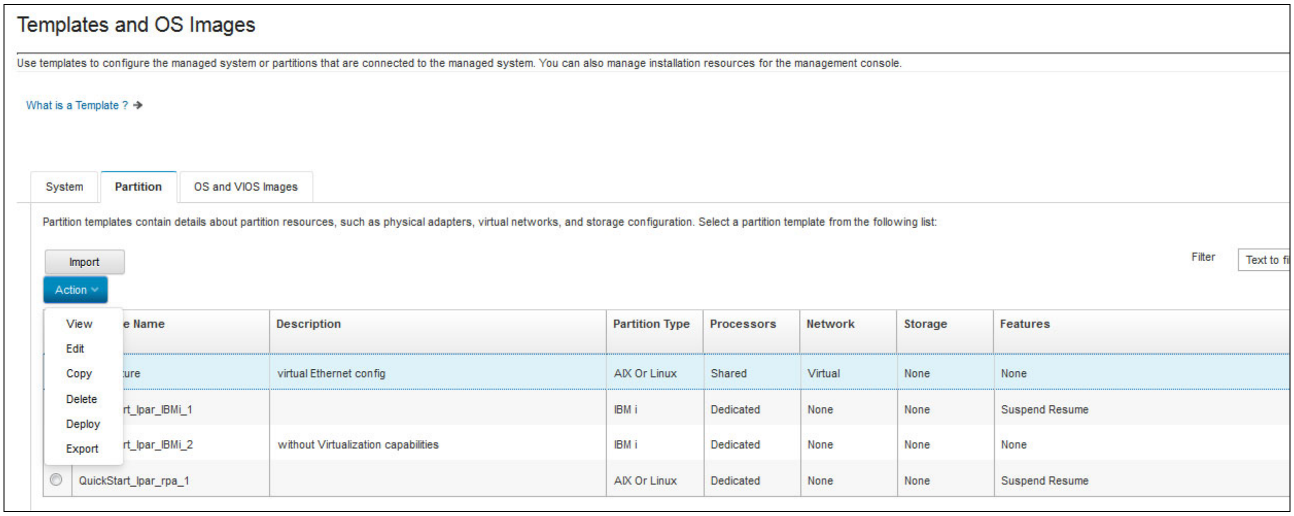


Figure 2-20 Template workflow

Figure 2-21 shows the functionality that is available with the templates in the Templates and OS Images window.


Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

What is a Template ?

Partition templates contain details about partition resources, such as physical adapters, virtual networks, and storage configuration. Select a partition template from the following list:

e Name	Description	Partition Type	Processors	Network	Storage	Features
ure	virtual Ethernet config	AIX Or Linux	Shared	Virtual	None	None
rt_lpar_IBMi_1		IBM i	Dedicated	None	None	Suspend Resume
rt_lpar_IBMi_2	without Virtualization capabilities	IBM i	Dedicated	None	None	None
QuickStart_lpar_rpa_1		AIX Or Linux	Dedicated	None	None	Suspend Resume

Figure 2-21 Template options in the Templates and OS Images window

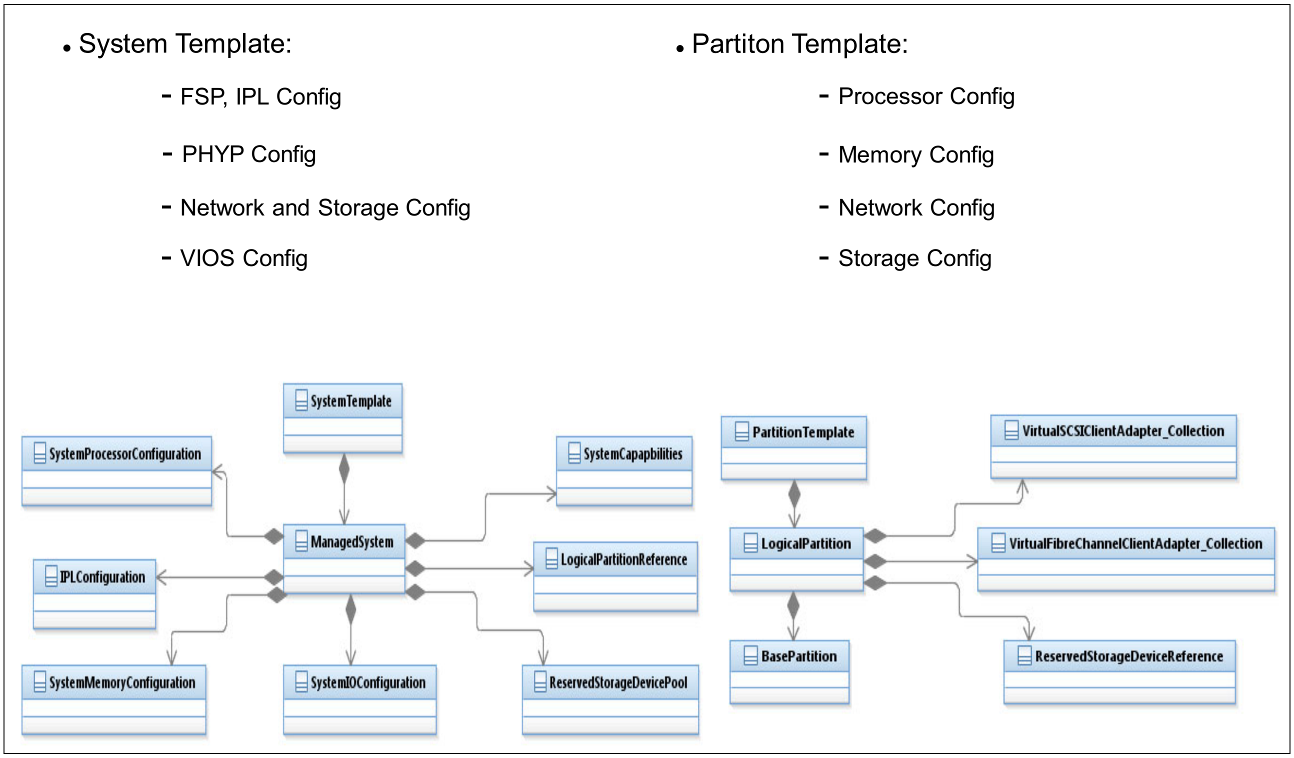
These functions are incorporated in to the template workflow and provide the ability to use a template that can be quickly deployed. If changes are necessary, the template can be modified to suit your needs without re-creating the template.

Customized templates can be copied and modified to suit an individual application or infrastructure requirement. This flexibility is limited only by your requirements and needs.

2.5.5 Template contents

Because a template is effectively a collection of configuration details that are captured or configured, a system or a partition can be deployed from a template with minimal input.

The following sections of this chapter have more detail about the templates and their contents. Figure 2-22 shows a high-level diagram of the contents of a template; it also shows the relationships between the configuration details and the template.



- System Template:
  - FSP, IPL Config
  - PHYP Config
  - Network and Storage Config
  - VIOS Config
- Partiton Template:
  - Processor Config
  - Memory Config
  - Network Config
  - Storage Config

SystemTemplate
SystemProcessorConfiguration
SystemCapapbilities
ManagedSystem
IPLConfiguration
LogicalPartitionReference
SystemMemoryConfiguration
SystemIOConfiguration
ReservedStorageDevicePool
PartitionTemplate
VirtualSCSIClientAdapter_Collection
LogicalPartition
VirtualFibreChannelClientAdapter_Collection
BasePartition
ReservedStorageDeviceReference

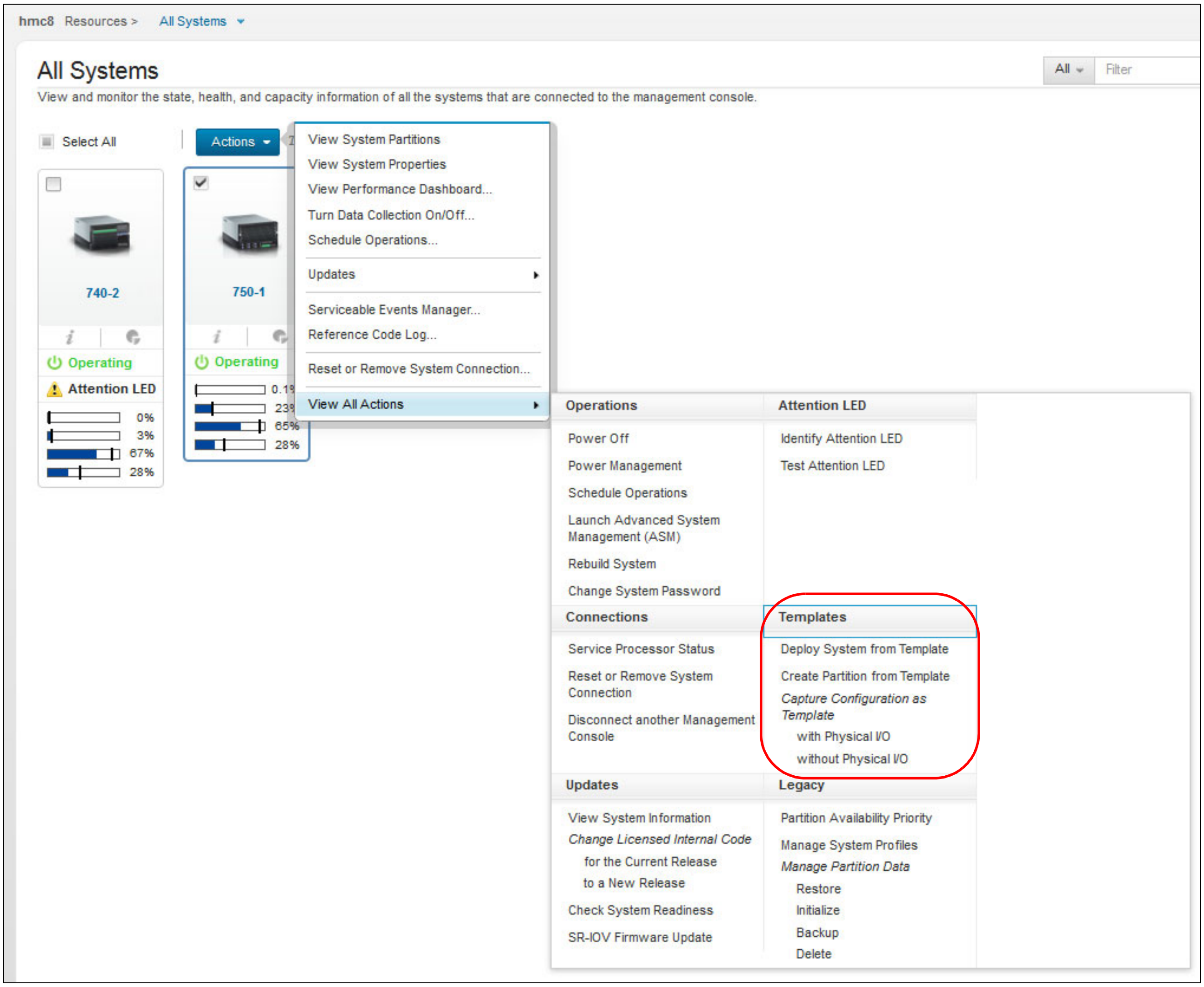
Figure 2-22 Template contents

2.5.6 Accessing templates

To view configuration information by using the HMC, complete the following steps:

1. Choose one of the following navigation options depending on the HMC interface type:
   - If you are using an HMC Enhanced interface, complete the following steps:
     i. In the navigation area, expand **Systems Management** → **Servers**.
     ii. Select a server and click **Templates** → **Template Library**.
   - If you are using an HMC Enhanced+ interface, complete the following steps:
     i. In the navigation pane, click the **HMC Management** icon. The icon represents the HMC Management function of the HMC.
     ii. Click **Templates and OS Images**, or click **Template Library** (Figure 2-23 on page 72).
2. In the Templates and O/S Images window, click the **System** tab.

3. Select the system template that you want to view and click **Actions** → **View**. You can view the details of Physical I/O, Host Ethernet Adapter, SR-IOV, Virtual I/O Servers, Virtual Networks, Virtual Storage, Shared Processor Pool, Shared Memory Pool and Reserved Storage, and Advanced System Settings by clicking the relevant tabs that are displayed. Alternately, you can view the template details from the Deploy System Template wizard.
4. Click **Close**.



View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

Figure 2-23 Accessing the Templates function

Note: To use templates fully, you must understand both PowerVM Virtualization concepts and have experience with using the HMC.

For more information about PowerVM and its concepts, see the following publications:

- *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940
- *IBM PowerVM Virtualization Managing and Monitoring*, SG24-7590
- *IBM PowerVM Enhancements What is New in 2013*, SG24-8198

2.5.7 System templates

System templates contain configuration information about resources, such as system properties, shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, HEAs, SR-IOV adapters, VIOS, virtual networks, virtual storage, and initial program load (IPL).

Many of the system settings that are previously configured by using HMC V7.7.9.0 or earlier can now be completed by using a system template.

The Templates and OS Images includes predefined system templates that contain configuration settings that are based on common usage scenarios. Predefined system templates are available for your immediate use.

You can create custom system templates that contain configuration settings that are specific to your environment.

You can create a custom template by copying any template that is available in the Templates and OS Images and then changing the copy to suit your environment.

You can also capture the configuration of an existing system and save the details in a template. You can deploy that template to other managed systems that require the same configuration.

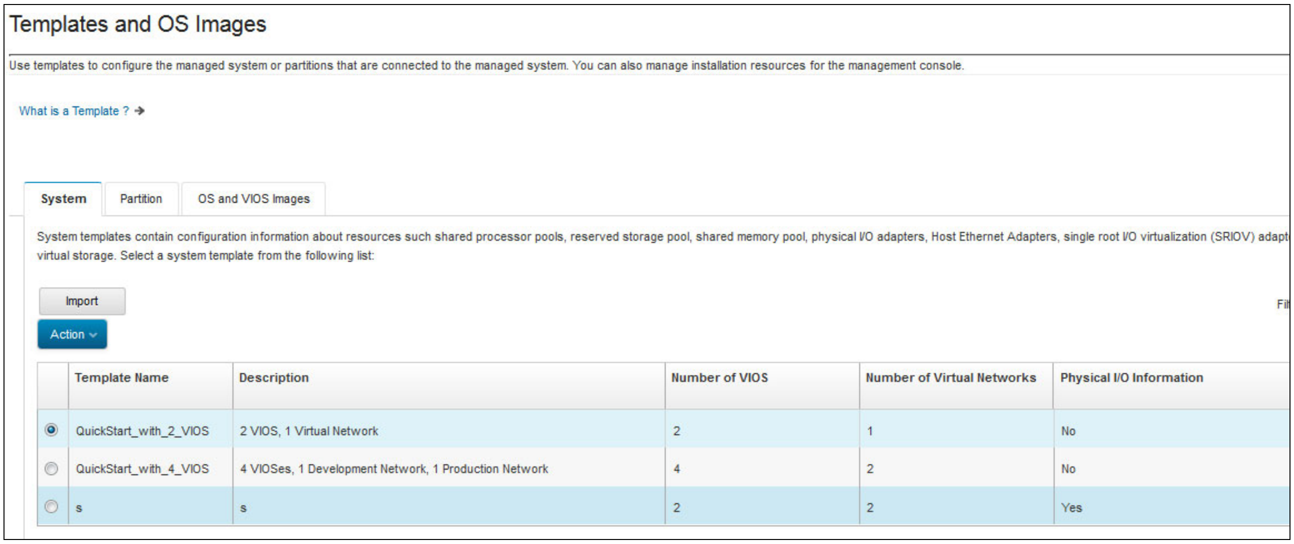
System templates are primarily used to deploy settings to new systems. To deploy new systems, complete the following tasks:

- View system template configuration information.
- Plan to deploy a system template.
- Capture a system configuration.
- Deploy a system by using a system template.

2.5.8 Viewing a system template

To view templates from HMC V8.8.4.0, complete the following steps:

1. Click **HMC Management**.
2. Select **Templates and OS Images** (Figure 2-24).



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

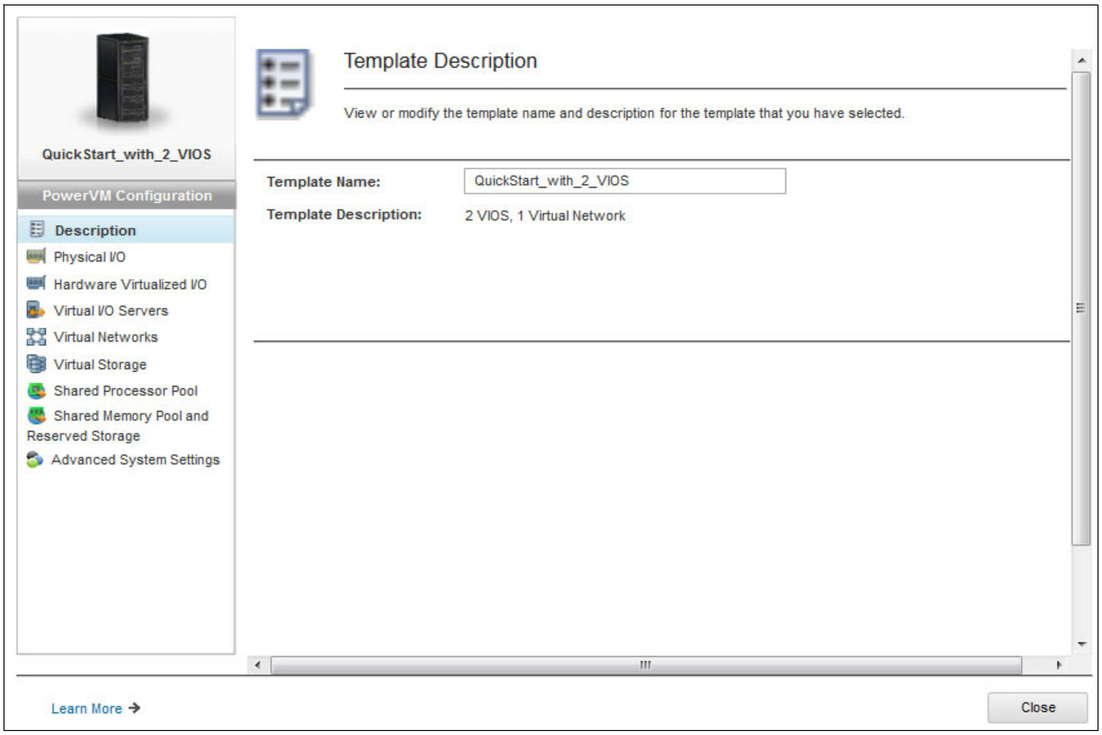
What is a Template ? →

System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet Adapters, single root I/O virtualization (SRIOV) adapt virtual storage. Select a system template from the following list:

	Template Name	Description	Number of VIOS	Number of Virtual Networks	Physical I/O Information
●	QuickStart_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1	No
○	QuickStart_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2	No
○	s	s	2	2	Yes

Figure 2-24 Templates and OS Images

3. Select a template, right-click it, and select **View**. A new window opens (Figure 2-25). In this window, you can select options on the left to use the various capabilities of PowerVM. These capabilities include Physical I/O, Virtual Storage, and Shared Processor Pools.



Template Description

View or modify the template name and description for the template that you have selected.

Template Name: QuickStart_with_2_VIOS

Template Description: 2 VIOS, 1 Virtual Network

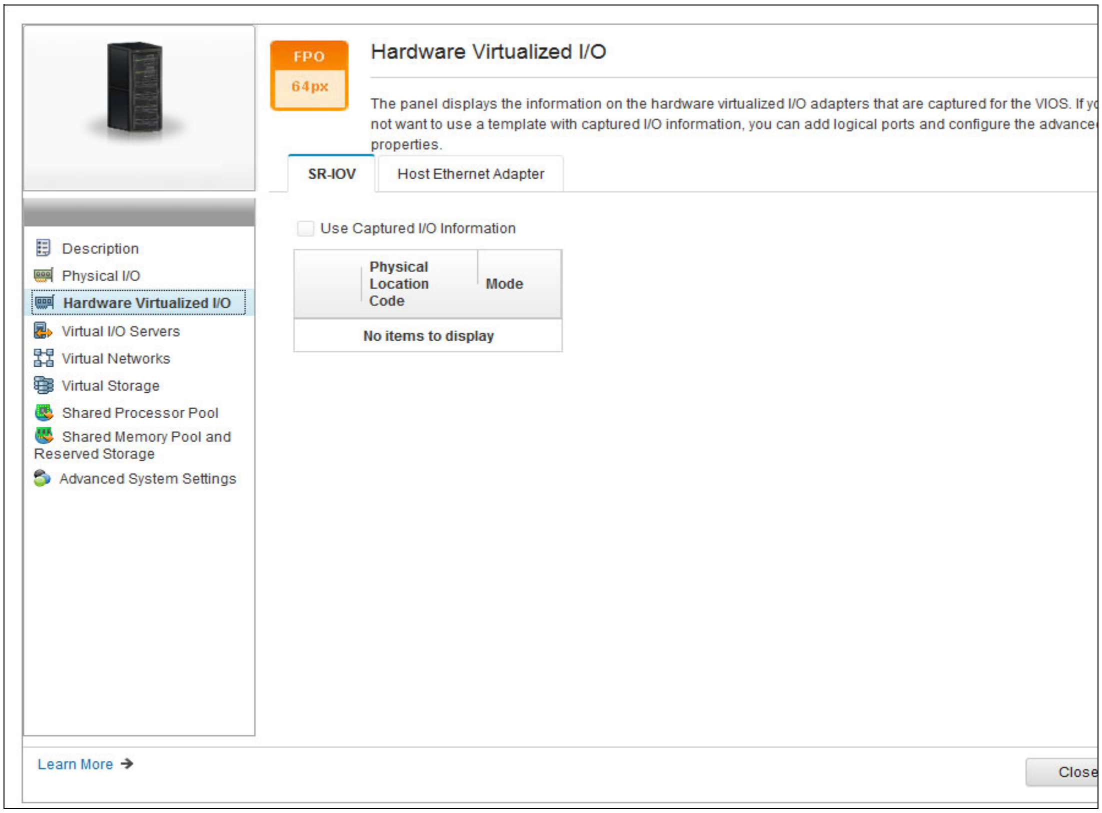
Figure 2-25 System template view

> **Note:** To fully use the capabilities of system templates and to implement them in to managed systems, you must have a thorough understanding of PowerVM and its capabilities. For more information about this topic, see *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940.

Clicking **Close** at any menu option returns you to the Templates and OS Images window.

When you select certain menu choices shown in Figure 2-25 on page 74, the following windows open, which show the capabilities of a system template:

- Figure 2-26
- Figure 2-27 on page 76
- Figure 2-28 on page 76



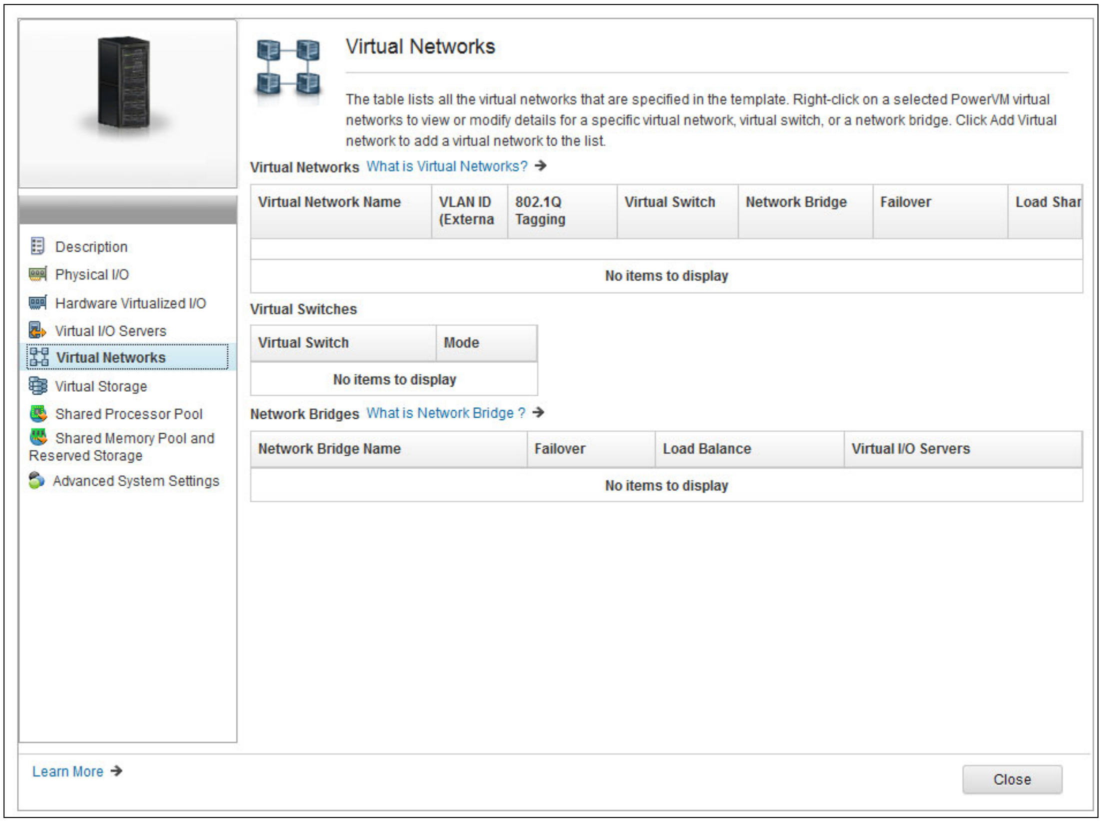
Hardware Virtualized I/O

The panel displays the information on the hardware virtualized I/O adapters that are captured for the VIOS. If yo not want to use a template with captured I/O information, you can add logical ports and configure the advance properties.

□ Use Captured I/O Information

Physical Location Code	Mode
No items to display	

Figure 2-26 System View: Hardware Virtualized I/O



Virtual Networks

The table lists all the virtual networks that are specified in the template. Right-click on a selected PowerVM virtual networks to view or modify details for a specific virtual network, virtual switch, or a network bridge. Click Add Virtual network to add a virtual network to the list.

Virtual Networks What is Virtual Networks? →

Virtual Network Name	VLAN ID (Externa	802.1Q Tagging	Virtual Switch	Network Bridge	Failover	Load Shar
No items to display						

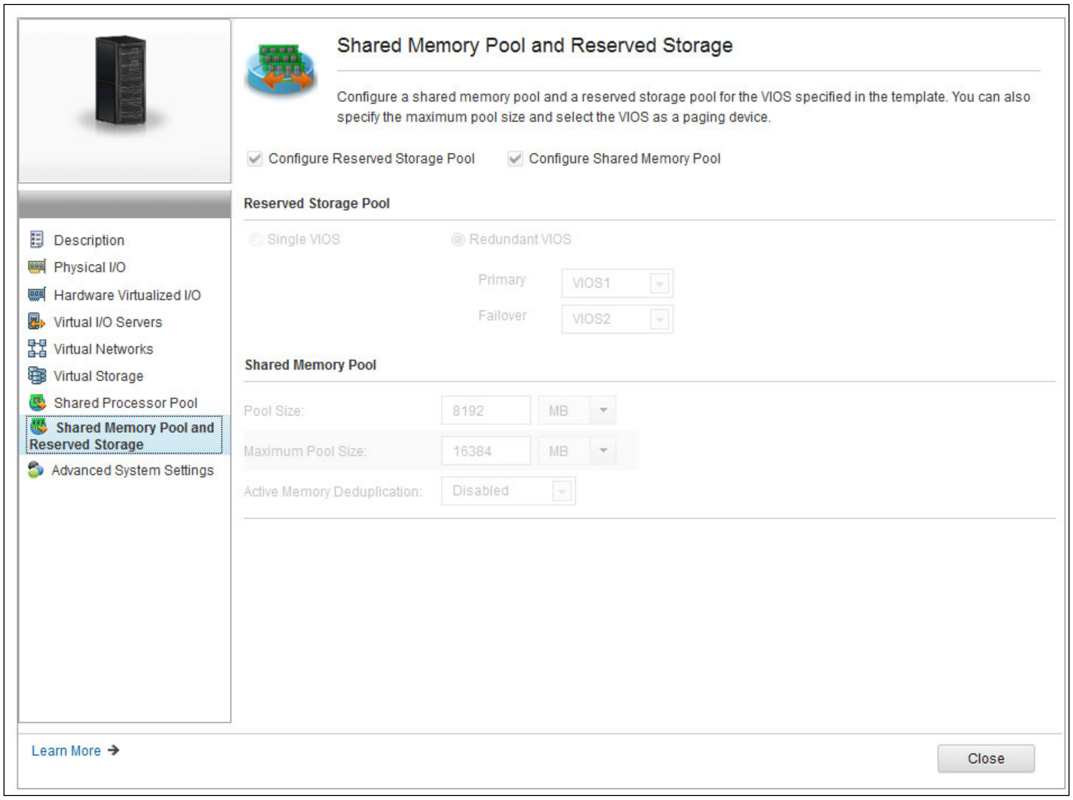
Virtual Switches

Virtual Switch	Mode
No items to display	

Network Bridges What is Network Bridge ? →

Network Bridge Name	Failover	Load Balance	Virtual I/O Servers
No items to display			

Figure 2-27 System View: Virtual Networks



Shared Memory Pool and Reserved Storage

Configure a shared memory pool and a reserved storage pool for the VIOS specified in the template. You can also specify the maximum pool size and select the VIOS as a paging device.

☑ Configure Reserved Storage Pool ☑ Configure Shared Memory Pool

Reserved Storage Pool

○ Single VIOS ● Redundant VIOS

Primary: VIOS1

Failover: VIOS2

Shared Memory Pool

Pool Size: 8192 MB

Maximum Pool Size: 16384 MB

Active Memory Deduplication: Disabled

Figure 2-28 Template View: Shared Memory Pool and Reserved Storage

2.5.9 Creating a system template

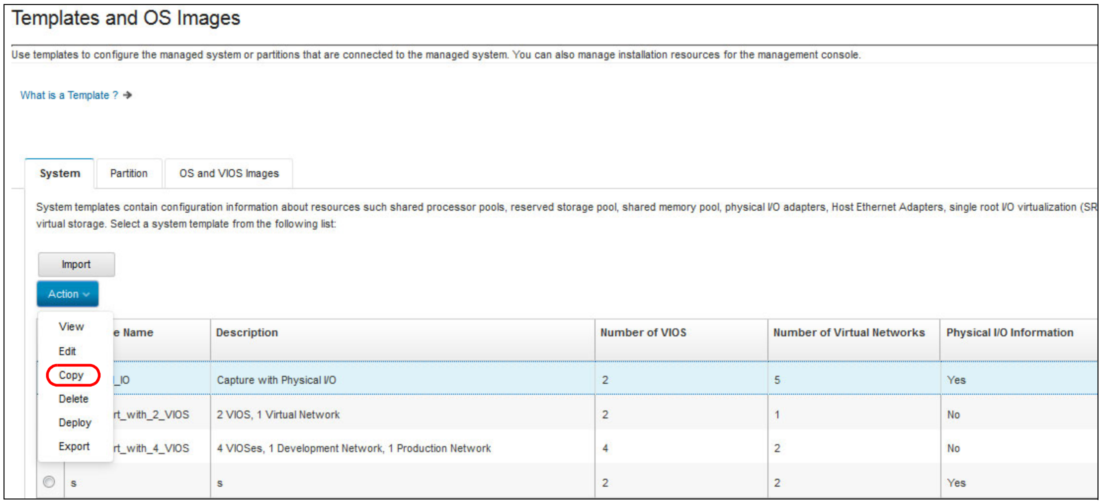
The two methods to create a system template from the HMC are as follows:

- *Copy* an existing template into a new template, which can then be modified as needed.
- *Capture* a running VIOS server or a VIOS server that is not in an activated state and save the configuration as a customized system template.

Copying a template

Complete the following steps:

1. From the Templates and OS Images window, select the system template to be copied, right-click the template, and select **Copy**, as shown in Figure 2-29.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

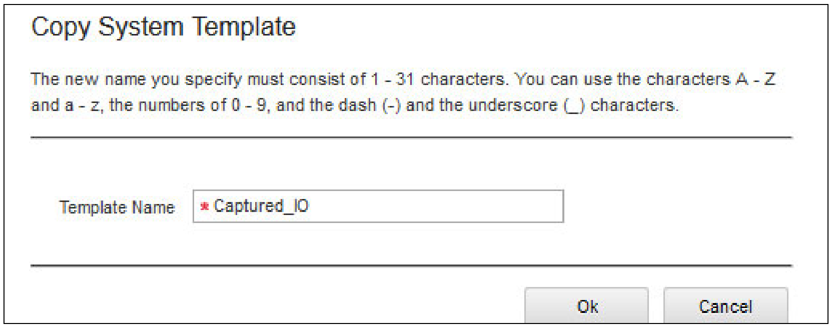
What is a Template ? ➔

System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet Adapters, single root I/O virtualization (SR
virtual storage. Select a system template from the following list:

e Name	Description	Number of VIOS	Number of Virtual Networks	Physical I/O Information
_IO	Capture with Physical I/O	2	5	Yes
rt_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1	No
rt_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2	No
s	s	2	2	Yes

Figure 2-29 System template: Copy

2. Enter an appropriate system template name, as shown in Figure 2-30.



Copy System Template

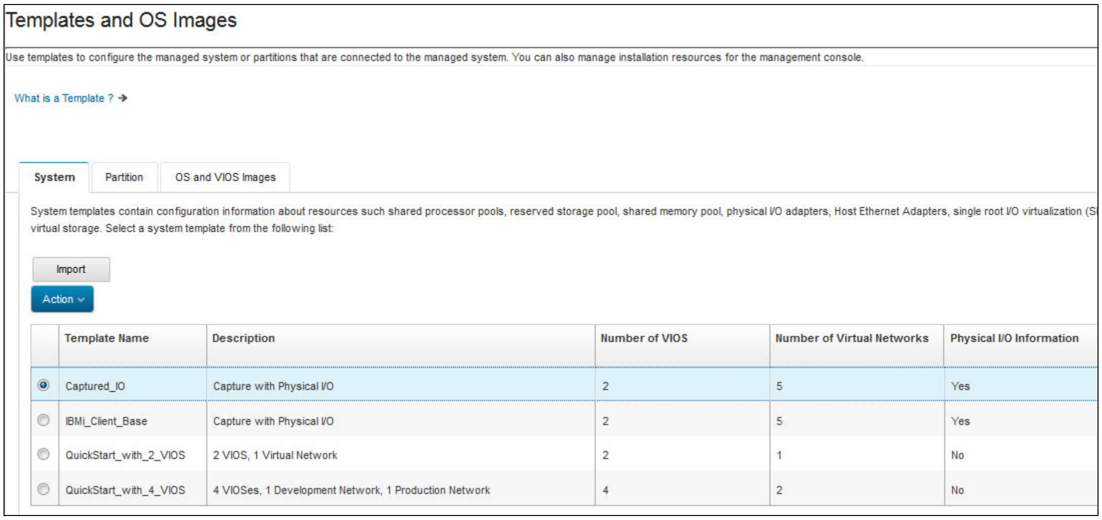
The new name you specify must consist of 1 - 31 characters. You can use the characters A - Z and a - z, the numbers of 0 - 9, and the dash (-) and the underscore (_) characters.

Template Name * Captured_IO

Figure 2-30 System template: Copy name

3. Click **OK**.

After the copy completes, your new template is displayed in the Templates and OS Images, as shown in Figure 2-31.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet Adapters, single root I/O virtualization (S
virtual storage. Select a system template from the following list:

	Template Name	Description	Number of VIOS	Number of Virtual Networks	Physical I/O Information
●	Captured_IO	Capture with Physical I/O	2	5	Yes
○	IBMi_Client_Base	Capture with Physical I/O	2	5	Yes
○	QuickStart_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1	No
○	QuickStart_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2	No

Figure 2-31 Templates and OS Images: template is listed

Capturing a configuration as a template

You can capture the configuration details from a running VIOS or a VIOS that is in the not activated state and save the configuration as a custom system template.

The option to capture configuration as a template is available only when the managed system is in the running state.

This function is useful if you want to deploy multiple systems with the same configuration.

Complete the following steps:

1. From the HMC work pane, select the managed system containing the VIOS servers from which you want to create a template.
2. At the bottom of the work pane, expand **Templates** and then select **Capture Configuration as Template,** as shown in Figure 2-32 on page 79, to reveal the two available capture options:

   – With Physical I/O
   – Without Physical I/O

   The configuration can be captured with or without physical I/O resources of the system. For managed systems with the same physical I/O resources, capturing with Physical I/O means that you do not have to select the resources on the target system manually upon template deployment.

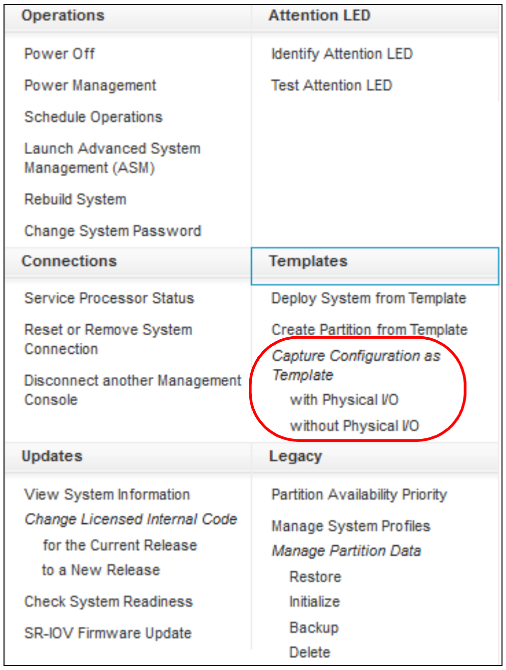
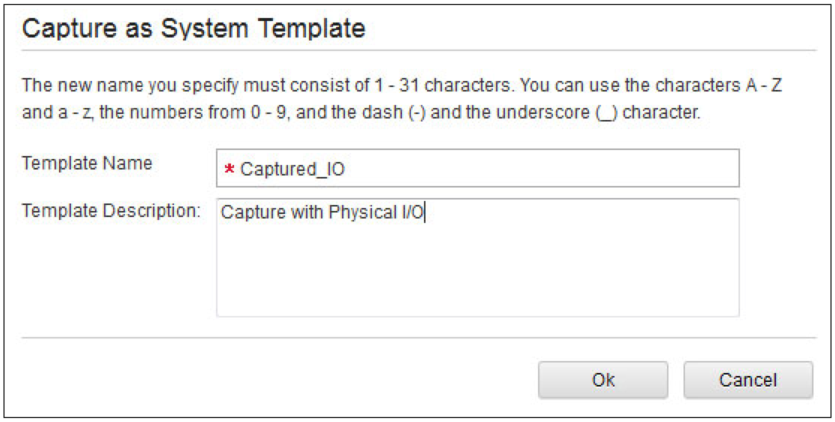


Figure 2-32 Capture Configuration as Template menu

3. This example captures the configuration with physical I/O. When you are prompted for a template name and description, enter them, as shown in Figure 2-33.



Capture as System Template

The new name you specify must consist of 1 - 31 characters. You can use the characters A - Z and a - z, the numbers from 0 - 9, and the dash (-) and the underscore (_) character.

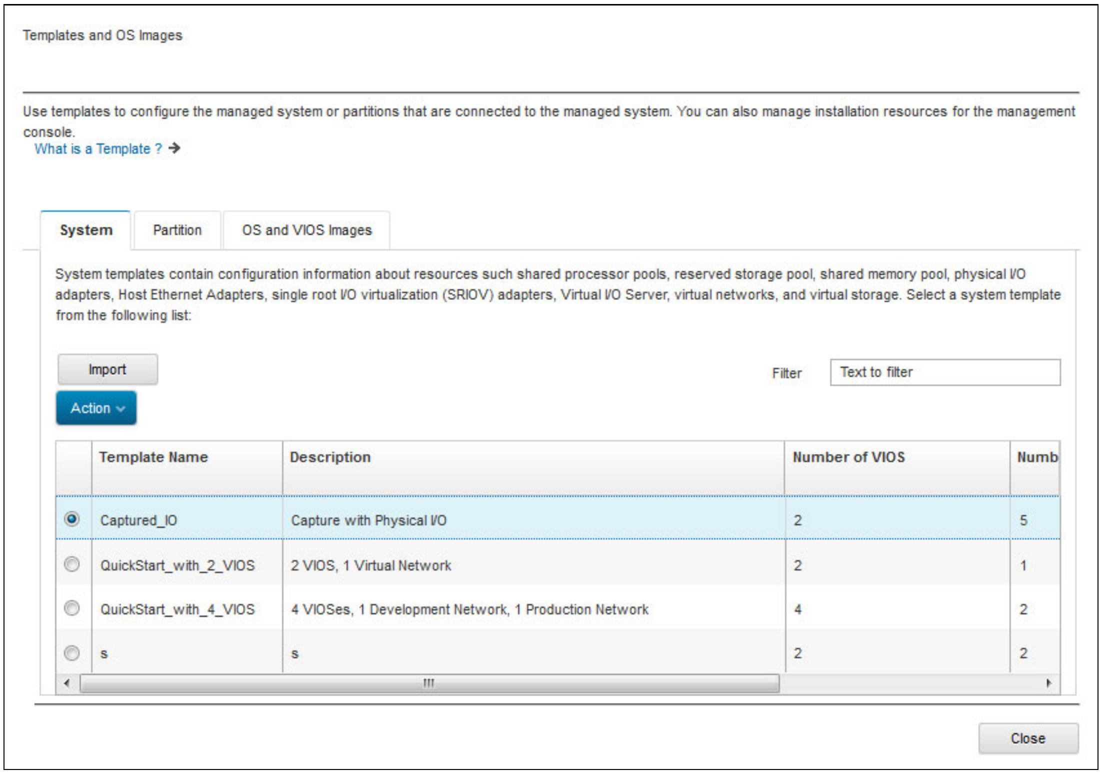
Template Name: * Captured_IO

Template Description: Capture with Physical I/O

Figure 2-33 Capture configuration: Name

4. Click **OK** to start the capture of the configuration.

   After the configuration is captured, you are returned to the Templates and OS Images, as shown in Figure 2-34. The captured template is highlighted.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

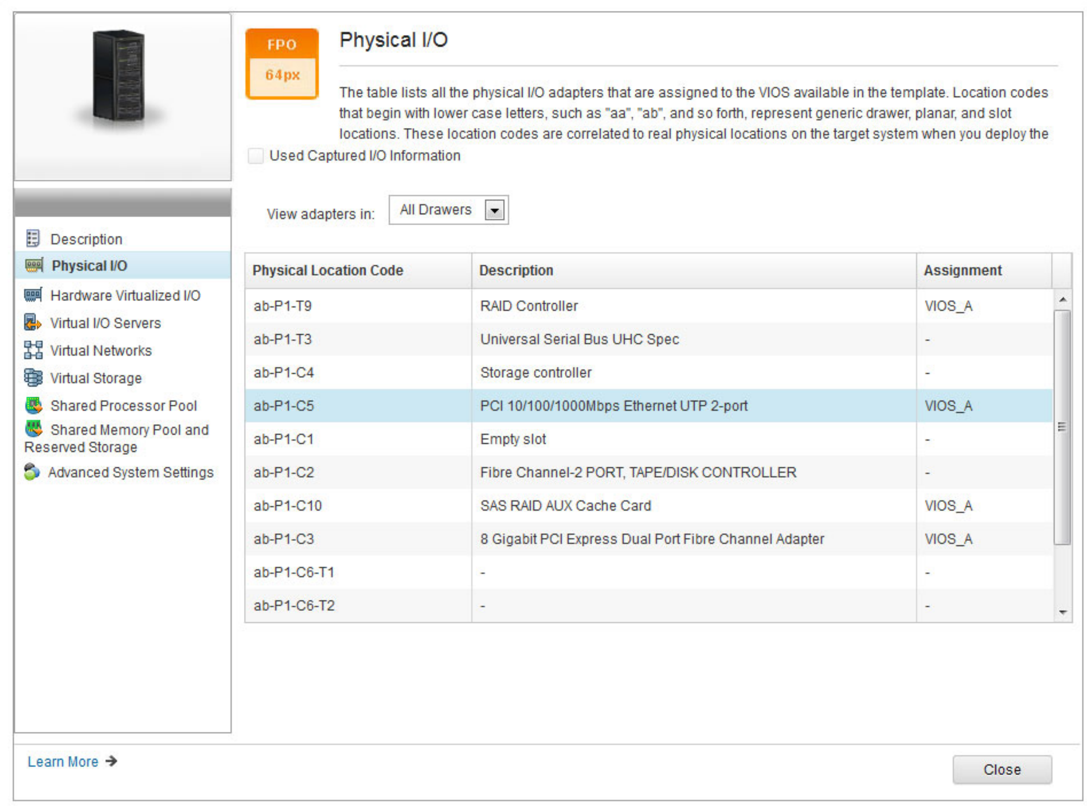
What is a Template ? →

System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet Adapters, single root I/O virtualization (SRIOV) adapters, Virtual I/O Server, virtual networks, and virtual storage. Select a system template from the following list:

	Template Name	Description	Number of VIOS	Numb
●	Captured_IO	Capture with Physical I/O	2	5
○	QuickStart_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1
○	QuickStart_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2
○	s	s	2	2

Figure 2-34 Templates and OS Images after capture

5. To look at the template properties, right-click the captured template and select **View**. Click **Physical I/O** to display the captured physical I/O resources, as shown in Figure 2-35. In a captured configuration with *no* physical I/O, no resources are displayed in this menu option.



Physical I/O

The table lists all the physical I/O adapters that are assigned to the VIOS available in the template. Location codes that begin with lower case letters, such as "aa", "ab", and so forth, represent generic drawer, planar, and slot locations. These location codes are correlated to real physical locations on the target system when you deploy the

□ Used Captured I/O Information

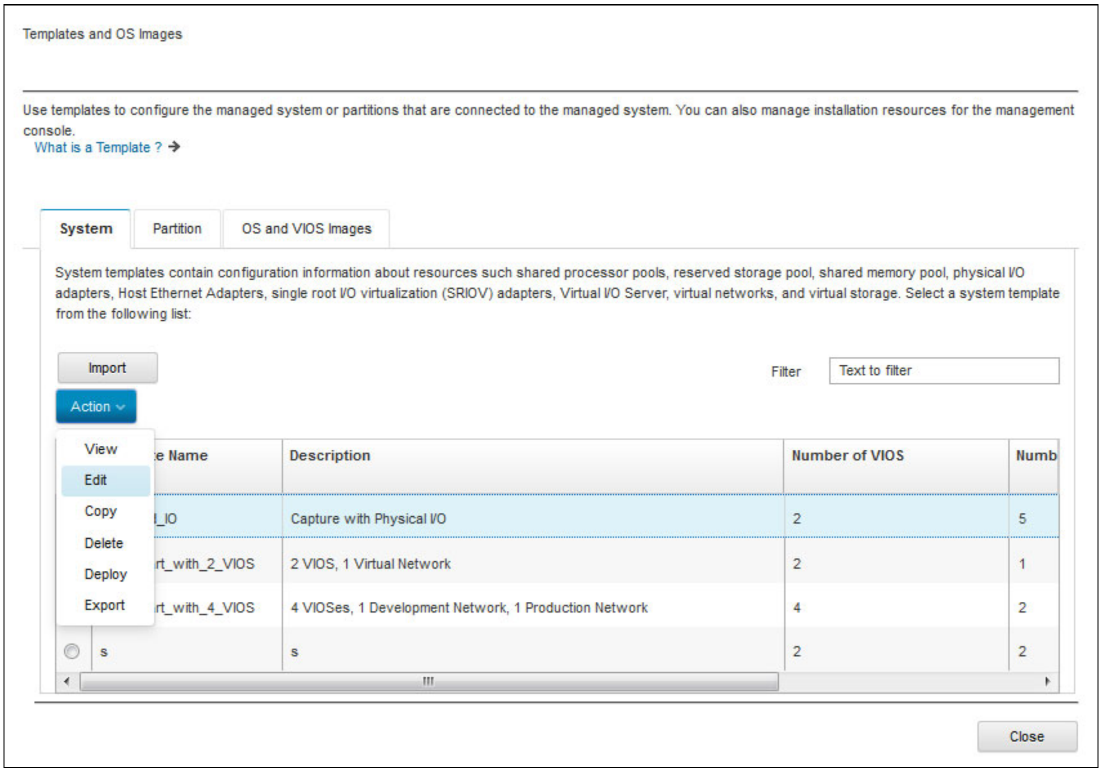
View adapters in: All Drawers

Physical Location Code	Description	Assignment
ab-P1-T9	RAID Controller	VIOS_A
ab-P1-T3	Universal Serial Bus UHC Spec	-
ab-P1-C4	Storage controller	-
ab-P1-C5	PCI 10/100/1000Mbps Ethernet UTP 2-port	VIOS_A
ab-P1-C1	Empty slot	-
ab-P1-C2	Fibre Channel-2 PORT, TAPE/DISK CONTROLLER	-
ab-P1-C10	SAS RAID AUX Cache Card	VIOS_A
ab-P1-C3	8 Gigabit PCI Express Dual Port Fibre Channel Adapter	VIOS_A
ab-P1-C6-T1	-	-
ab-P1-C6-T2	-	-

Figure 2-35 System template with captured I/O

2.5.10 Editing a system template

To edit templates, in the Templates and OS Images window, right-click the selected template and select **Actions** → **Edit**, as shown in Figure 2-36.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

What is a Template ? →

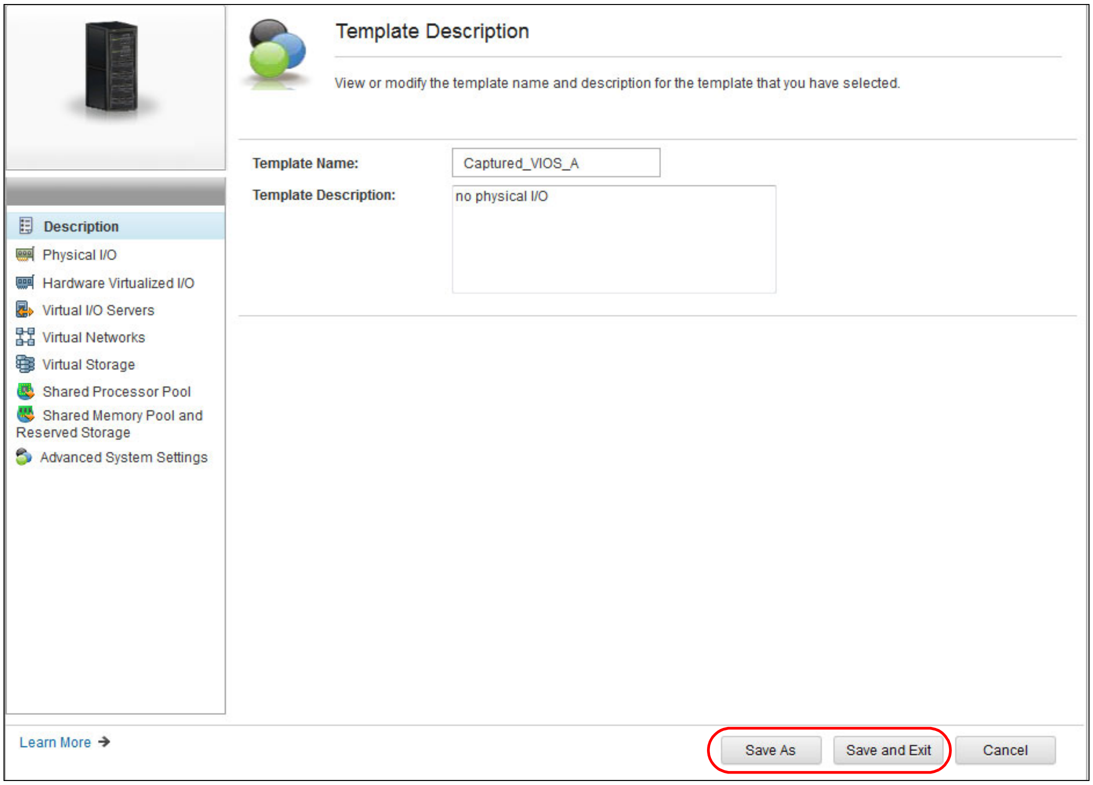
System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet Adapters, single root I/O virtualization (SRIOV) adapters, Virtual I/O Server, virtual networks, and virtual storage. Select a system template from the following list:

Filter: Text to filter

	e Name	Description	Number of VIOS	Numb
	l_IO	Capture with Physical I/O	2	5
	rt_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1
	rt_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2
○	s	s	2	2

Figure 2-36 System template: Edit

A new window opens (Figure 2-37). This is the initial system template edit window with the available menu options on the left side of the window.



Template Name: Captured_VIOS_A

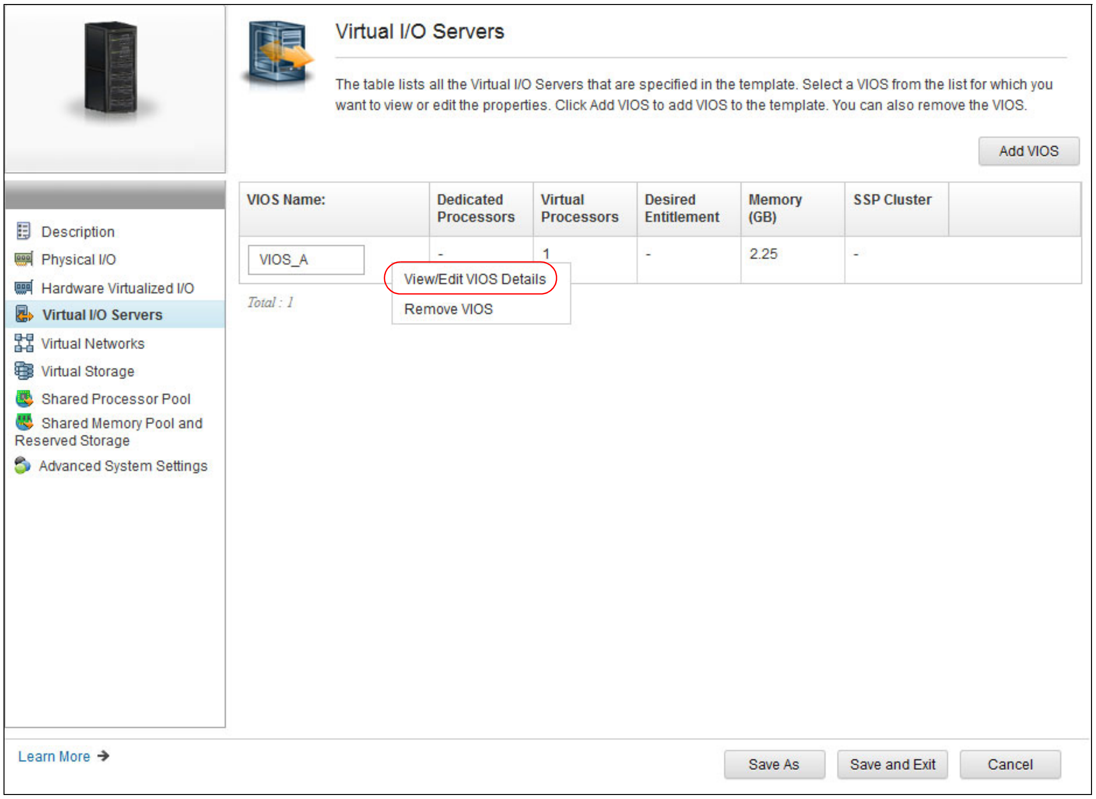
Template Description: no physical I/O

Figure 2-37 Edit system template: initial window

To save any changes to your template from any menu option, click **Save and Exit**, which updates your template, as shown in Figure 2-37.

Clicking **Save As** saves your template configuration, including changes, in a *new* system template. This is the same process as copying a template, which is described in “Copying a template” on page 114.

You can click **Virtual I/O Servers** to modify a captured VIOS configuration and add an extra VIOS if your environment requires its implementation. Select the VIOS and right-click it to display the available options, as shown in Figure 2-38.



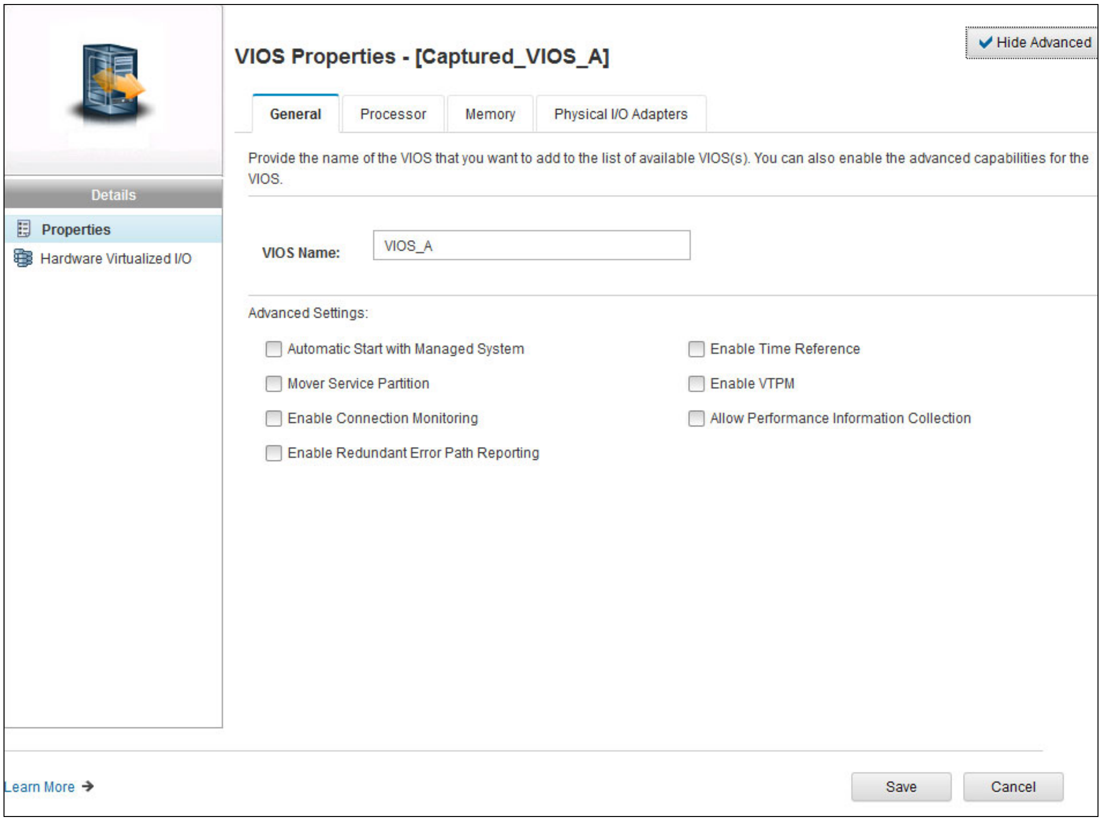
The table lists all the Virtual I/O Servers that are specified in the template. Select a VIOS from the list for which you want to view or edit the properties. Click Add VIOS to add VIOS to the template. You can also remove the VIOS.

VIOS Name:	Dedicated Processors	Virtual Processors	Desired Entitlement	Memory (GB)	SSP Cluster
VIOS_A	-	1	-	2.25	-

Total : 1

Figure 2-38   Edit system template: VIOS servers

Click **View/Edit VIOS Details** to edit the VIOS configuration. You can then edit the VIOS details, as shown in Figure 2-39.



VIOS Properties - [Captured_VIOS_A]

Provide the name of the VIOS that you want to add to the list of available VIOS(s). You can also enable the advanced capabilities for the VIOS.

VIOS Name: VIOS_A

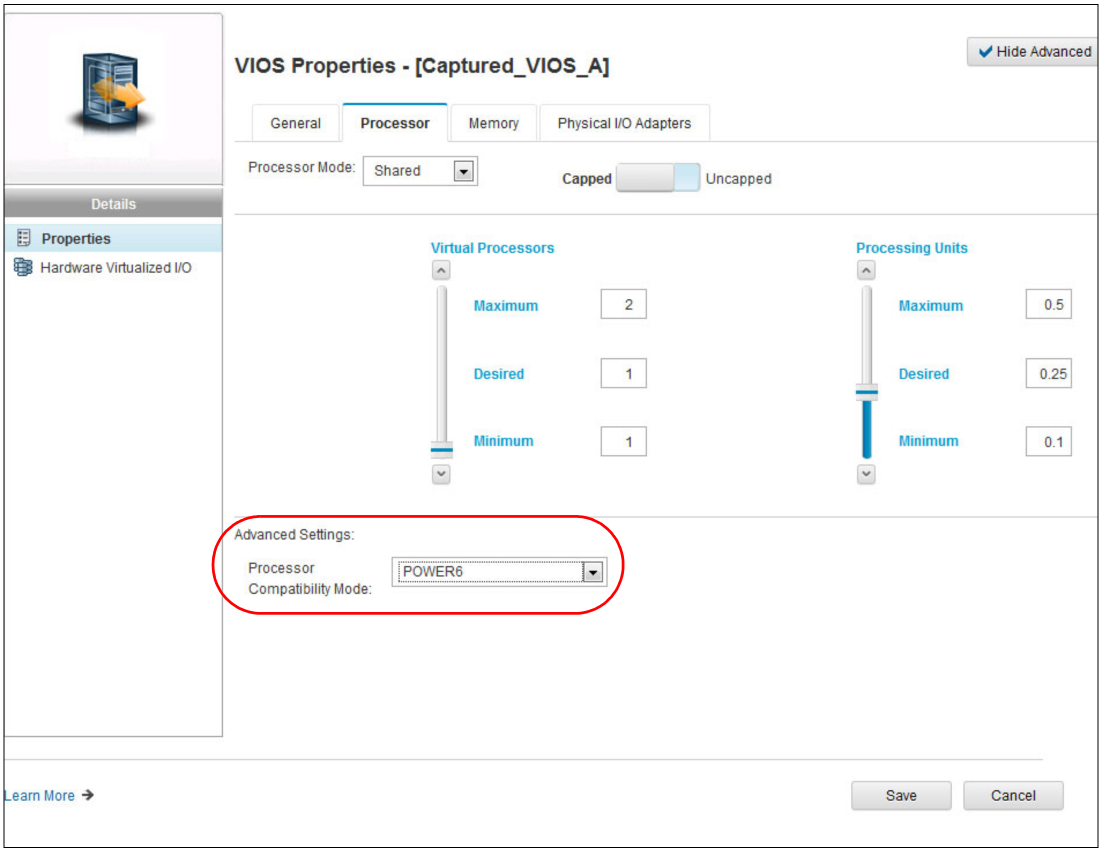
Advanced Settings:

- □ Automatic Start with Managed System
- □ Mover Service Partition
- □ Enable Connection Monitoring
- □ Enable Redundant Error Path Reporting
- □ Enable Time Reference
- □ Enable VTPM
- □ Allow Performance Information Collection

Figure 2-39 Edit VIOS details: general

Clicking **Show Advanced** displays the available Advanced Settings for the VIOS. Modify these settings to suit your environment.

You can click the **Processor** tab to change the Processor mode, assign processor values, and change the Processor Compatibility Mode, as shown in Figure 2-40.



VIOS Properties - [Captured_VIOS_A]

Processor Mode: Shared

Capped Uncapped

Virtual Processors

Maximum 2

Desired 1

Minimum 1

Processing Units

Maximum 0.5

Desired 0.25

Minimum 0.1

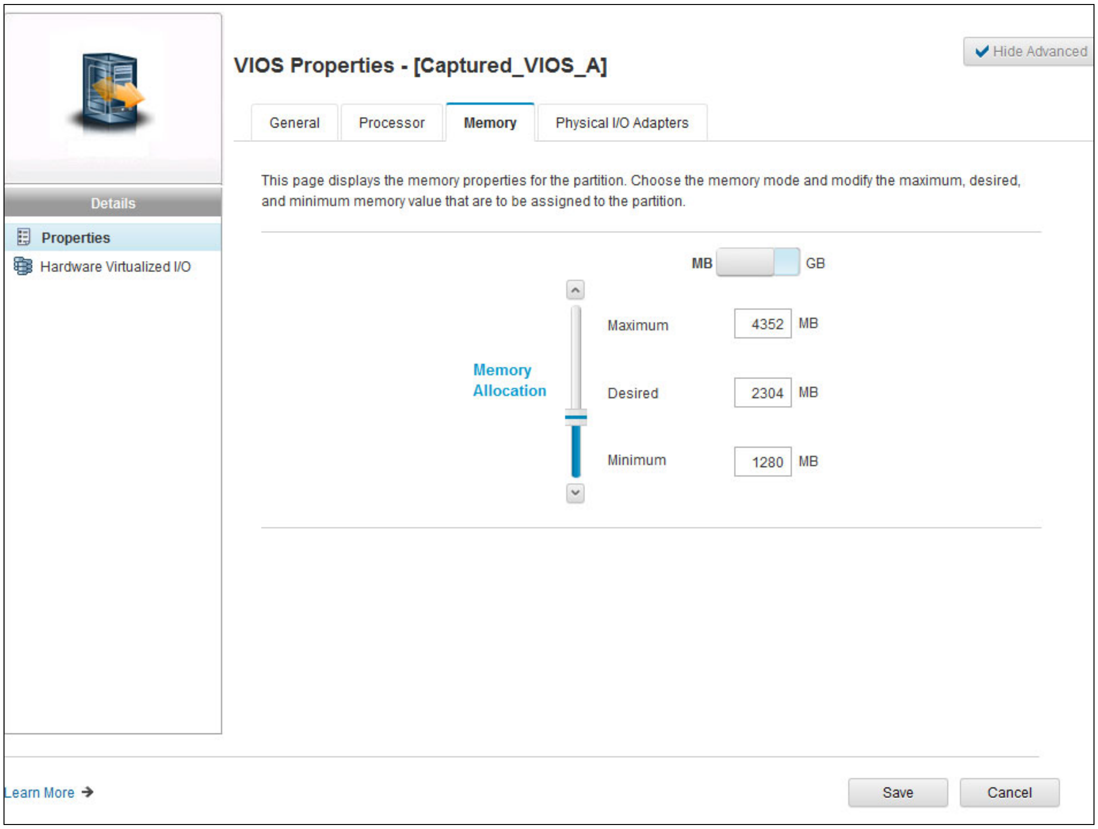
Advanced Settings:

Processor Compatibility Mode: POWER6

Figure 2-40 Edit VIOS details: processor

Click **Show Advanced** to display the option to change the Processor Compatibility Mode. Adjust the processor mode and processor values to suit your environment.

You can click the **Memory** tab to change the assigned memory, as shown in Figure 2-41. Adjust the memory requirements to suit your environment.



VIOS Properties - [Captured_VIOS_A]

This page displays the memory properties for the partition. Choose the memory mode and modify the maximum, desired, and minimum memory value that are to be assigned to the partition.

Memory Allocation

Maximum 4352 MB

Desired 2304 MB

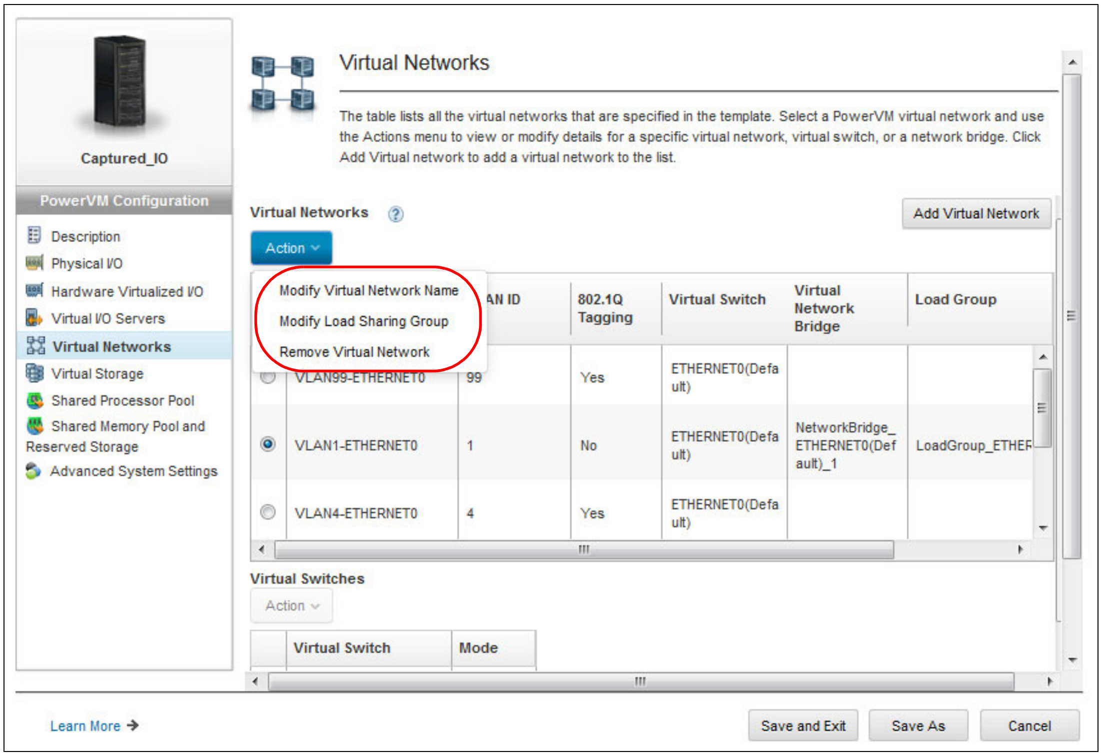
Minimum 1280 MB

Figure 2-41 Edit VIOS details: memory

Click **Save** to update your VIOS configuration and return to Figure 2-38 on page 84.

Click **Virtual Networks** to modify the virtual networks that are on the managed system.

More virtual networks can be added to this system template. You can select the appropriate virtual network to modify the selected virtual network configuration, as shown in Figure 2-42.



The table lists all the virtual networks that are specified in the template. Select a PowerVM virtual network and use the Actions menu to view or modify details for a specific virtual network, virtual switch, or a network bridge. Click Add Virtual network to add a virtual network to the list.

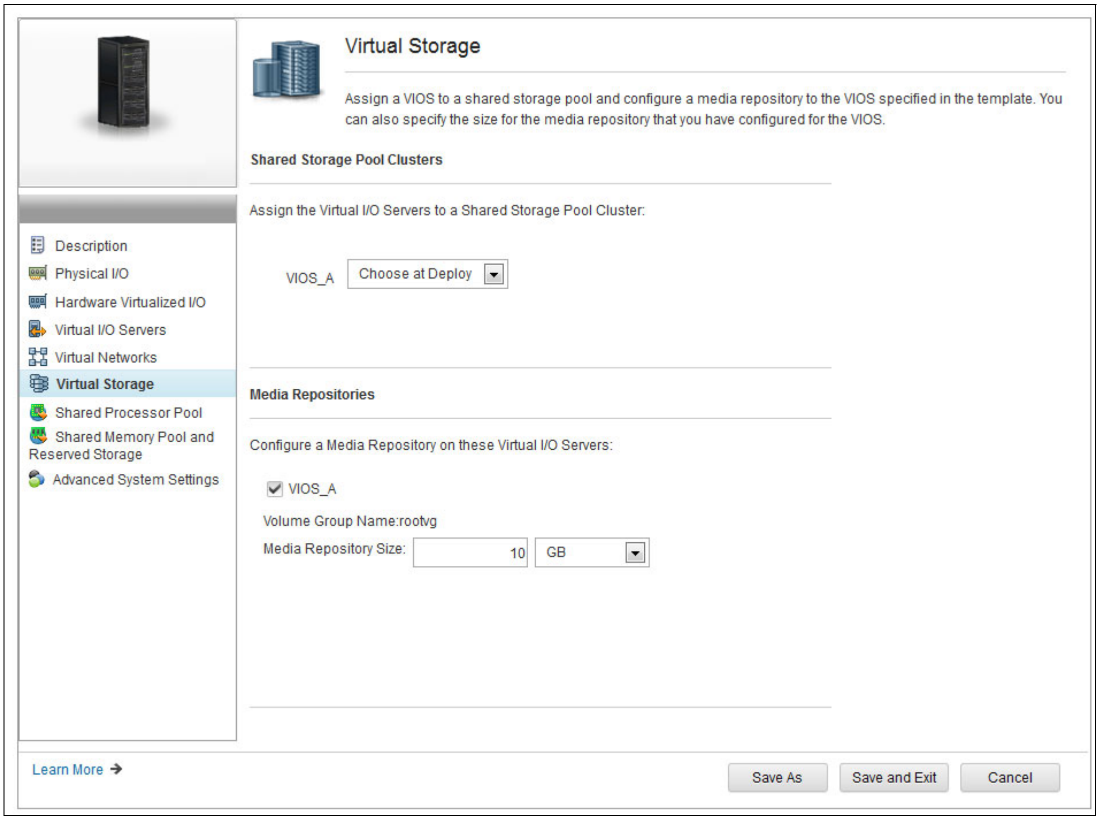
		AN ID	802.1Q Tagging	Virtual Switch	Virtual Network Bridge	Load Group
○	VLAN99-ETHERNET0	99	Yes	ETHERNET0(Default)		
●	VLAN1-ETHERNET0	1	No	ETHERNET0(Default)	NetworkBridge_ETHERNET0(Default)_1	LoadGroup_ETHEF
○	VLAN4-ETHERNET0	4	Yes	ETHERNET0(Default)		

	Virtual Switch	Mode

Figure 2-42 Edit system template: Virtual Networks

Modify your virtual network settings to suit your environment.

You can click **Virtual Storage** to configure a Media Repository and specify a repository size, as shown in Figure 2-43.



Virtual Storage

Assign a VIOS to a shared storage pool and configure a media repository to the VIOS specified in the template. You can also specify the size for the media repository that you have configured for the VIOS.

Shared Storage Pool Clusters

Assign the Virtual I/O Servers to a Shared Storage Pool Cluster:

VIOS_A: Choose at Deploy

Media Repositories

Configure a Media Repository on these Virtual I/O Servers:

☑ VIOS_A

Volume Group Name:rootvg

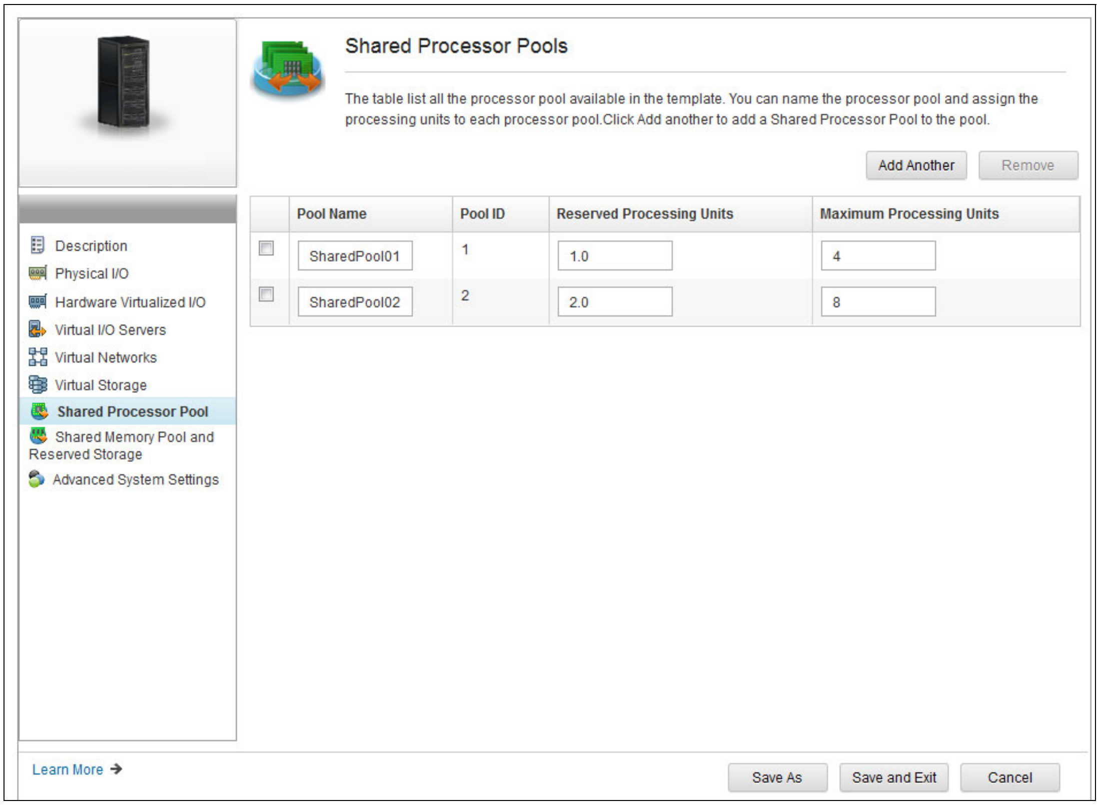
Media Repository Size: 10 GB

Figure 2-43 Edit system template: Virtual Storage

Modify the virtual storage to suit your environment.

You can click **Shared Processor Pool** to modify the assigned reserved and maximum processing units.

Additional Shared Processor Pools with assigned reserved and maximum processing units can be added to the template, as shown in Figure 2-44.



Shared Processor Pools

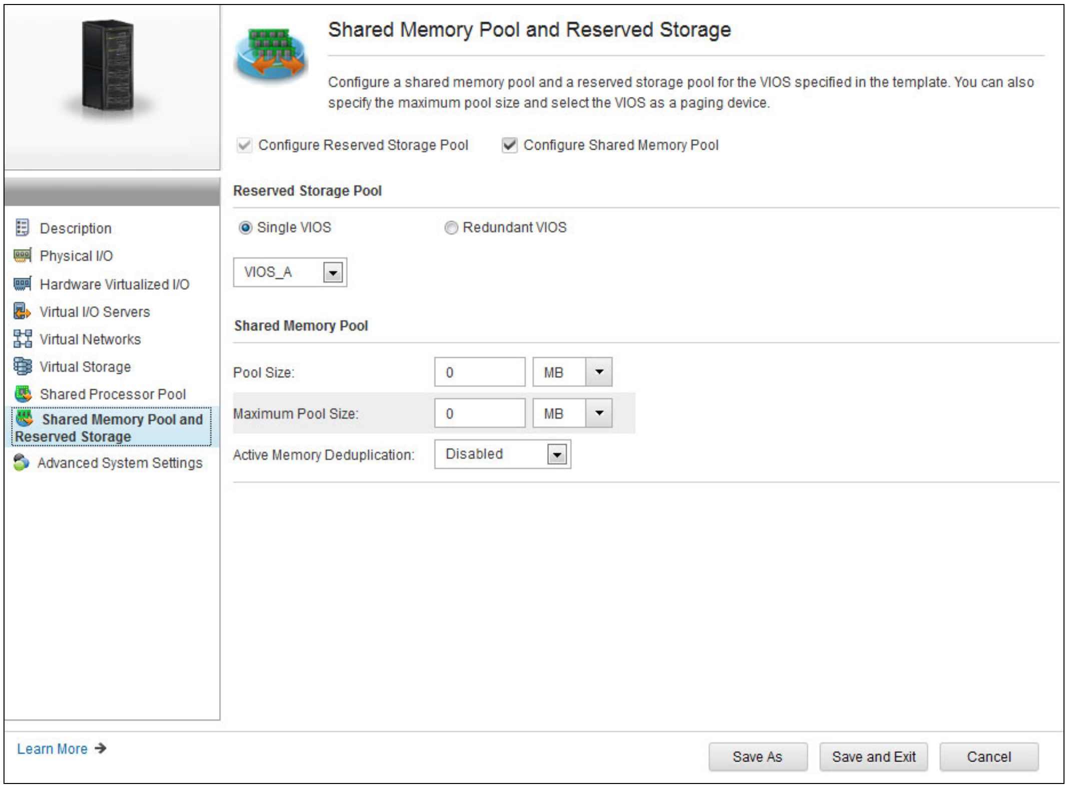
The table list all the processor pool available in the template. You can name the processor pool and assign the processing units to each processor pool.Click Add another to add a Shared Processor Pool to the pool.

	Pool Name	Pool ID	Reserved Processing Units	Maximum Processing Units
□	SharedPool01	1	1.0	4
□	SharedPool02	2	2.0	8

Figure 2-44 Edit system template: Shared Processor Pool

Modify shared processor pools to suit your environment.

You can click **Memory Pool and Reserved Storage** to modify the configured Shared Memory Pool, as shown in Figure 2-45.



Shared Memory Pool and Reserved Storage

Configure a shared memory pool and a reserved storage pool for the VIOS specified in the template. You can also specify the maximum pool size and select the VIOS as a paging device.

☑ Configure Reserved Storage Pool ☑ Configure Shared Memory Pool

Reserved Storage Pool

● Single VIOS ○ Redundant VIOS

VIOS_A

Shared Memory Pool

Pool Size: 0 MB

Maximum Pool Size: 0 MB

Active Memory Deduplication: Disabled

Figure 2-45 Edit System template: Shared Memory Pool

Modify the shared memory pool and reserved storage configurations to suit your environment.

> **Note:** Not all menu choices are shown in this section. Depending on your environment, the other menu options might be relevant and require configuration to become part of your customized system template.

2.5.11 Deploying a template

The Deploy System from Template wizard guides you in providing target system-specific information that is required to complete the deployment on to the selected system. Before you deploy a system template, be sure the following prerequisites are met:

- The HMC is at version 8.8.4.0 or later.
- The hypervisor is in the operating or standby state.
- The managed system is in the operating or standby state.
- The managed system does not have any logical partitions that are associated to it.

  If logical partitions are configured on the target system, an error message is displayed; if you continue with the deployment, the HMC completes the following actions:

  - All system level configurations are initialized to the default values.
  - All LPARs that are in the running state are shut down and removed automatically.
  - All the Virtual I/O Servers that are in the running state are shut down and removed automatically.

The wizard completes the following tasks:

- Configures the system settings, assigns I/O adapters, and creates Virtual I/O Servers.
- Installs the VIOS software.
- Configures the network and storage I/O settings.

If you install the VIOS from a Network Installation Management (NIM) server, you must have the NIM server information that is required by the HMC.

When you deploy a system from a template, the HMC checks whether the configuration that is specified meets the required system capabilities.

To deploy a system template, select the target managed system in the HMC and select **Templates** → **Deploy System from Template**, as shown in Figure 2-46.

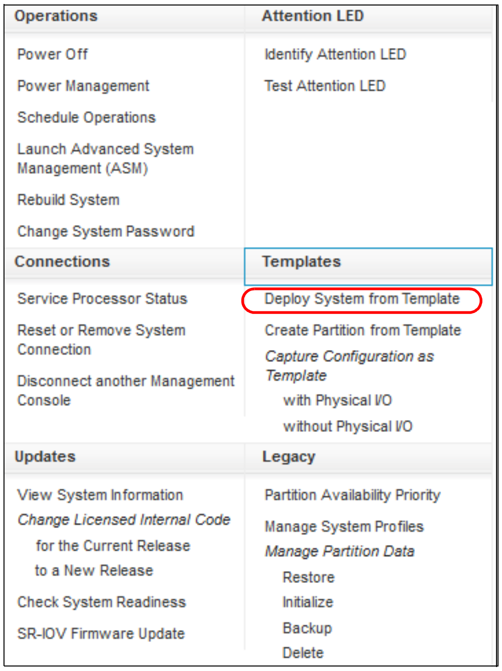
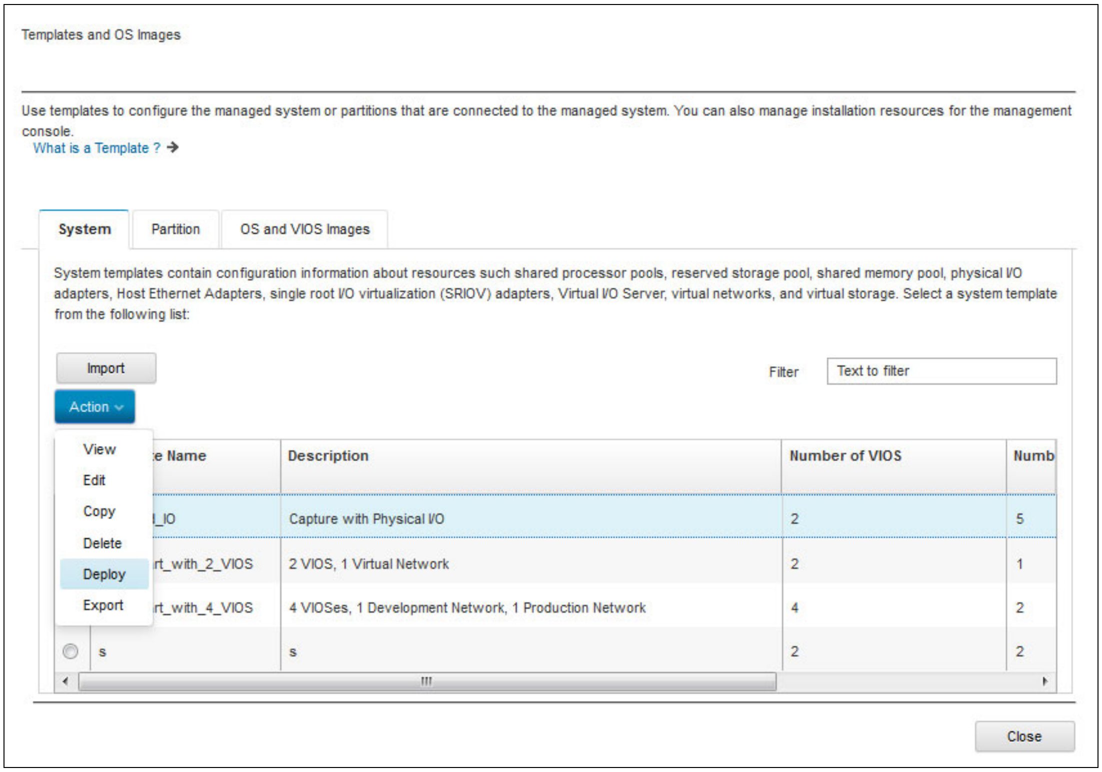


Figure 2-46 Deploy System from Template selection

Alternatively, select your system template from the Templates and OS Images, right-click the template, and select **Action** → **Deploy**, as shown in Figure 2-47.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

What is a Template ? →

System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet Adapters, single root I/O virtualization (SRIOV) adapters, Virtual I/O Server, virtual networks, and virtual storage. Select a system template from the following list:

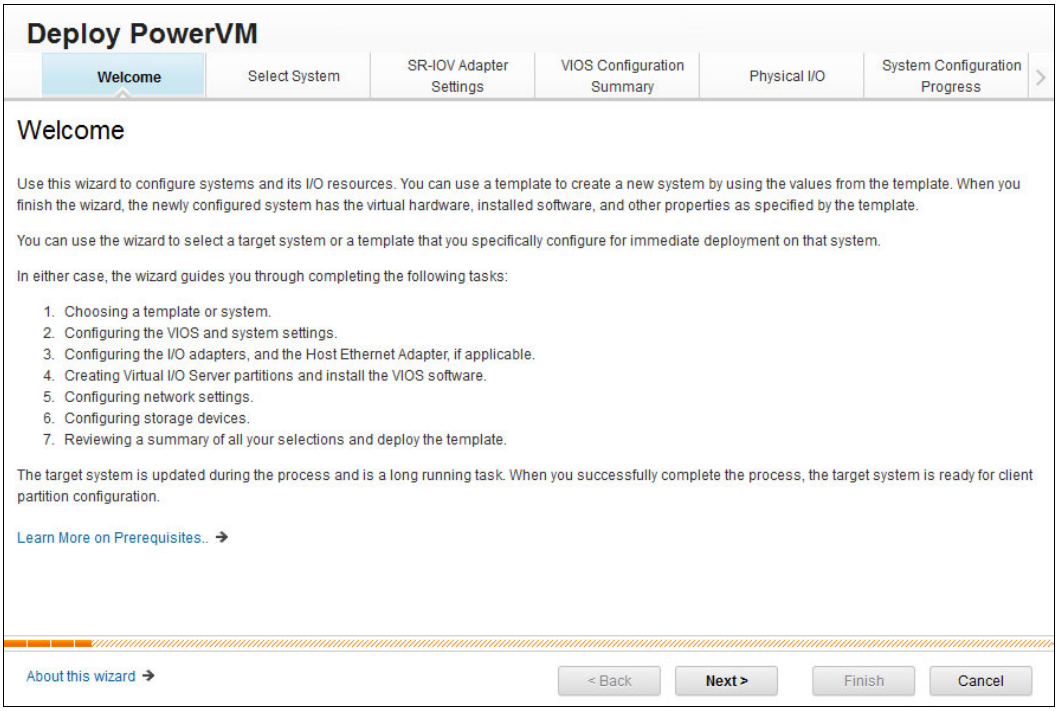
Filter: Text to filter

	e Name	Description	Number of VIOS	Numb
	l_IO	Capture with Physical I/O	2	5
	rt_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1
	rt_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2
○	s	s	2	2

Figure 2-47 Deploy: Templates and OS Images

The only difference between the two methods is that when you deploy from the Templates and OS Images window, you are prompted by the deployment wizard to select the target system.

Selecting **Deploy** on the system template starts the deployment wizard (Figure 2-48).



Deploy PowerVM

Welcome

Use this wizard to configure systems and its I/O resources. You can use a template to create a new system by using the values from the template. When you finish the wizard, the newly configured system has the virtual hardware, installed software, and other properties as specified by the template.

You can use the wizard to select a target system or a template that you specifically configure for immediate deployment on that system.

In either case, the wizard guides you through completing the following tasks:

1. Choosing a template or system.
2. Configuring the VIOS and system settings.
3. Configuring the I/O adapters, and the Host Ethernet Adapter, if applicable.
4. Creating Virtual I/O Server partitions and install the VIOS software.
5. Configuring network settings.
6. Configuring storage devices.
7. Reviewing a summary of all your selections and deploy the template.

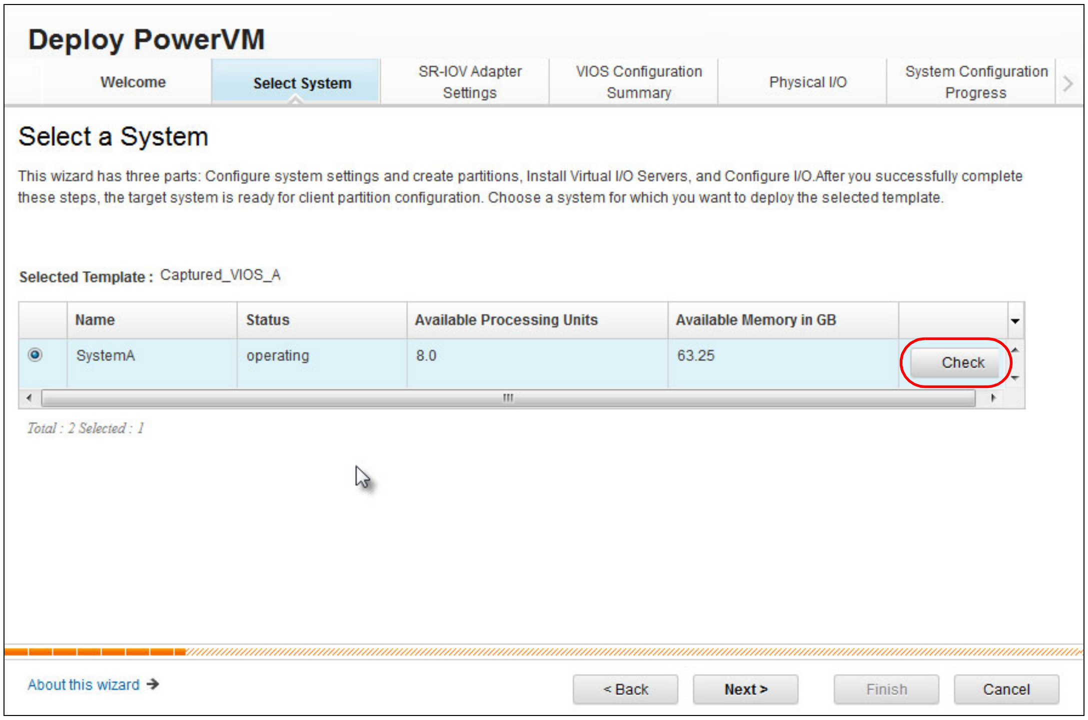
The target system is updated during the process and is a long running task. When you successfully complete the process, the target system is ready for client partition configuration.

Learn More on Prerequisites.. →

Figure 2-48 Deployment wizard

Click **Next** to move to the next tab.

You use the Select System tab to select the target system to which the template is deployed, as shown in Figure 2-49.



Deploy PowerVM

Select a System

This wizard has three parts: Configure system settings and create partitions, Install Virtual I/O Servers, and Configure I/O.After you successfully complete these steps, the target system is ready for client partition configuration. Choose a system for which you want to deploy the selected template.

Selected Template : Captured_VIOS_A

	Name	Status	Available Processing Units	Available Memory in GB	
●	SystemA	operating	8.0	63.25	Check

Total : 2 Selected : 1

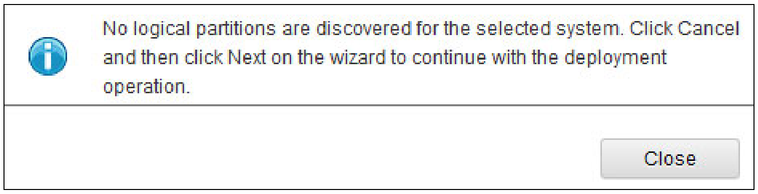
Figure 2-49 Deploy: Select a System

If you selected **Deploy System from Template** on the HMC work pane, the system is preselected in the Select System tab and you must select the system template that is used for the deployment.

When you select a target system, the **Check** option becomes available, as highlighted in Figure 2-49 on page 94.

Note: Click **Check** because the system must be reset to the manufacturer's default configuration as part of the system template deployment wizard.

The target system also is checked for available logical partitions, which are removed, as with the tasks that are involved with deploying a system from a system template. The target system that is selected for the deployment that is detailed in this section has no partitions that are configured (Figure 2-50) and had the **Check** option selected.



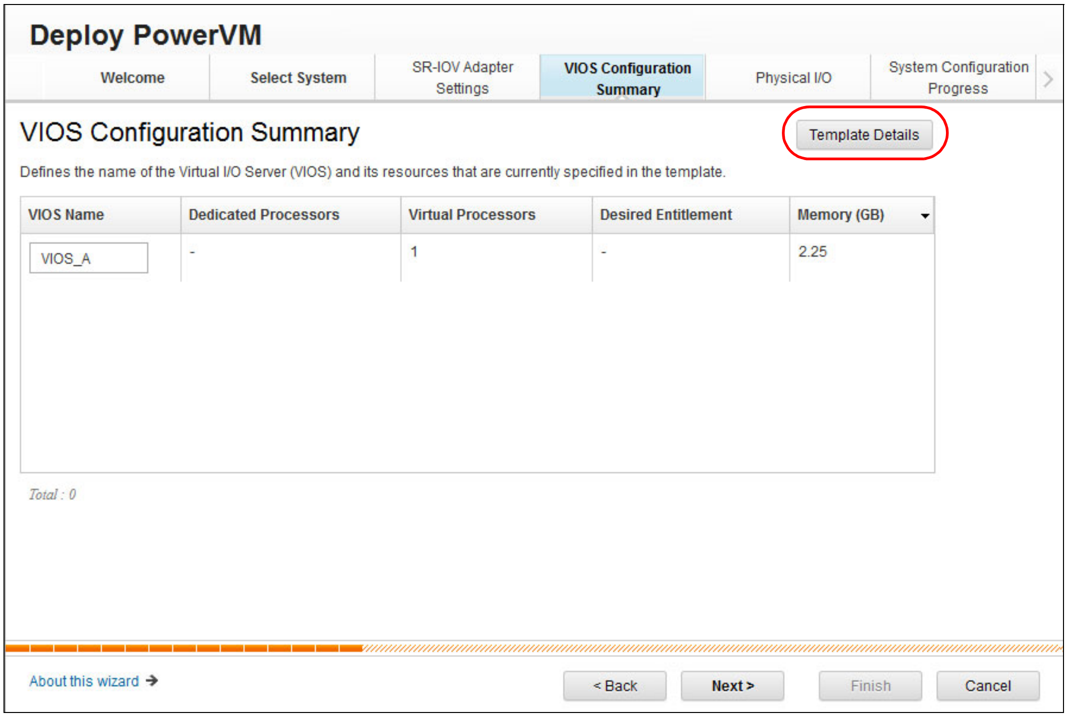
No logical partitions are discovered for the selected system. Click Cancel and then click Next on the wizard to continue with the deployment operation.

Figure 2-50 Deploy: Check target system

Close this window and click **Next** to move to the next tab.

The deployment wizard checks the target system for available resources.

As shown in Figure 2-51, the SR-IOV Adapter Settings tab is skipped because the selected system has no SR-IOV capable adapters. The VIOS Configuration Summary tab shows the VIOS configuration that is specified by the system template. To review the template, click **Template Details**.



VIOS Configuration Summary

Defines the name of the Virtual I/O Server (VIOS) and its resources that are currently specified in the template.

VIOS Name	Dedicated Processors	Virtual Processors	Desired Entitlement	Memory (GB)
VIOS_A	-	1	-	2.25

Total : 0

Figure 2-51   Deploy: VIOS Configuration Summary

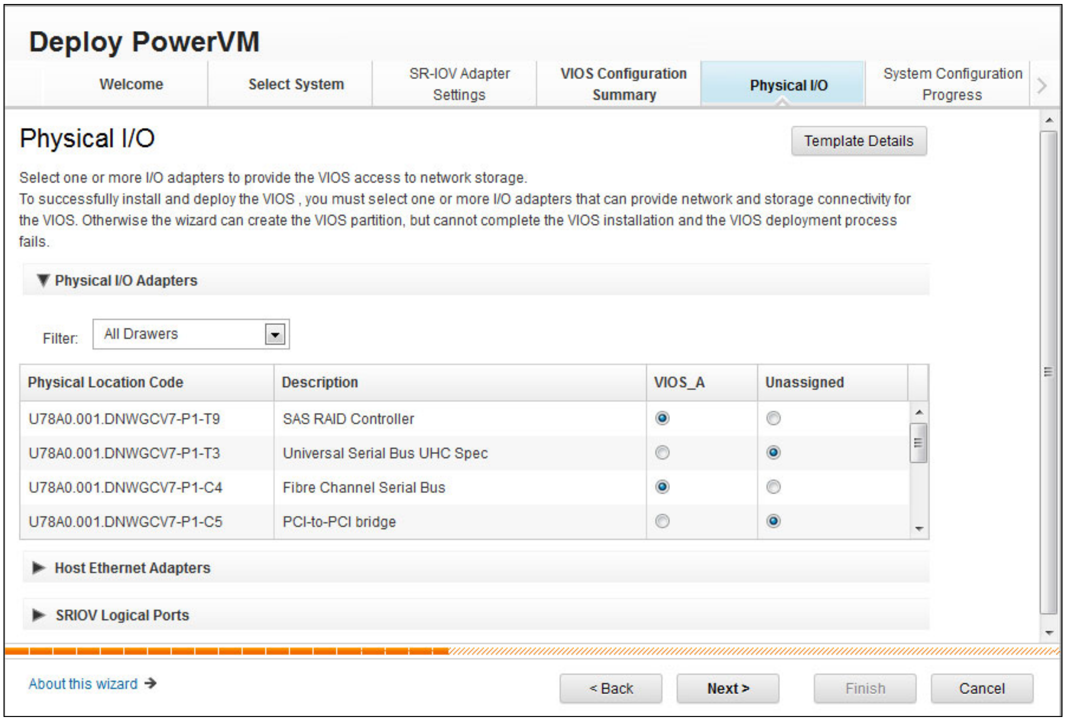
The template can be viewed only when you click **Template Details**, as described in 2.5.8, “Viewing a system template” on page 74.

If you want to edit the template details, cancel the deployment wizard, edit the system template, and then recommence with the deployment wizard.

The system template in this example has only one VIOS specified; a template with an additional VIOS displays the second VIOS server in this tab.

Click **Next** to move to the next tab.

You use the Physical I/O tab to select the physical resources on the target system that will be allocated to the VIOS. Expanding **Physical I/O Adapters** displays the available physical resources on the target system, as shown in Figure 2-52.



Physical I/O

Select one or more I/O adapters to provide the VIOS access to network storage.
To successfully install and deploy the VIOS , you must select one or more I/O adapters that can provide network and storage connectivity for the VIOS. Otherwise the wizard can create the VIOS partition, but cannot complete the VIOS installation and the VIOS deployment process fails.

Filter: All Drawers

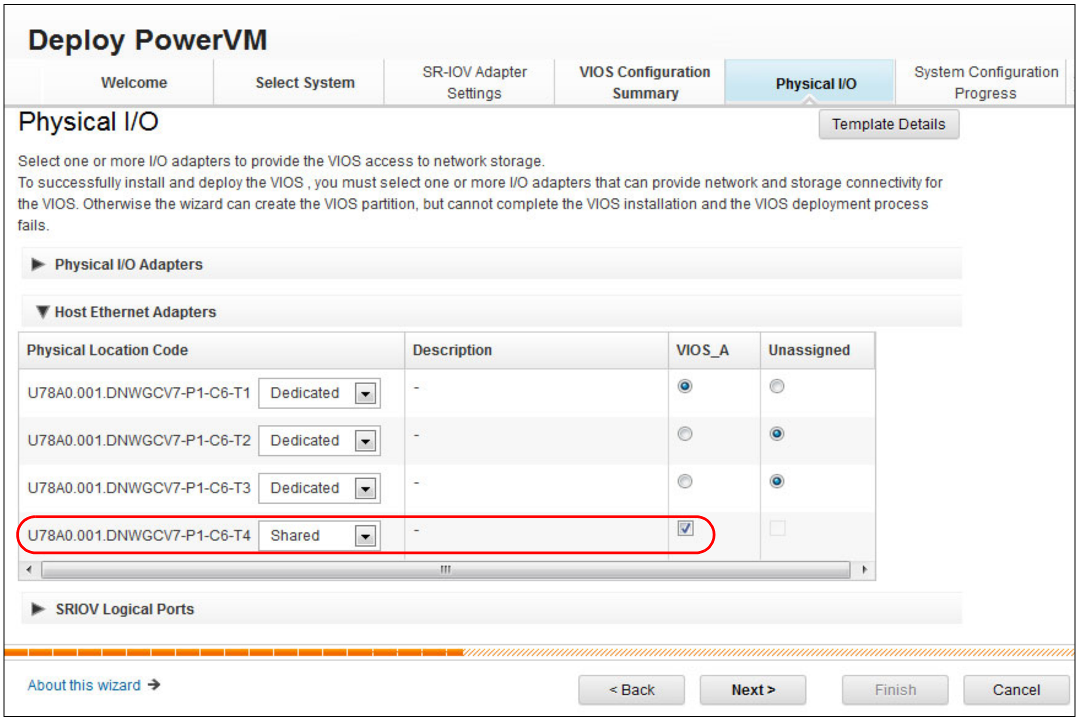
Physical Location Code	Description	VIOS_A	Unassigned
U78A0.001.DNWGCV7-P1-T9	SAS RAID Controller	●	○
U78A0.001.DNWGCV7-P1-T3	Universal Serial Bus UHC Spec	○	●
U78A0.001.DNWGCV7-P1-C4	Fibre Channel Serial Bus	●	○
U78A0.001.DNWGCV7-P1-C5	PCI-to-PCI bridge	○	●

Figure 2-52 Deploy: Physical I/O

Select the resources to suit your environment by selecting the radio button next to the required resource.

Expanding **Host Ethernet Adapters** displays the HEA resources that are available on the target system.

As shown in Figure 2-53, an HEA port can be either a Dedicated or Shared resource. Select the drop-down box next to the required port and assign the port to the VIOS. If the VIOS will share a HEA port, set the required port as a Shared resource and select the check box next to the HEA that you want to assign to the VIOS.



Physical I/O

Select one or more I/O adapters to provide the VIOS access to network storage.
To successfully install and deploy the VIOS , you must select one or more I/O adapters that can provide network and storage connectivity for the VIOS. Otherwise the wizard can create the VIOS partition, but cannot complete the VIOS installation and the VIOS deployment process fails.

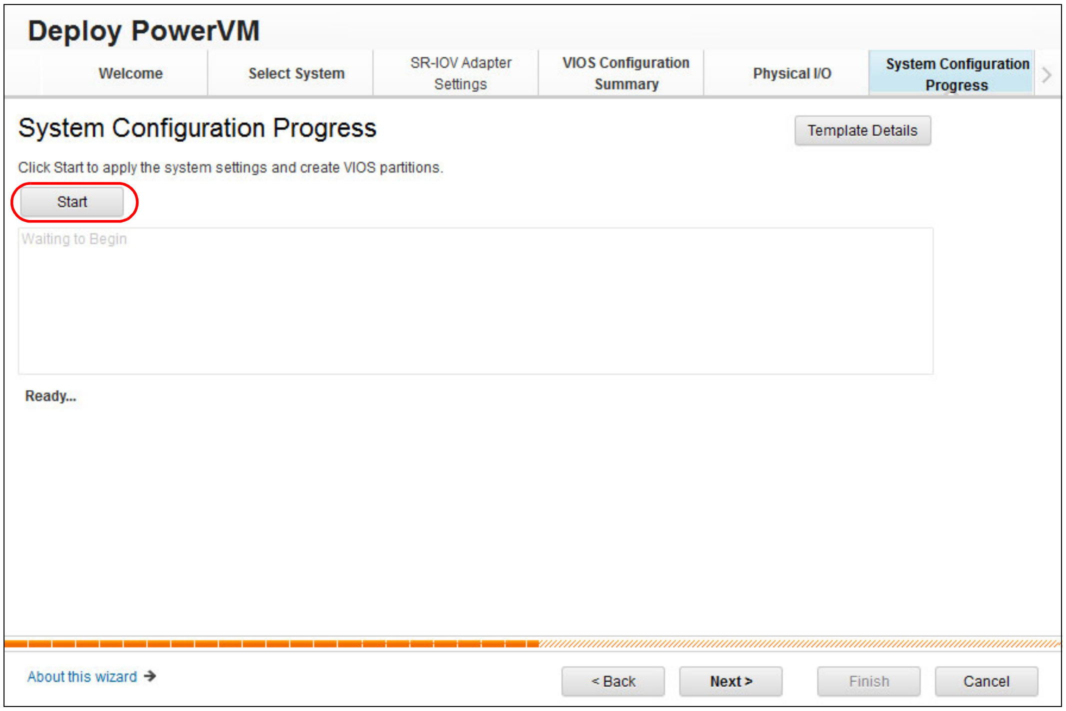
Physical Location Code		Description	VIOS_A	Unassigned
U78A0.001.DNWGCV7-P1-C6-T1	Dedicated	-	●	○
U78A0.001.DNWGCV7-P1-C6-T2	Dedicated	-	○	●
U78A0.001.DNWGCV7-P1-C6-T3	Dedicated	-	○	●
U78A0.001.DNWGCV7-P1-C6-T4	Shared	-	☑	□

Figure 2-53 Deploy: Physical I/O - HEA

HEAs and SR-IOV Logical Ports display resources only if they are supported by your target system.

Select the resources to suit your environment and click **Next** to move to the next tab.

You use the System Configuration Progress tab to apply system settings to the target system and create the VIOS partition. Click **Start** to begin this process (Figure 2-54).


Deploy PowerVM

System Configuration Progress

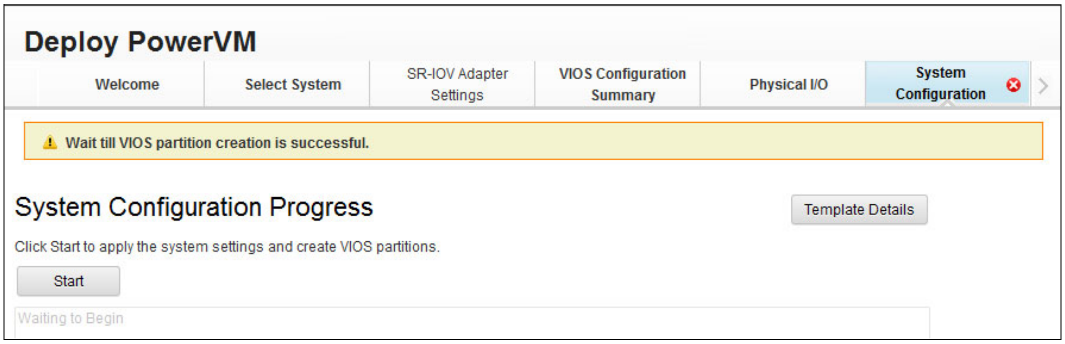
Click Start to apply the system settings and create VIOS partitions.

Waiting to Begin

Ready...

Figure 2-54 Deploy: System Configuration Progress

If you *do not* click **Start** but click **Next** instead, an error prompt opens in the deployment wizard window (Figure 2-55).


Deploy PowerVM

Wait till VIOS partition creation is successful.

System Configuration Progress

Click Start to apply the system settings and create VIOS partitions.

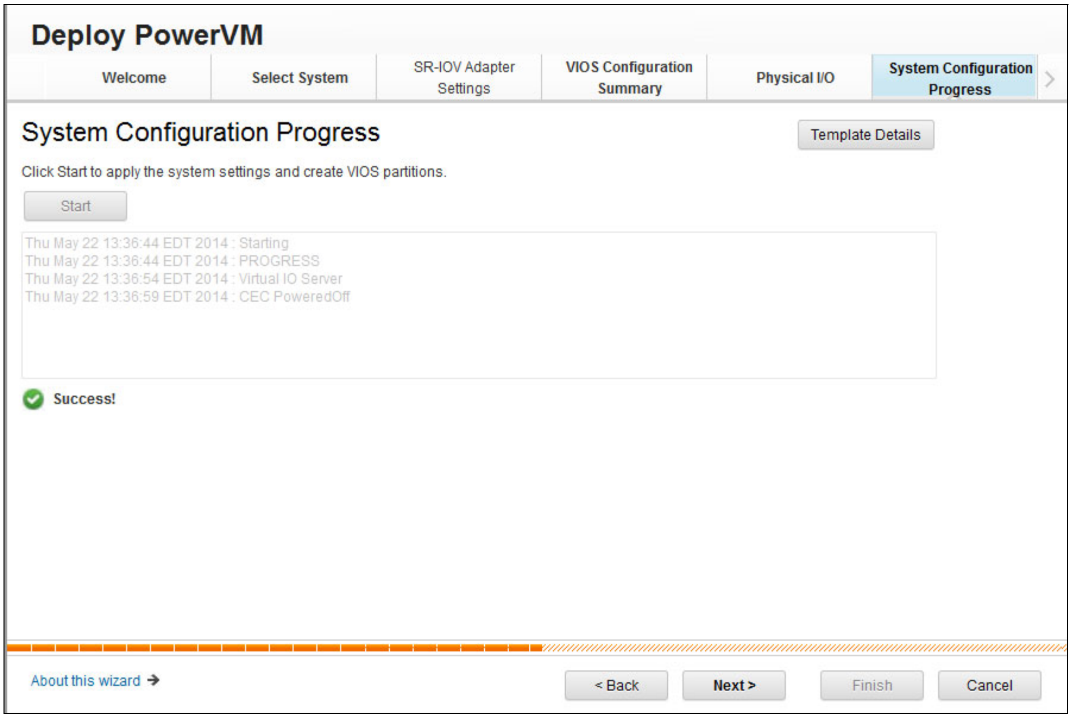
Waiting to Begin

Figure 2-55 Deploy: System Configuration Progress - error

Click **Start** to apply the system settings and to create the VIOS partition.

The template deployment wizard applies the system configuration and creates the VIOS partition on the target system.

The deployment shows the successful creation of a VIOS partition on the target system (Figure 2-56).



System Configuration Progress

Click Start to apply the system settings and create VIOS partitions.

```
Thu May 22 13:36:44 EDT 2014 : Starting
Thu May 22 13:36:44 EDT 2014 : PROGRESS
Thu May 22 13:36:54 EDT 2014 : Virtual IO Server
Thu May 22 13:36:59 EDT 2014 : CEC PoweredOff
```

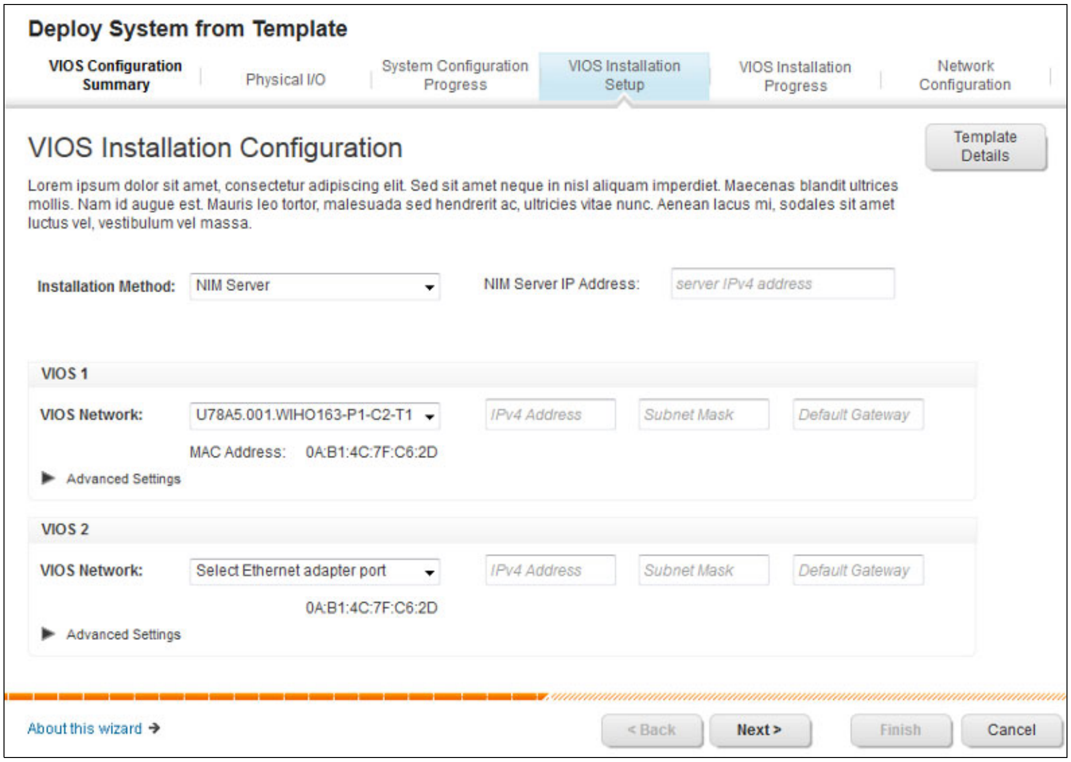
✓ Success!

Figure 2-56 Deploy: System Configuration Progress - success

Click **Next** to move to the next tab.

You use the VIOS Installation Configuration tab to select the installation method for VIOS. If you use a NIM server for installation, you need the appropriate authentication credentials.

For each VIOS server, specify the Ethernet port and TCP/IP configuration, as shown in Figure 2-57.



Deploy System from Template

VIOS Installation Configuration

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed sit amet neque in nisl aliquam imperdiet. Maecenas blandit ultrices mollis. Nam id augue est. Mauris leo tortor, malesuada sed hendrerit ac, ultricies vitae nunc. Aenean lacus mi, sodales sit amet luctus vel, vestibulum vel massa.

Installation Method: NIM Server NIM Server IP Address: server IPv4 address

VIOS 1

VIOS Network: U78A5.001.WIHO163-P1-C2-T1 IPv4 Address Subnet Mask Default Gateway

MAC Address: 0A:B1:4C:7F:C6:2D

VIOS 2

VIOS Network: Select Ethernet adapter port IPv4 Address Subnet Mask Default Gateway

0A:B1:4C:7F:C6:2D

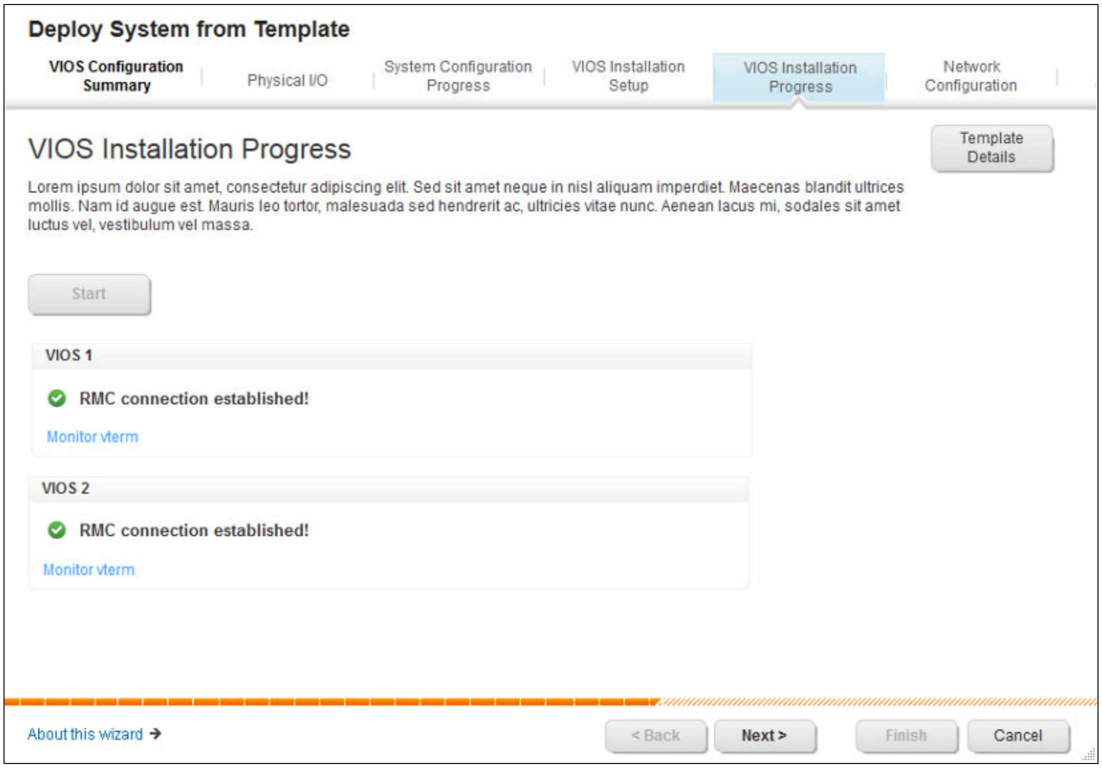
Figure 2-57 Deploy: VIOS Installation Configuration

Select the resources and TCP/IP configuration to suit your environment.

Click **Next** to move to the next tab.

You use the VIOS Installation Progress tab to establish a Resource Monitoring and Control (RMC) connection between the HMC and VIOS logical partition.

Click **Start** to establish the RMC connection, as shown in Figure 2-58.



Deploy System from Template

VIOS Configuration Summary
Physical I/O
System Configuration Progress
VIOS Installation Setup
VIOS Installation Progress
Network Configuration
Template Details

VIOS Installation Progress

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed sit amet neque in nisl aliquam imperdiet. Maecenas blandit ultrices mollis. Nam id augue est. Mauris leo tortor, malesuada sed hendrerit ac, ultricies vitae nunc. Aenean lacus mi, sodales sit amet luctus vel, vestibulum vel massa.

VIOS 1

✓ RMC connection established!

Monitor vterm

VIOS 2

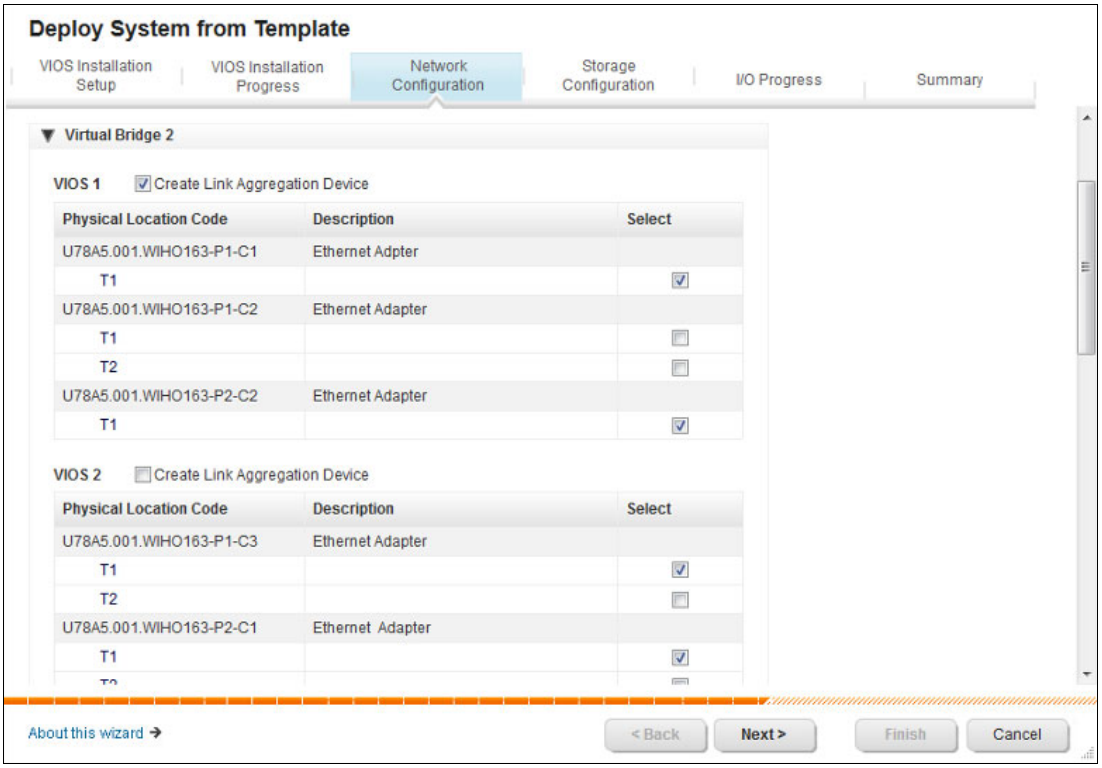
✓ RMC connection established!

Monitor vterm

Figure 2-58 Deploy: VIOS Installation Progress

After the RMC connection is established, click **Next** to move to the next tab.

You use the Network Bridge Configuration tab to set up network bridges, as shown in Figure 2-59.



Deploy System from Template

▼ Virtual Bridge 2

VIOS 1 ☑ Create Link Aggregation Device

Physical Location Code	Description	Select
U78A5.001.WIHO163-P1-C1	Ethernet Adpter	
T1		☑
U78A5.001.WIHO163-P1-C2	Ethernet Adapter	
T1		□
T2		□
U78A5.001.WIHO163-P2-C2	Ethernet Adapter	
T1		☑

VIOS 2 □ Create Link Aggregation Device

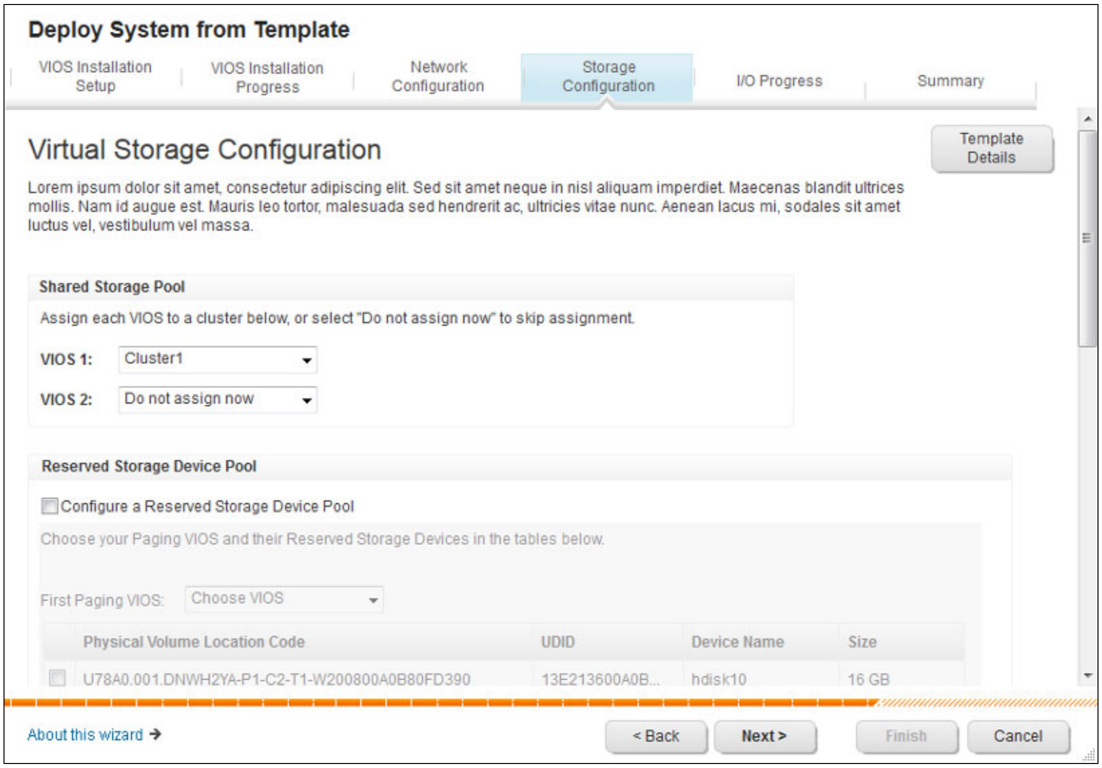
Physical Location Code	Description	Select
U78A5.001.WIHO163-P1-C3	Ethernet Adapter	
T1		☑
T2		□
U78A5.001.WIHO163-P2-C1	Ethernet Adapter	
T1		☑

Figure 2-59 Deploy: Network bridge configuration

Select the resources to suit your environment and click **Next** to move to the next tab.

You use the Storage Configuration tab to create and configure a Shared Storage Pool if one is required by your environment.

A Reserved Storage Device Pool can be configured, as shown in Figure 2-60.



Virtual Storage Configuration

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed sit amet neque in nisl aliquam imperdiet. Maecenas blandit ultrices mollis. Nam id augue est. Mauris leo tortor, malesuada sed hendrerit ac, ultricies vitae nunc. Aenean lacus mi, sodales sit amet luctus vel, vestibulum vel massa.

Shared Storage Pool

Assign each VIOS to a cluster below, or select "Do not assign now" to skip assignment.

VIOS 1: Cluster1

VIOS 2: Do not assign now

Reserved Storage Device Pool

□ Configure a Reserved Storage Device Pool

Choose your Paging VIOS and their Reserved Storage Devices in the tables below.

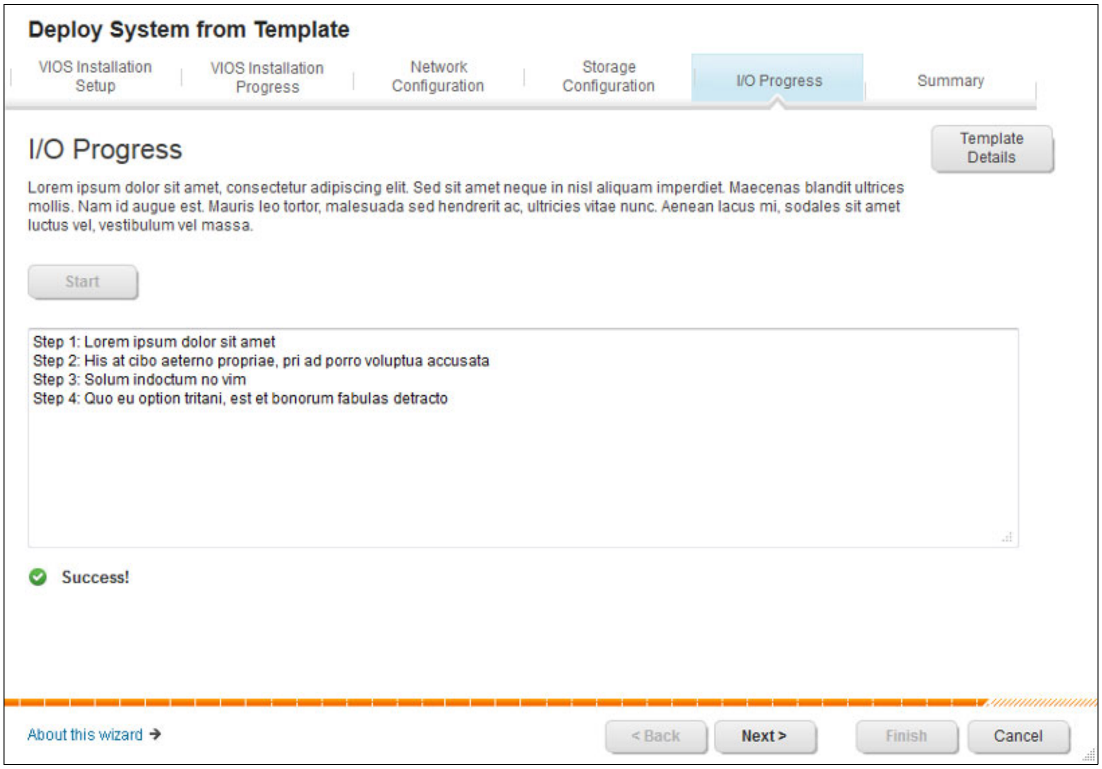
First Paging VIOS: Choose VIOS

	Physical Volume Location Code	UDID	Device Name	Size
□	U78A0.001.DNWH2YA-P1-C2-T1-W200800A0B80FD390	13E213600A0B...	hdisk10	16 GB

Figure 2-60 Deploy: Reserved Storage Device configuration

Configure the virtual storage to suit your environment and click **Next** to move to the next tab.

The I/O Progress tab shows the progress of the VIOS configuration on the target system after you click **Start**, as shown in Figure 2-61. The deployment wizard displays the progress of the VIOS installation and the configuration of virtual storage, as specified in the Storage Configuration tab of the wizard.



I/O Progress

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed sit amet neque in nisl aliquam imperdiet. Maecenas blandit ultrices mollis. Nam id augue est. Mauris leo tortor, malesuada sed hendrerit ac, ultricies vitae nunc. Aenean lacus mi, sodales sit amet luctus vel, vestibulum vel massa.

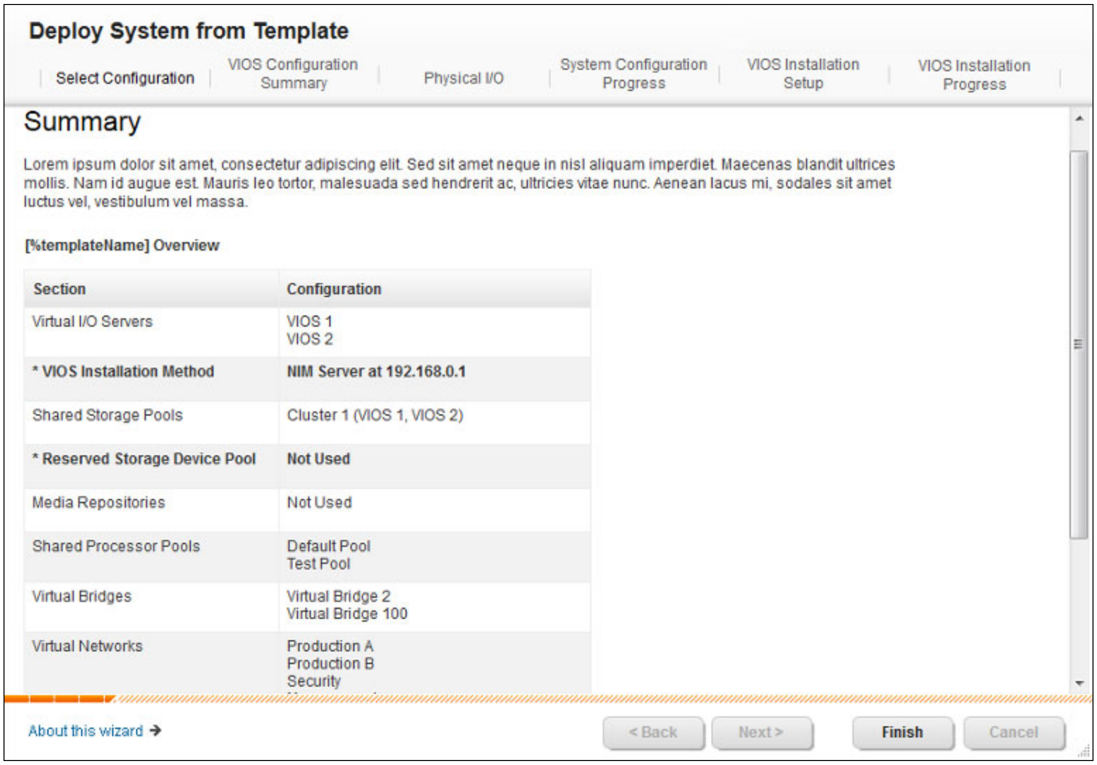
```
Step 1: Lorem ipsum dolor sit amet
Step 2: His at cibo aeterno propriae, pri ad porro voluptua accusata
Step 3: Solum indoctum no vim
Step 4: Quo eu option tritani, est et bonorum fabulas detracto
```

✓ Success!

Figure 2-61 Deploy: I/O Progress tab

The deployment wizard shows the successful creation of a VIOS running on the target system.

Click **Next** to move to the Summary tab, which shows the results of the wizard (Figure 2-62).


Deploy System from Template
Select Configuration
VIOS Configuration Summary
Physical I/O
System Configuration Progress
VIOS Installation Setup
VIOS Installation Progress
About this wizard ➔
< Back
Next >
Finish
Cancel

Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed sit amet neque in nisl aliquam imperdiet. Maecenas blandit ultrices mollis. Nam id augue est. Mauris leo tortor, malesuada sed hendrerit ac, ultricies vitae nunc. Aenean lacus mi, sodales sit amet luctus vel, vestibulum vel massa.

[%templateName] Overview

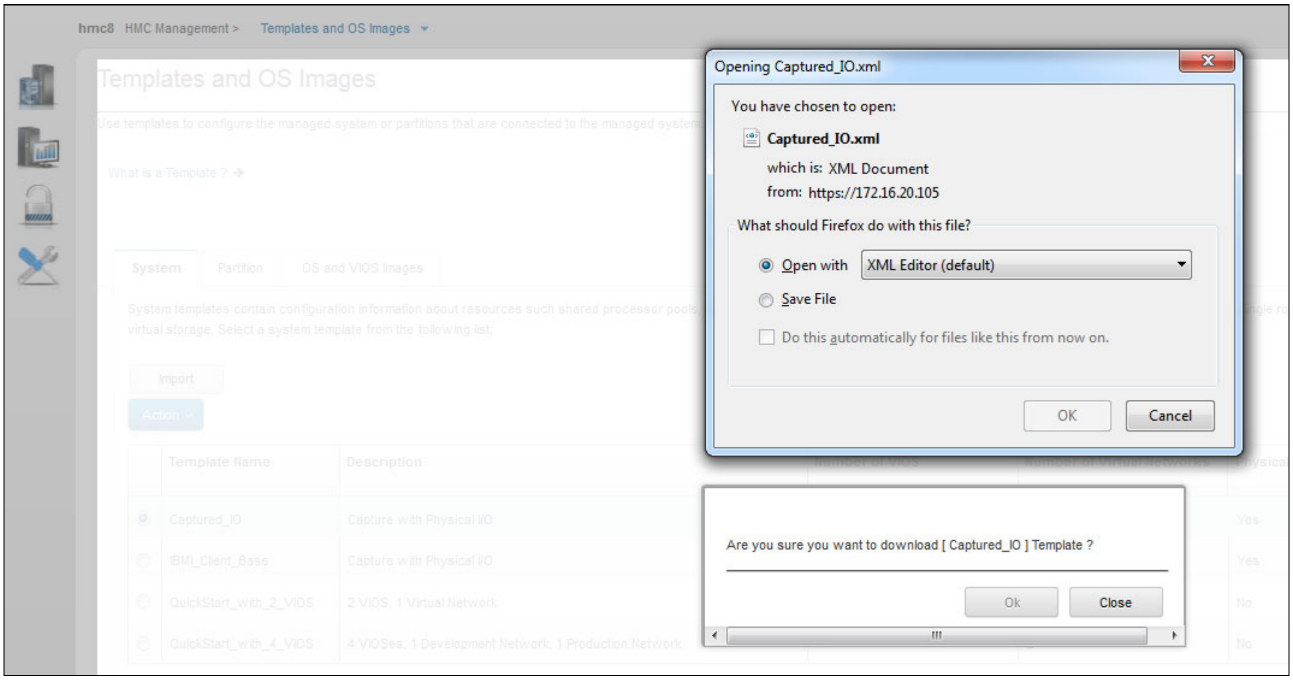
Section	Configuration
Virtual I/O Servers	VIOS 1 VIOS 2
*** VIOS Installation Method**	**NIM Server at 192.168.0.1**
Shared Storage Pools	Cluster 1 (VIOS 1, VIOS 2)
*** Reserved Storage Device Pool**	**Not Used**
Media Repositories	Not Used
Shared Processor Pools	Default Pool Test Pool
Virtual Bridges	Virtual Bridge 2 Virtual Bridge 100
Virtual Networks	Production A Production B Security

Figure 2-62 Deploy: Summary

At this stage, the target system has a running VIOS with your configuration and is ready to accept VIOS client logical partition connections, which can be created by using partition templates (for more information, see 2.6, “Partition templates” on page 108).

2.5.12 Exporting a system template

The new template functions of the HMC can export your system template configuration. To do so, select your template in the Templates and OS Images, right-click your system template, and select **Export**. A dialog box opens, as shown in Figure 2-63.



Opening Captured_IO.xml

You have chosen to open:

Captured_IO.xml

which is: XML Document

from: https://172.16.20.105

What should Firefox do with this file?

● Open with XML Editor (default)

○ Save File

□ Do this automatically for files like this from now on.

OK Cancel

Are you sure you want to download [Captured_IO] Template ?

Ok Close

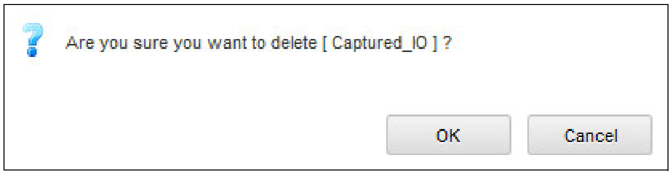
Figure 2-63 Export of system template

You can use this function to export your template configuration to another HMC that supports templates. To do so, click **Export** in the Templates and OS Images.

You also can use this function as an off-site type backup of your customized templates.

2.5.13 Deleting a system template

The template functions of the HMC can delete your template configuration. To do so, select your system template in the Templates and OS Images, right-click your template, and select **Delete**. A dialog box opens, as shown in Figure 2-64.



Are you sure you want to delete [Captured_IO] ?

OK Cancel

Figure 2-64 Delete a system template

2.6 Partition templates

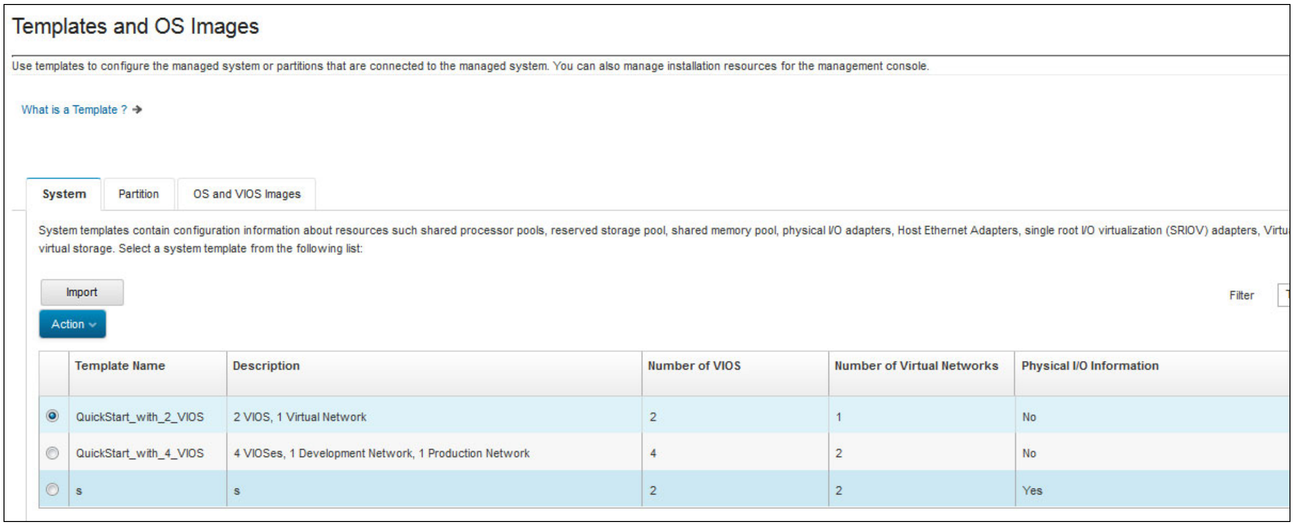
With HMC V8.8.4.0, you can create an AIX, IBM i, or Linux logical partition from any predefined or custom template in the Templates and OS Images.

The managed system must be in a running state before you can create a logical partition from a template on that managed system. You cannot create a partition from a template when the server is in a powered off state.

> **Notes:**
>
> - You can choose to work with one template at a time, whether you are editing, viewing, or deploying a template.
> - You can select only one system at a time when deploying a partition template.

2.6.1 Viewing templates

To view templates from the HMC, select your managed system from the navigator pane and, at the bottom of the work pane, expand **Templates**, as shown in Figure 2-65.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

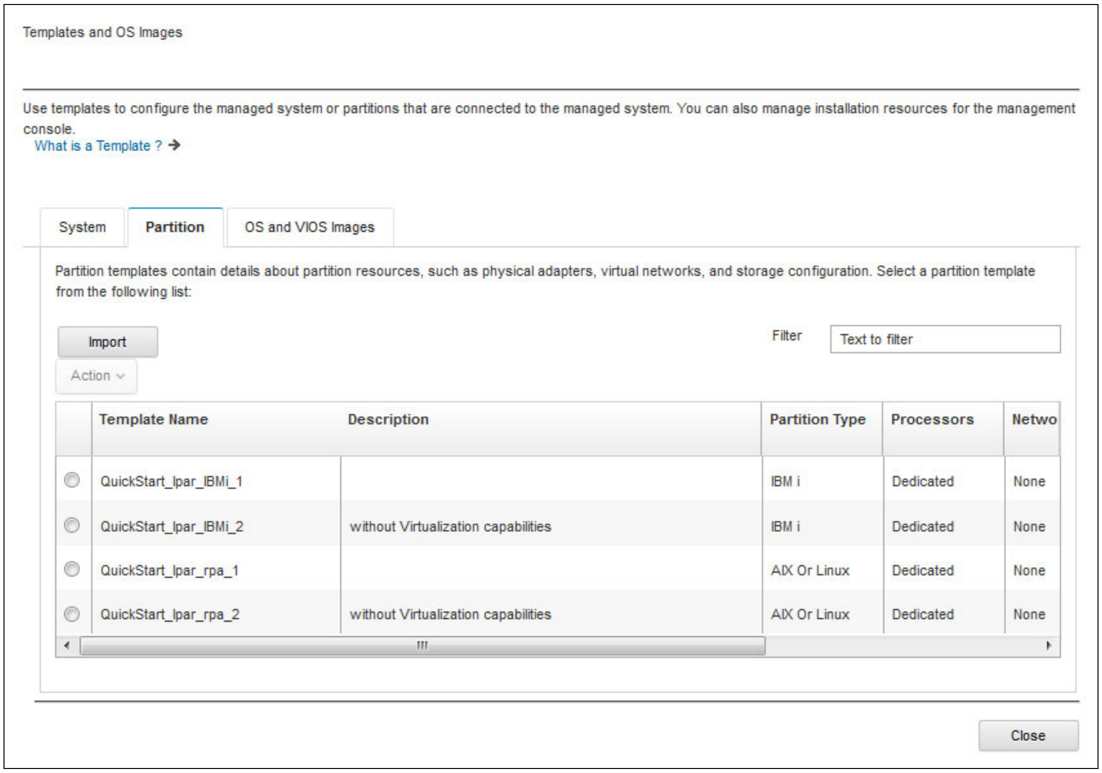
System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet Adapters, single root I/O virtualization (SRIOV) adapters, Virtu virtual storage. Select a system template from the following list:

	Template Name	Description	Number of VIOS	Number of Virtual Networks	Physical I/O Information
●	QuickStart_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1	No
○	QuickStart_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2	No
○	s	s	2	2	Yes

Figure 2-65 Template menu

Complete the following steps:

1. Click **Templates and OS Images**. A new window opens, where you can view the available templates. Click the **Partition** tab, as shown in Figure 2-66.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

What is a Template ? ➔

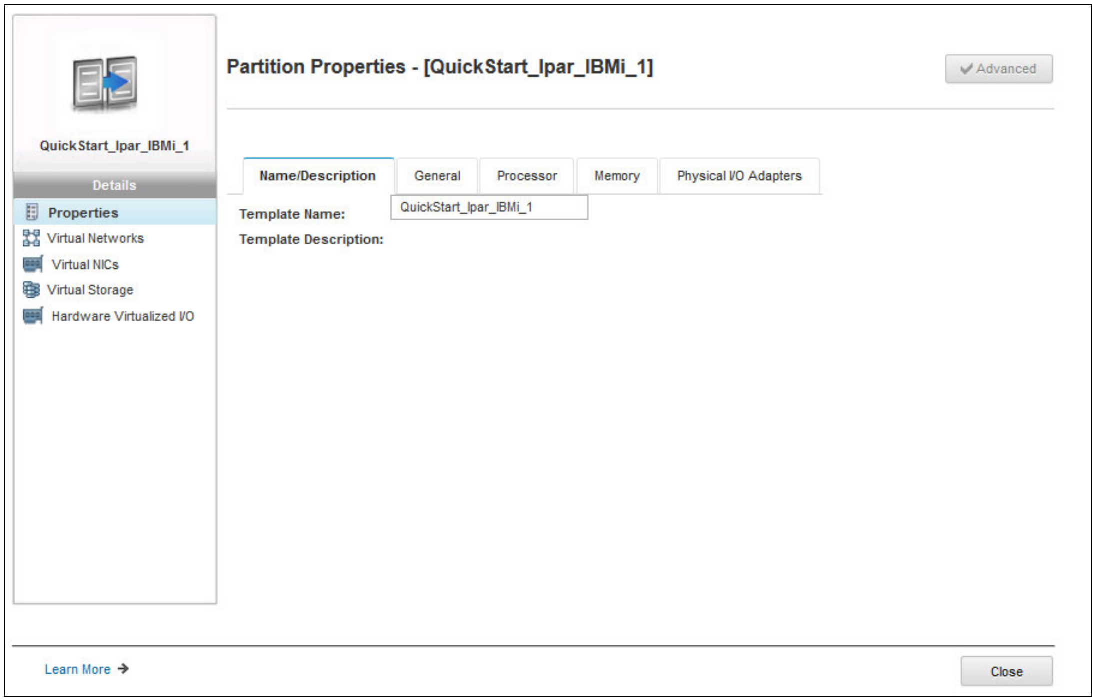
Partition templates contain details about partition resources, such as physical adapters, virtual networks, and storage configuration. Select a partition template from the following list:

	Template Name	Description	Partition Type	Processors	Netwo
○	QuickStart_lpar_IBMi_1		IBM i	Dedicated	None
○	QuickStart_lpar_IBMi_2	without Virtualization capabilities	IBM i	Dedicated	None
○	QuickStart_lpar_rpa_1		AIX Or Linux	Dedicated	None
○	QuickStart_lpar_rpa_2	without Virtualization capabilities	AIX Or Linux	Dedicated	None

Figure 2-66 View the template

2. Right-click the template that you want to view and see the available options for the template.

3. Click **View** to display the initial template window, where you can navigate to the required option and view its properties (Figure 2-67). When you finish with this view, click **Close**.



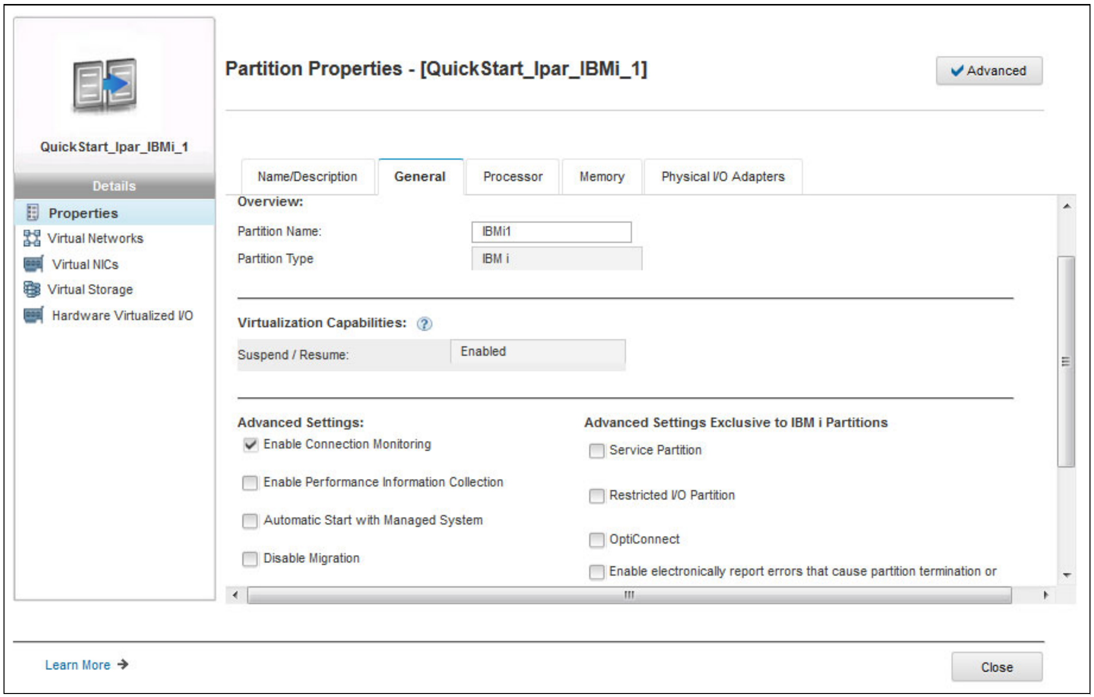
Partition Properties - [QuickStart_lpar_IBMi_1]

Template Name: QuickStart_lpar_IBMi_1

Template Description:

Figure 2-67 View template: Properties - Name

Click the **General** tab and then click **Show Advanced** to open the window that displays the advanced properties of the template (Figure 2-68).



Partition Properties - [QuickStart_lpar_IBMi_1]

Overview:

Partition Name: IBMi1

Partition Type IBM i

Virtualization Capabilities: ?

Suspend / Resume: Enabled

Advanced Settings:

☑ Enable Connection Monitoring

☐ Enable Performance Information Collection

☐ Automatic Start with Managed System

☐ Disable Migration

Advanced Settings Exclusive to IBM i Partitions

☐ Service Partition

☐ Restricted I/O Partition

☐ OptiConnect

☐ Enable electronically report errors that cause partition termination or

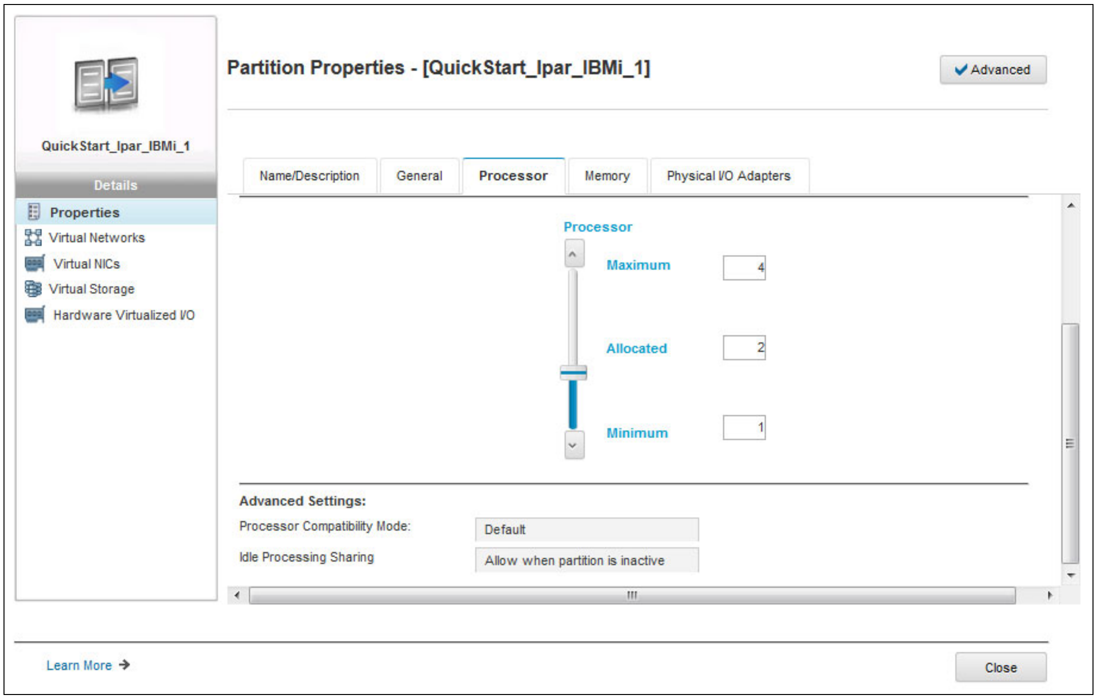
Figure 2-68 View template: Properties - General tab

Notes:

- When you deploy the template to create a logical partition profile, the template's assigned values are imported into the profile.
- To see the advanced options for each tab, click **Show Advanced**, and each tab displays its advanced options when it is opened.

Click the **Processor** tab to show the processor configuration that is specified by this template.

As shown in Figure 2-69, this template is configured for Dedicated mode with assigned values and a default Processor Compatibility Mode. If you want to change the Processor mode to, for example, Shared Mode, you must edit the template, which is described in 2.6.3, "Editing templates" on page 116.



Partition Properties - [QuickStart_lpar_IBMi_1]

Processor

Maximum 4

Allocated 2

Minimum 1

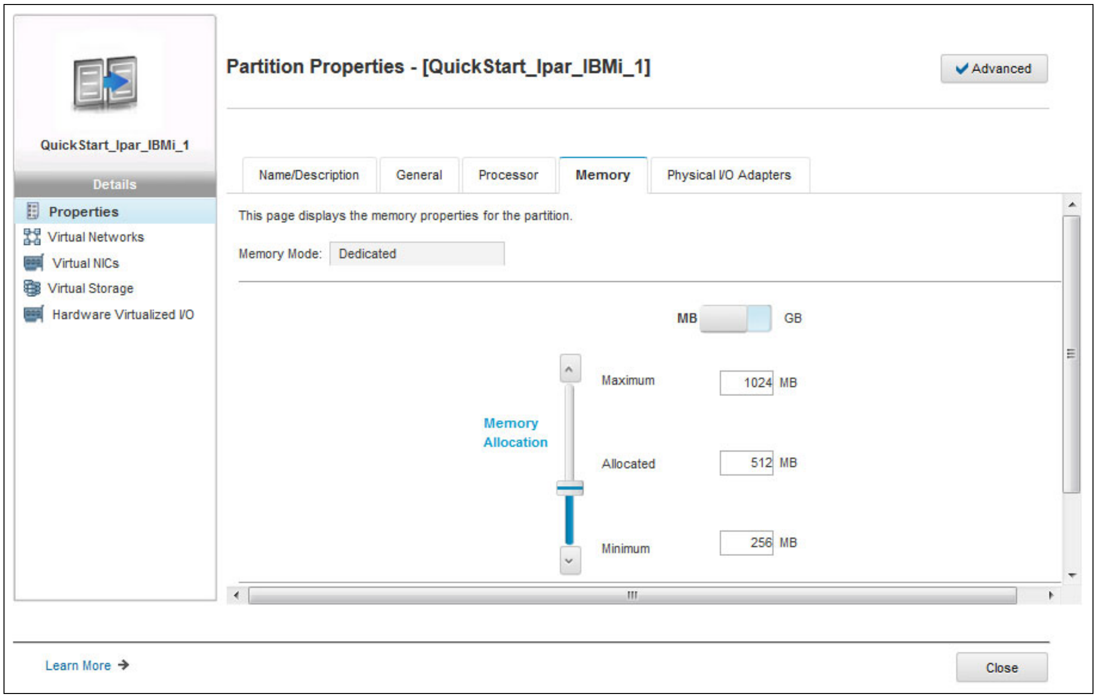
Advanced Settings:

Processor Compatibility Mode: Default

Idle Processing Sharing: Allow when partition is inactive

Figure 2-69 View template: Properties - Processors tab

Click the **Memory** tab to show the memory configuration that is specified by this template, which is shown in Figure 2-70.



Partition Properties - [QuickStart_lpar_IBMi_1]

This page displays the memory properties for the partition.

Memory Mode: Dedicated

Maximum 1024 MB

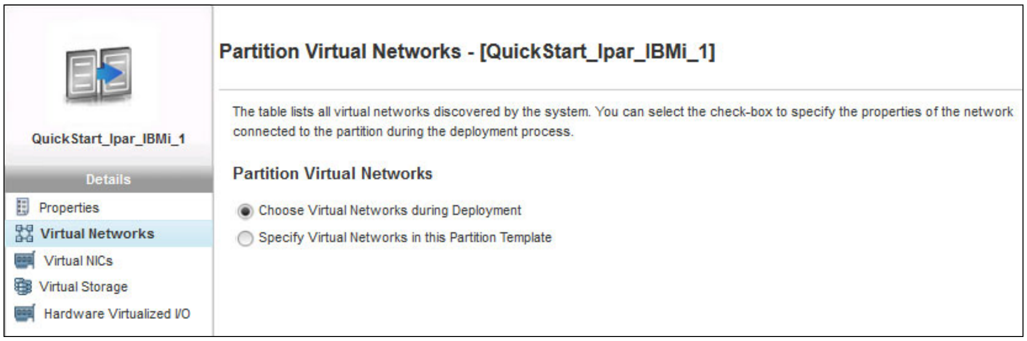
Allocated 512 MB

Minimum 256 MB

Figure 2-70 View template: Properties - Memory tab

If you click **Virtual Networks** in the Template View window, you can see whether the template is configured for either of the following mode options, which are shown in Figure 2-71:

- Choose Virtual Networks during Deployment
- Specify Virtual Networks in this Partition Template



Partition Virtual Networks - [QuickStart_lpar_IBMi_1]

The table lists all virtual networks discovered by the system. You can select the check-box to specify the properties of the network connected to the partition during the deployment process.

Partition Virtual Networks

● Choose Virtual Networks during Deployment

○ Specify Virtual Networks in this Partition Template

Figure 2-71 View template: Virtual Networks

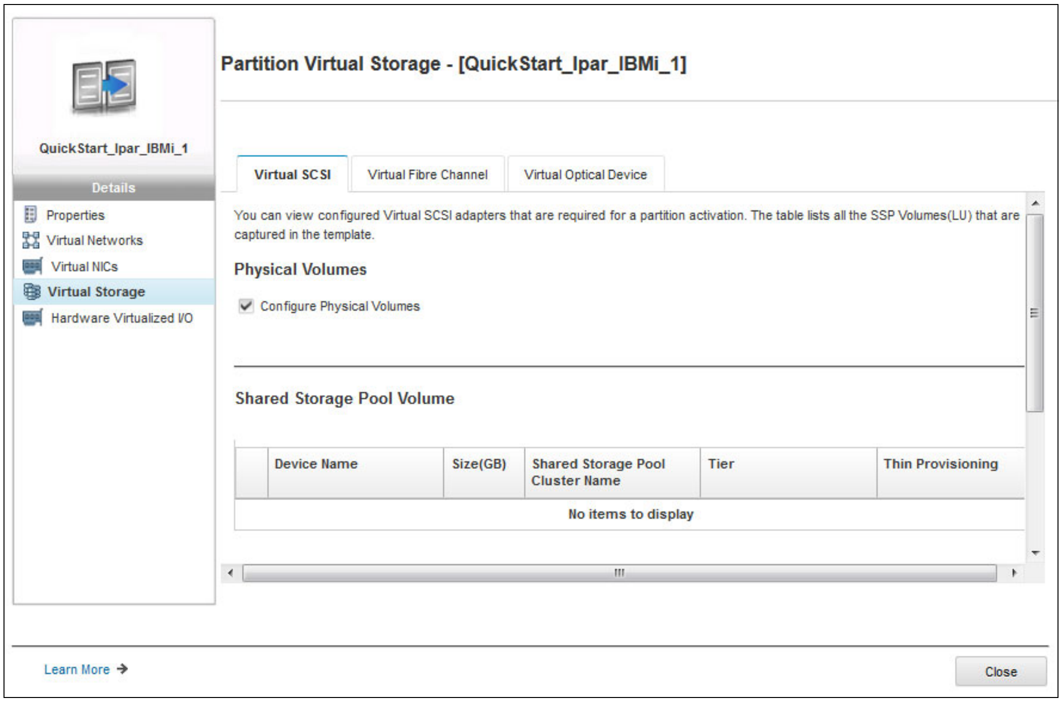
If you click **Virtual Storage** in the Template View window, you see the following extra tabs:

- Virtual SCSI
- Virtual Fibre Channel
- Virtual Optical Device

For each tab, you can view how each virtual resource type is configured, with these options:

- Configure virtual resource during deployment
- Configure virtual resource with captured information
- Do not configure virtual resource

For this example (Figure 2-72), the Virtual SCSI is configured to Configure the Virtual SCSI storage during deployment.



Partition Virtual Storage - [QuickStart_lpar_IBMi_1]

You can view configured Virtual SCSI adapters that are required for a partition activation. The table lists all the SSP Volumes(LU) that are captured in the template.

Physical Volumes

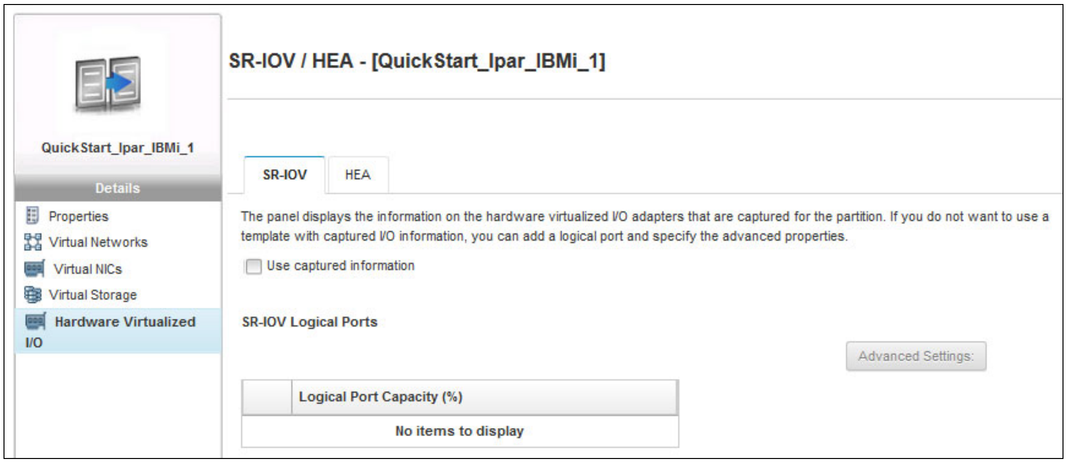
☑ Configure Physical Volumes

Shared Storage Pool Volume

	Device Name	Size(GB)	Shared Storage Pool Cluster Name	Tier	Thin Provisioning
No items to display					

Figure 2-72 View template: Virtual Storage

If you click **Hardware Virtualized I/O** and then the appropriate tab, you see the options that are selected for SR-IOV or HEA resources, as shown in Figure 2-73.



SR-IOV / HEA - [QuickStart_lpar_IBMi_1]

The panel displays the information on the hardware virtualized I/O adapters that are captured for the partition. If you do not want to use a template with captured I/O information, you can add a logical port and specify the advanced properties.

☐ Use captured information

SR-IOV Logical Ports

	Logical Port Capacity (%)
No items to display	

Figure 2-73 View template: Hardware Virtualized I/O

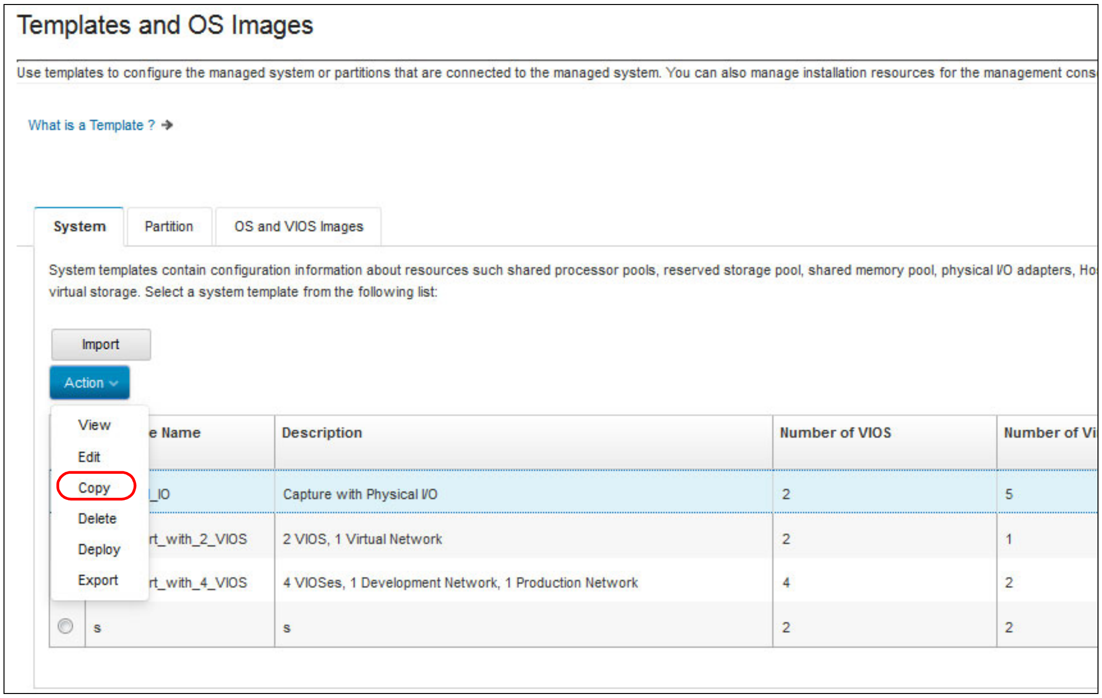
2.6.2 Creating templates

The two methods to create a partition template through the HMC are as follows:

- *Copy* an existing template in to a new template, which can then be modified as needed.
- *Capture* a running logical partition or a logical partition that is not in an activated state and save the configuration as a customized template.

Copying a template

From Templates and OS Images, click the **System** tab, right-click the template that you want to copy, and click **Copy**. For this example, we copy one of the starter templates, as shown in Figure 2-74.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management cons

What is a Template ?

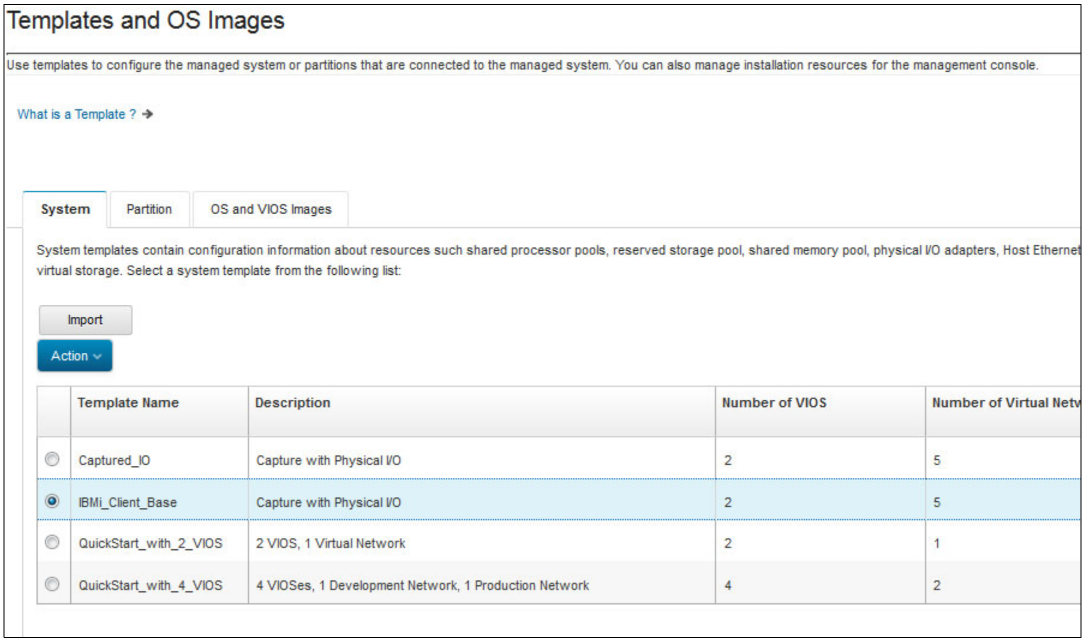
System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Ho virtual storage. Select a system template from the following list:

	e Name	Description	Number of VIOS	Number of Vi
	_IO	Capture with Physical I/O	2	5
	rt_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1
	rt_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2
○	s	s	2	2

Figure 2-74 Copy of a template

Enter an appropriate template name and click **OK**.

After the copy completes, your new template is listed in the Templates and OS Images, as shown in Figure 2-75.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

What is a Template ?

System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet virtual storage. Select a system template from the following list:

	Template Name	Description	Number of VIOS	Number of Virtual Netw
○	Captured_IO	Capture with Physical I/O	2	5
●	IBMi_Client_Base	Capture with Physical I/O	2	5
○	QuickStart_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1
○	QuickStart_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2

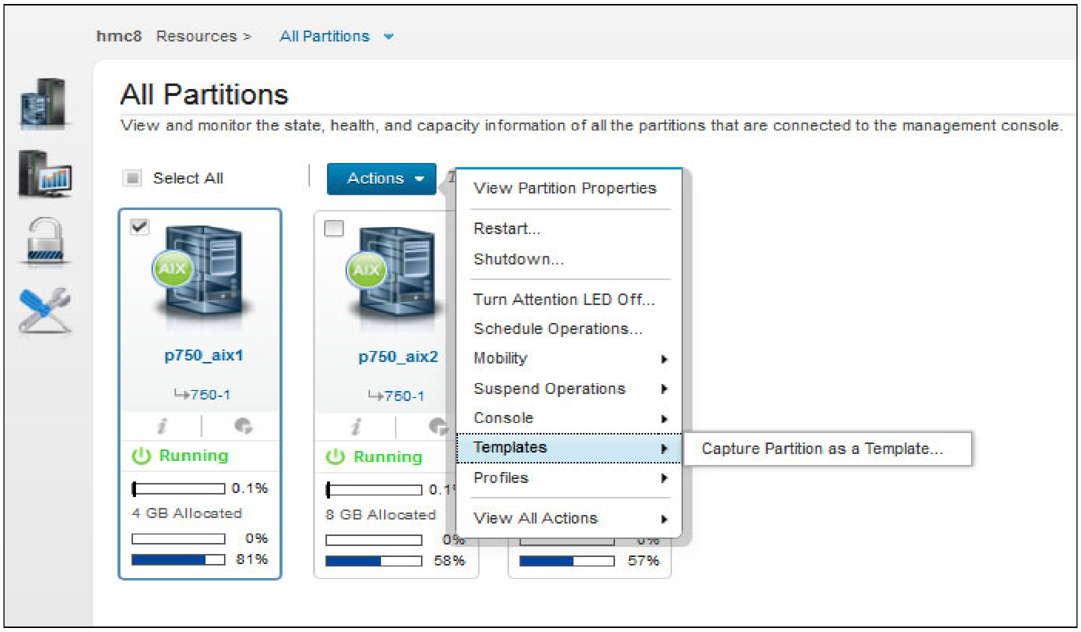
Figure 2-75 Copied template

Capturing a logical partition to create a template

You can capture the configuration details from a *running* partition or a partition that is in the *not activated* state and save the configuration as a custom template.

This function is useful if you want to create multiple partitions with the same configuration from a correctly configured logical partition, including virtual resources that are used in your environment.

In the HMC, click the **Resource** icon, select **All Partitions**, select the logical partition from which you want to create a template. Click **Actions** → **Templates** → **Capture Partition as Template**, as shown in Figure 2-76.

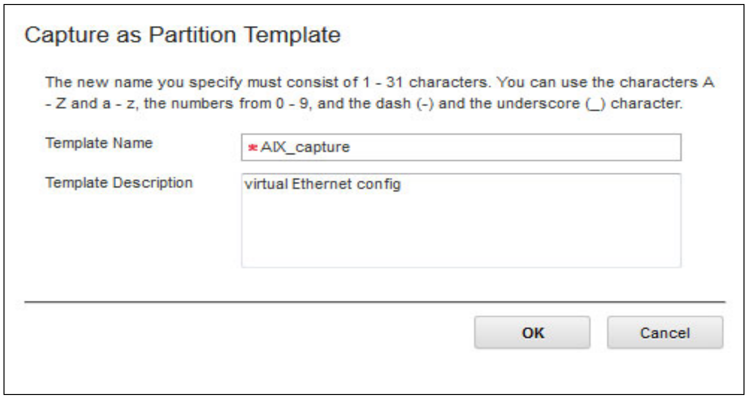


All Partitions

View and monitor the state, health, and capacity information of all the partitions that are connected to the management console.

Figure 2-76 Capture Configuration as Template

A window opens. You are prompted to name your captured template and provide an optional description of it, as shown in Figure 2-77.



Capture as Partition Template

The new name you specify must consist of 1 - 31 characters. You can use the characters A - Z and a - z, the numbers from 0 - 9, and the dash (-) and the underscore (_) character.

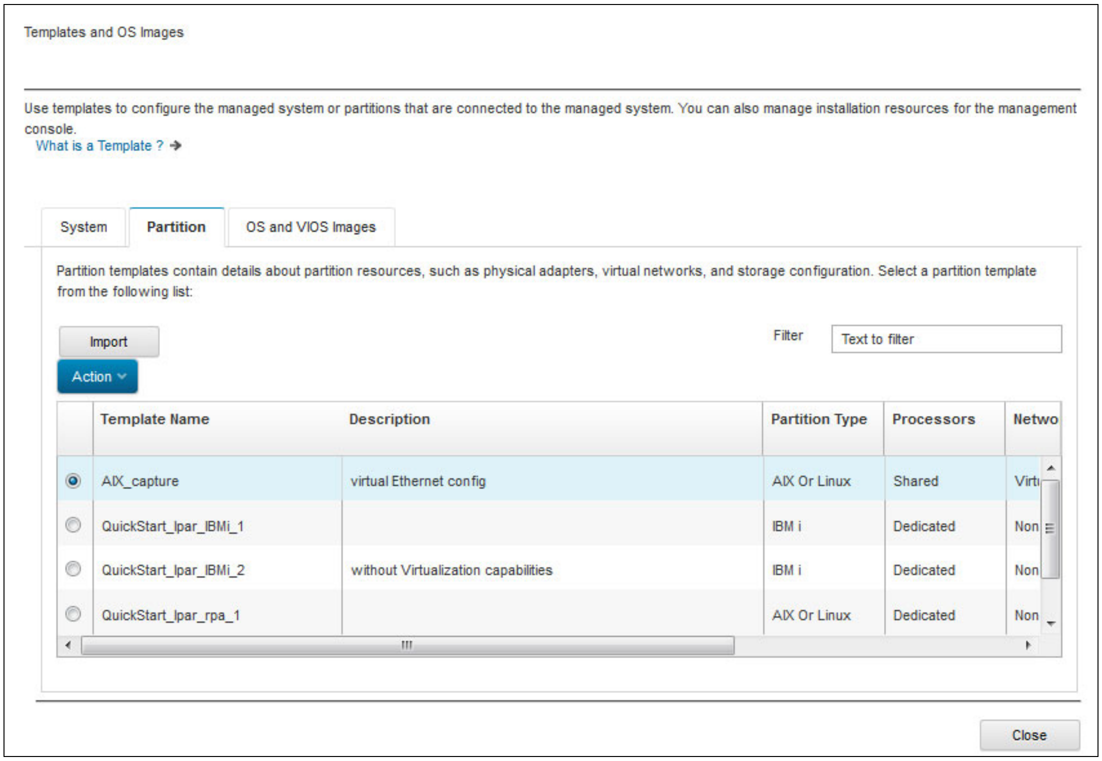
Template Name: * AIX_capture

Template Description: virtual Ethernet config

Figure 2-77 Naming the captured logical partition

Click **OK** to begin the capture.

After the capture function completes, the Templates and OS Images window opens, where you can view your captured template, as shown in Figure 2-78.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

What is a Template ?

Partition templates contain details about partition resources, such as physical adapters, virtual networks, and storage configuration. Select a partition template from the following list:

	Template Name	Description	Partition Type	Processors	Netwo
●	AIX_capture	virtual Ethernet config	AIX Or Linux	Shared	Virt
○	QuickStart_lpar_IBMi_1		IBM i	Dedicated	Non
○	QuickStart_lpar_IBMi_2	without Virtualization capabilities	IBM i	Dedicated	Non
○	QuickStart_lpar_rpa_1		AIX Or Linux	Dedicated	Non

Figure 2-78 Captured logical partition as a template

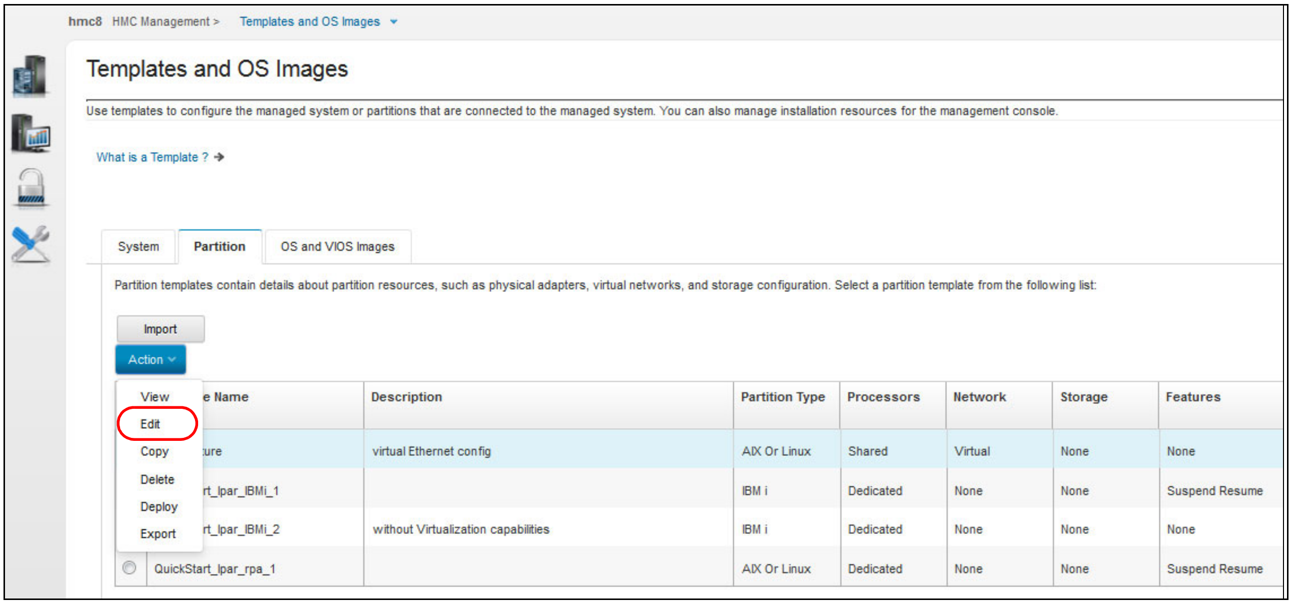
A template that is created by copying an existing template or by capturing a configured logical partition can be edited or recopied. These edited or recopied templates create additional templates that can, for example, be used for specific applications requirements by making granular changes from a base template.

2.6.3 Editing templates

To edit templates, on the HMC, select your managed system in the navigator pane, and in the work pane, expand **Templates**.

Select **Templates and OS Images** from the menu choices to view the available templates, which display in a new window. Click the **Partition** tab and the template you want to edit.

Right-click the template and select **Edit**, as shown in Figure 2-79. In this example, the AIX Capture template is selected to edit the template properties.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

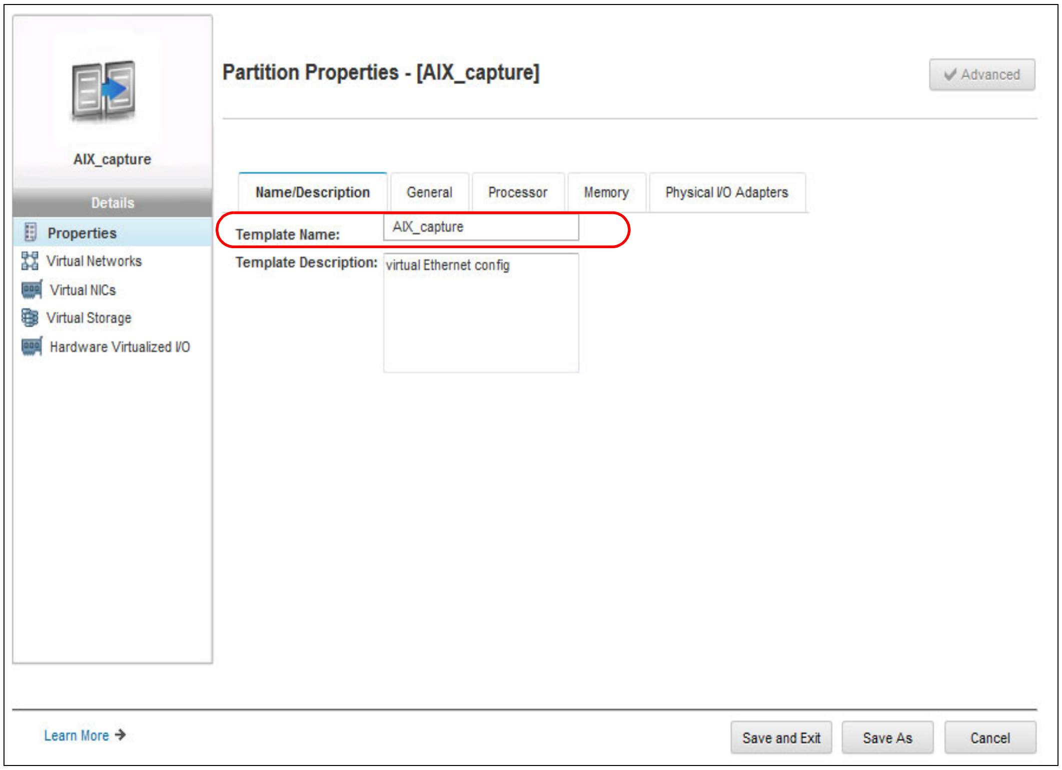
What is a Template ?

Partition templates contain details about partition resources, such as physical adapters, virtual networks, and storage configuration. Select a partition template from the following list:

e Name	Description	Partition Type	Processors	Network	Storage	Features
ure	virtual Ethernet config	AIX Or Linux	Shared	Virtual	None	None
rt_lpar_IBMi_1		IBM i	Dedicated	None	None	Suspend Resume
rt_lpar_IBMi_2	without Virtualization capabilities	IBM i	Dedicated	None	None	None
○ QuickStart_lpar_rpa_1		AIX Or Linux	Dedicated	None	None	Suspend Resume

Figure 2-79 Edit a partition template

A window opens, as shown in Figure 2-80. You can change the name of your template by modifying the Template Name and then clicking **Save and Exit**.



Partition Properties - [AIX_capture]

Template Name: AIX_capture

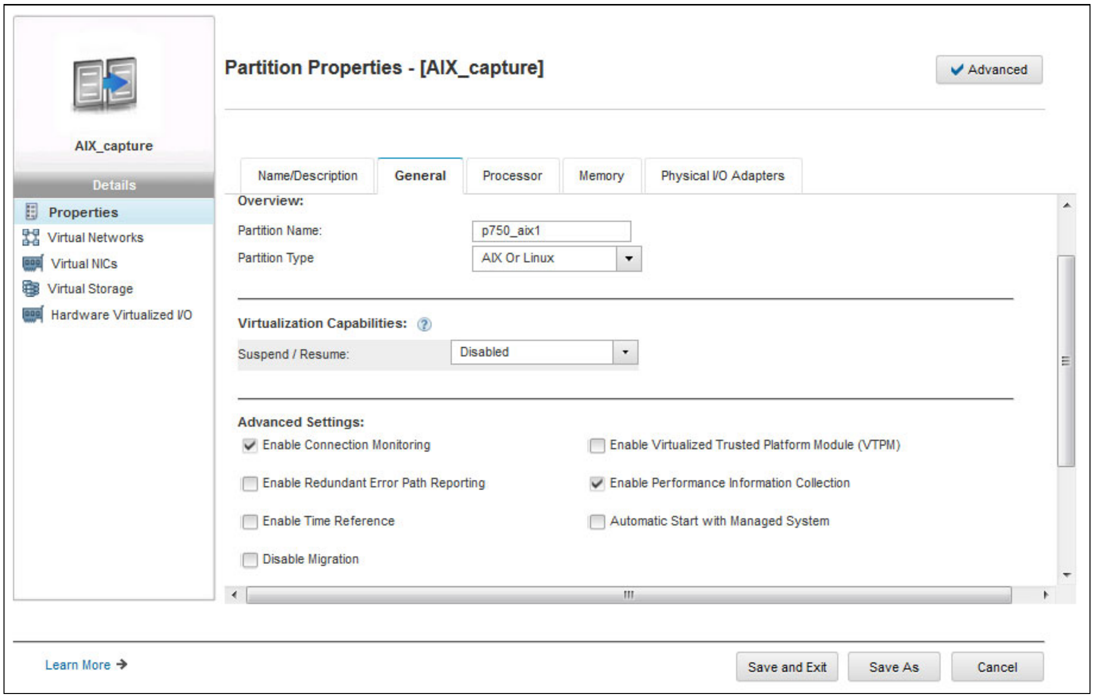
Template Description: virtual Ethernet config

Figure 2-80 Edit template: Name/Description tab

While you are using the template edit function, within any menu or tab, clicking **Save and Exit** saves the edited changes and reopens the Templates and OS Images window.

Clicking **Save As** initiates the template copy function, which is described in "Copying a template" on page 114.

Click **Properties** and then the **General** tab (Figure 2-81). Click **Show Advanced** to display the advanced parameters.



Partition Properties - [AIX_capture]

Overview:

Partition Name: p750_aix1

Partition Type: AIX Or Linux

Virtualization Capabilities:

Suspend / Resume: Disabled

Advanced Settings:

☑ Enable Connection Monitoring

☐ Enable Virtualized Trusted Platform Module (VTPM)

☐ Enable Redundant Error Path Reporting

☑ Enable Performance Information Collection

☐ Enable Time Reference

☐ Automatic Start with Managed System

☐ Disable Migration

Figure 2-81 Edit template: General tab

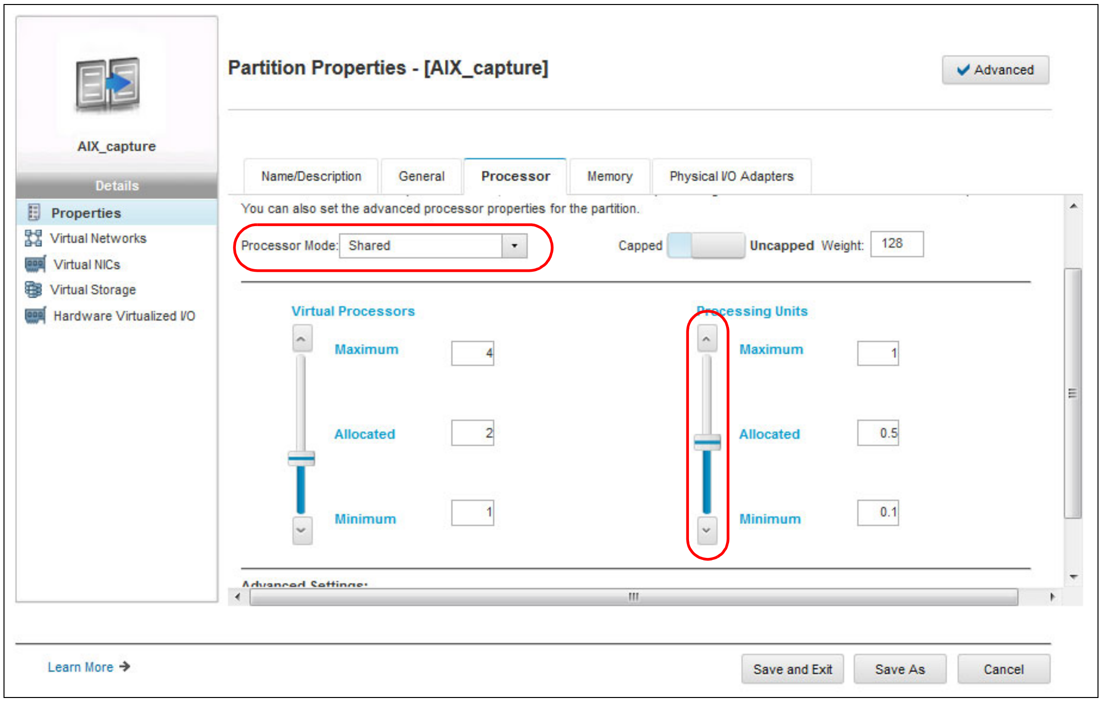
Because you selected the Show Advanced option, *all* tabs of the Properties menu show the advanced properties for each tab by default.

In this example, the following properties are specified:

- Maximum number of Virtual Adapters
- Enabled Connection Monitoring
- Enabled Performance Information Collection

Modify your selections to suit your environment.

You can click the **Processor** tab to change the Processor mode, assign processor values, and change the Processor Compatibility Mode. To change the processor mode from Dedicated to Shared, click the Processor Mode drop-down box, as shown in Figure 2-82.



Partition Properties - [AIX_capture]

You can also set the advanced processor properties for the partition.

Processor Mode: Shared

Weight: 128

Virtual Processors

Maximum 4

Allocated 2

Minimum 1

Processing Units

Maximum 1

Allocated 0.5

Minimum 0.1

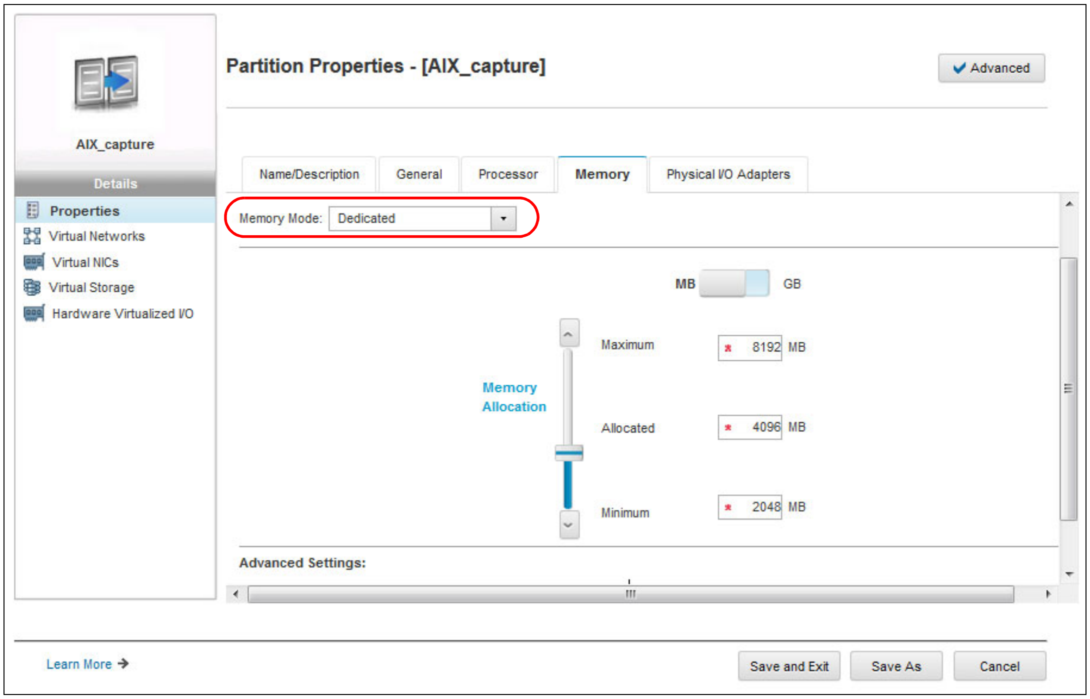
Figure 2-82 Edit template: Processor tab

In this example, changing the Processor Mode to Shared enables the editing of the Virtual Processors and Processing Units. A value can be set by either entering the required value or moving the slider arm to the wanted value.

You can use Processor Compatibility Mode to select the appropriate mode, with selections from POWER6 to POWER8-enhanced. For more information about Processor Compatibility Modes, see 1.2.12, “POWER8 processor-based systems support” on page 25.

Modify the processor assigned values to suit your environment.

You can click the **Memory** tab to change the Memory Mode. To change the Memory Mode from Dedicated to Shared, click the Memory Mode drop-box, as shown in Figure 2-83.



Partition Properties - [AIX_capture]

Memory Mode: Dedicated

Maximum 8192 MB

Allocated 4096 MB

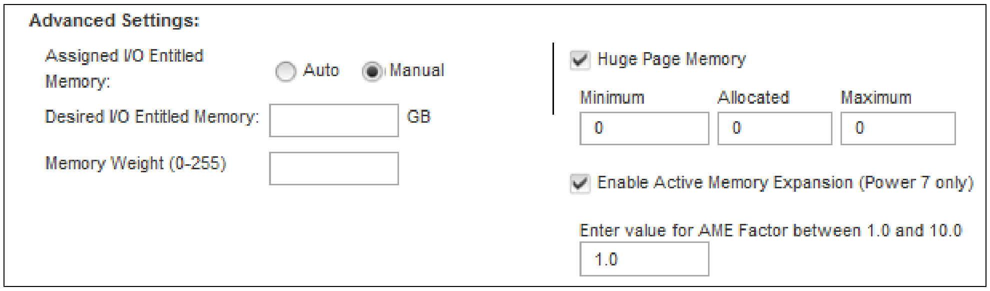
Minimum 2048 MB

Figure 2-83 Edit template: Memory tab

In this example, the Memory Mode remains as dedicated memory and has the assigned values that are shown.

Under this tab is the PowerVM capability of Active Memory Expansion (AME). Select the check box and enter an appropriate AME factor.

Selecting **Shared Memory Mode** changes the Advanced Settings in the memory tab, as shown in Figure 2-84.



Advanced Settings:

Assigned I/O Entitled Memory: ○ Auto ● Manual

Desired I/O Entitled Memory: GB

Memory Weight (0-255)

☑ Huge Page Memory

Minimum	Allocated	Maximum
0	0	0

☑ Enable Active Memory Expansion (Power 7 only)

Enter value for AME Factor between 1.0 and 10.0

1.0

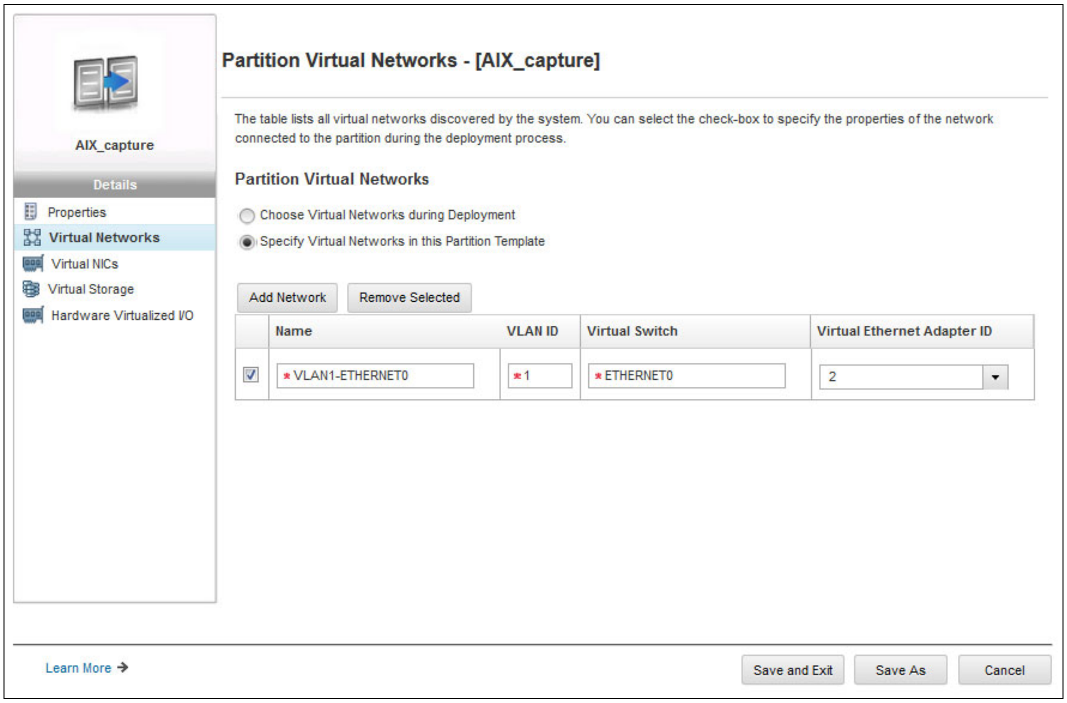
Figure 2-84 Edit template: Shared memory advanced settings

Modify the memory configuration to suit your environment.

You can click **Virtual Networks** so that the template can choose either of the following settings:

- Choose Virtual Networks during Deployment
- Specify Virtual Networks in this Partition Template

Figure 2-85 shows that this template specifies a virtual network during deployment and has an appropriate value.



Partition Virtual Networks - [AIX_capture]

The table lists all virtual networks discovered by the system. You can select the check-box to specify the properties of the network connected to the partition during the deployment process.

Partition Virtual Networks

○ Choose Virtual Networks during Deployment

● Specify Virtual Networks in this Partition Template

	Name	VLAN ID	Virtual Switch	Virtual Ethernet Adapter ID
☑	* VLAN1-ETHERNET0	* 1	* ETHERNET0	2

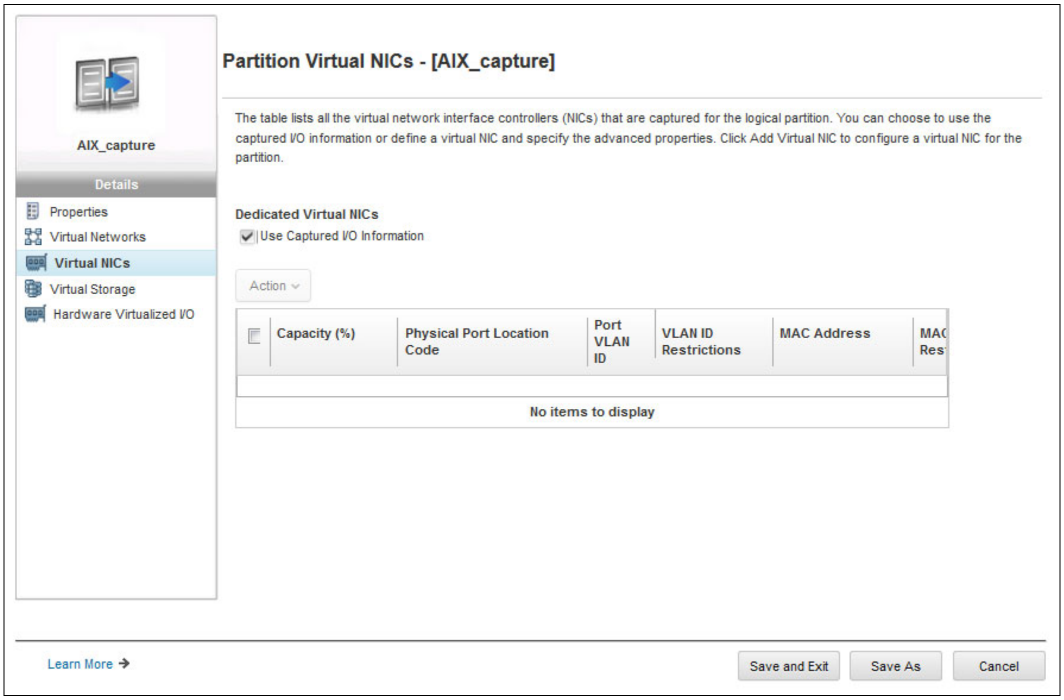
Figure 2-85 Edit template: Virtual Networks

if you are using the template function to create a logical partition and specify virtual resources in the template, the preferred practice is that the virtual resources are created *before* editing the template.

If no virtual networks are specified on the managed system and you select the **Choose Virtual Networks during Deployment** option, no available options display during template deployment. This situation is covered in more detail in 2.6.4, “Deploying templates” on page 125.

Modify the virtual network configuration to suit your environment.

You can also view the properties of a virtual Network Interface Controller (vNIC) in a partition profile by using the HMC, as shown in Figure 2-86.



Partition Virtual NICs - [AIX_capture]

The table lists all the virtual network interface controllers (NICs) that are captured for the logical partition. You can choose to use the captured I/O information or define a virtual NIC and specify the advanced properties. Click Add Virtual NIC to configure a virtual NIC for the partition.

Dedicated Virtual NICs

☑ Use Captured I/O Information

□	Capacity (%)	Physical Port Location Code	Port VLAN ID	VLAN ID Restrictions	MAC Address	MAC Res

No items to display

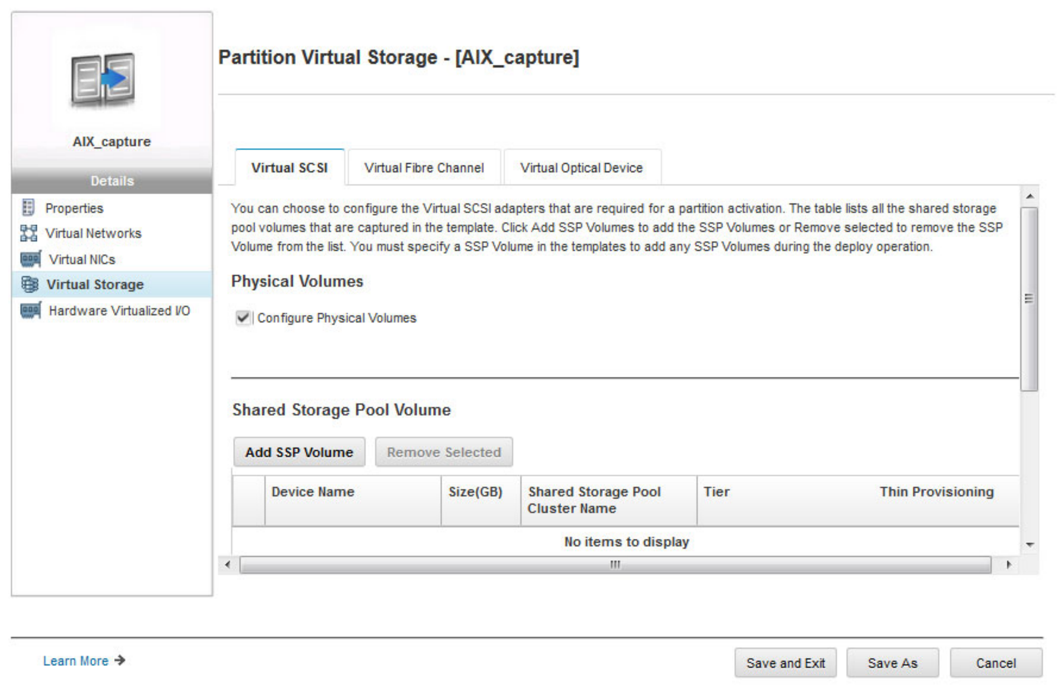
Figure 2-86 Edit template virtual NICs

A *virtual Network Interface Controller (vNIC)* is a type of virtual Ethernet adapter that can be configured on client logical partitions. Each vNIC is backed by a single root I/O virtualization (SR-IOV) logical port that is owned by the VIOS.

You can click **Virtual Storage** so that the template can be configured with the following PowerVM capabilities:

- Virtual SCSI
- Virtual Fibre Channel
- Virtual Optical Device

As shown in Figure 2-87, the new template can include virtual storage resources as part of your template deployment.



Partition Virtual Storage - [AIX_capture]

You can choose to configure the Virtual SCSI adapters that are required for a partition activation. The table lists all the shared storage pool volumes that are captured in the template. Click Add SSP Volumes to add the SSP Volumes or Remove selected to remove the SSP Volume from the list. You must specify a SSP Volume in the templates to add any SSP Volumes during the deploy operation.

Physical Volumes

☑ Configure Physical Volumes

Shared Storage Pool Volume

	Device Name	Size(GB)	Shared Storage Pool Cluster Name	Tier	Thin Provisioning
No items to display					

Figure 2-87 Edit template: Virtual Storage

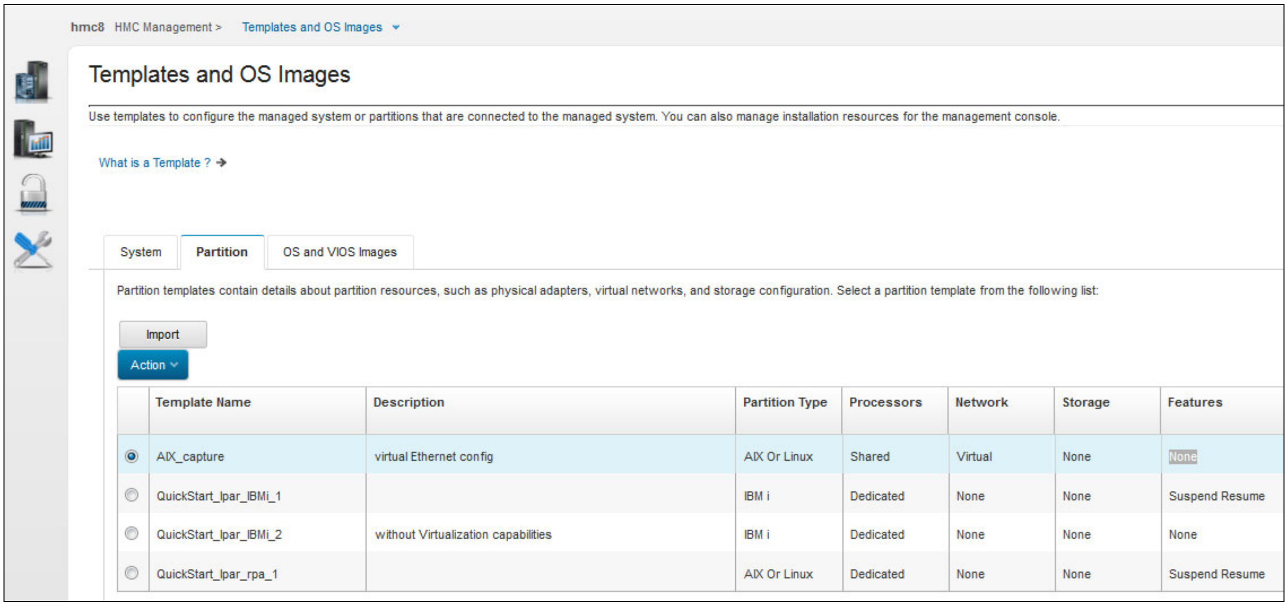
Depending on the environment that is used by the logical partition that you are going to deploy from this template, you can create virtual SCSI adapters, virtual Fibre Channel adapters, and virtual optical devices.

In this example, during the template deployment, you are prompted to configure your virtual resources as you create the logical partition. To use the template to deploy virtual resources, have a thorough understanding of PowerVM and its concepts.

Modify the virtual storage to suit your environment.

When you click **Save and Exit** at any time while using the template edit function, the HMC saves the changes and returns to the Templates and OS Images window.

As shown in Figure 2-88, the edited changes are saved, and the template details in the Templates and OS Images window are changed.



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

What is a Template ? →

Partition templates contain details about partition resources, such as physical adapters, virtual networks, and storage configuration. Select a partition template from the following list:

	Template Name	Description	Partition Type	Processors	Network	Storage	Features
●	AIX_capture	virtual Ethernet config	AIX Or Linux	Shared	Virtual	None	None
○	QuickStart_lpar_IBMi_1		IBM i	Dedicated	None	None	Suspend Resume
○	QuickStart_lpar_IBMi_2	without Virtualization capabilities	IBM i	Dedicated	None	None	None
○	QuickStart_lpar_rpa_1		AIX Or Linux	Dedicated	None	None	Suspend Resume

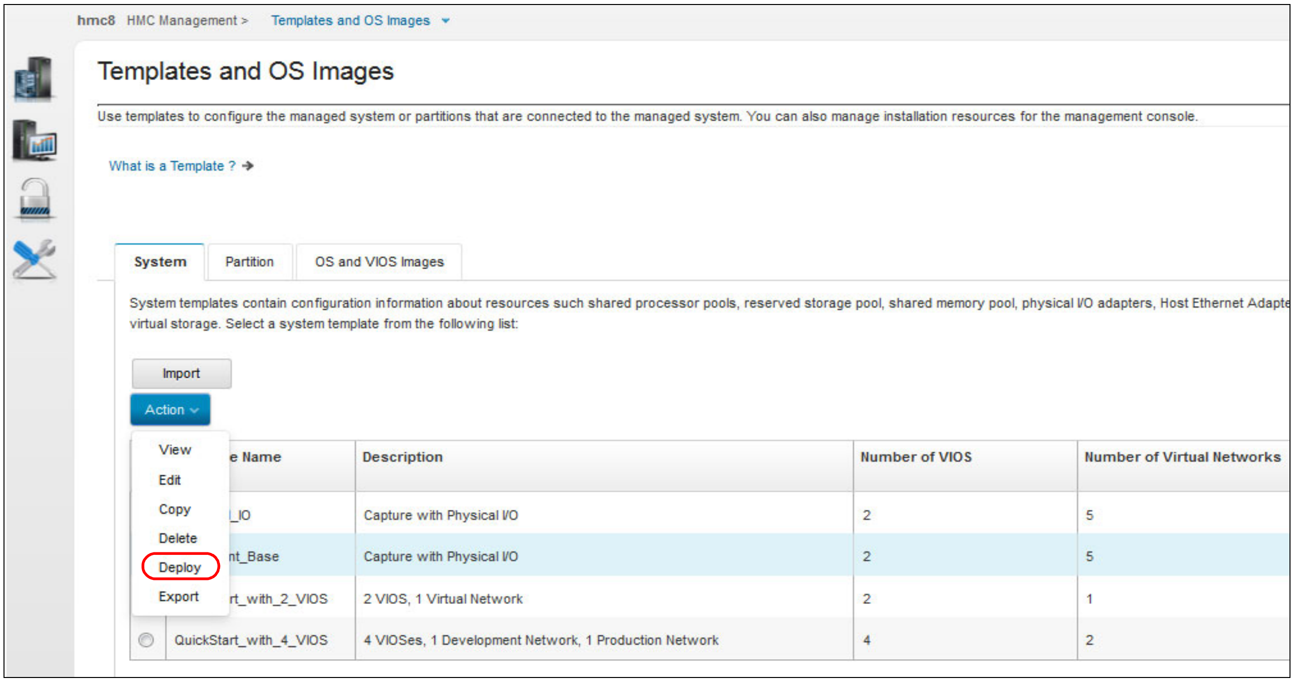
Figure 2-88 Edited template

For the AIX Capture template shown in Figure 2-88, the Processor mode was changed from Dedicated to Shared Mode and the virtual networks were updated to include details about the configured virtual networks.

2.6.4 Deploying templates

To create a logical partition by deploying it from a template, complete the following steps:

1. click **HMC Management**, click **Templates and OS Images**, select your template, right-click the template, and select **Deploy**, as shown in Figure 2-89.



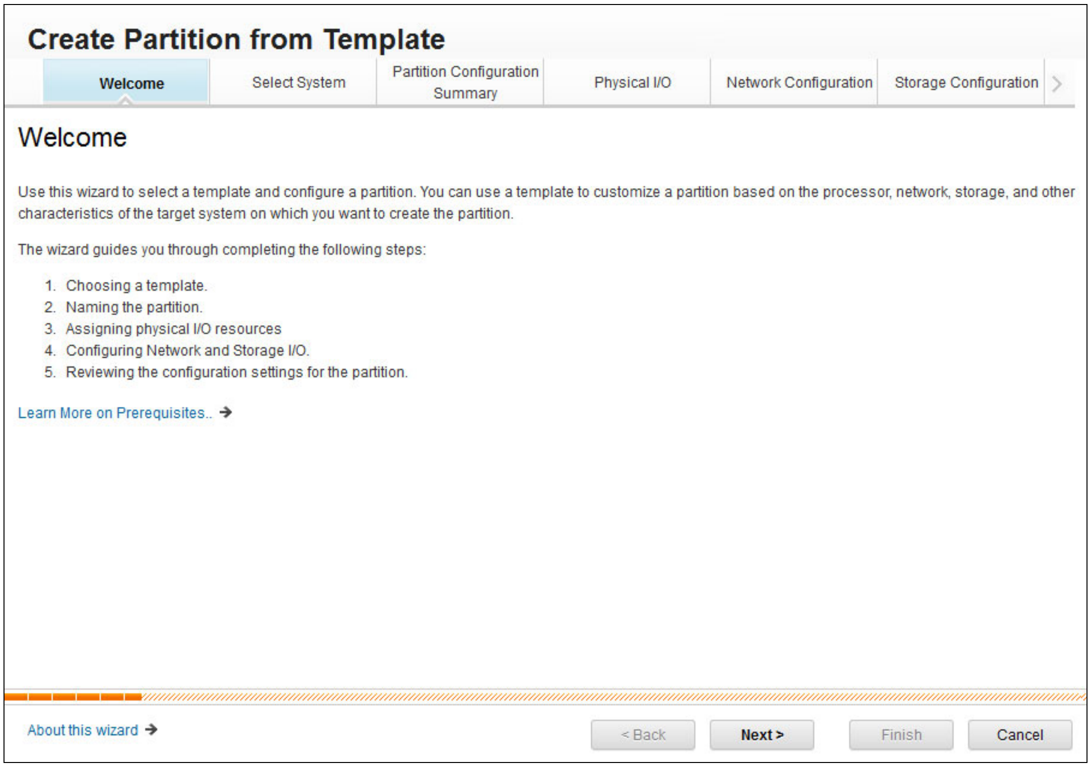
Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

System templates contain configuration information about resources such shared processor pools, reserved storage pool, shared memory pool, physical I/O adapters, Host Ethernet Adapte virtual storage. Select a system template from the following list:

e Name	Description	Number of VIOS	Number of Virtual Networks
_IO	Capture with Physical I/O	2	5
nt_Base	Capture with Physical I/O	2	5
rt_with_2_VIOS	2 VIOS, 1 Virtual Network	2	1
○ QuickStart_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network	4	2

Figure 2-89 Template deployment from the Templates and OS Images

If you selected **Create Partition from Template**, the only difference from the window that is shown in Figure 2-90 is an additional tab where you must specify the template to use for the deployment.



Create Partition from Template

Welcome

Use this wizard to select a template and configure a partition. You can use a template to customize a partition based on the processor, network, storage, and other characteristics of the target system on which you want to create the partition.

The wizard guides you through completing the following steps:

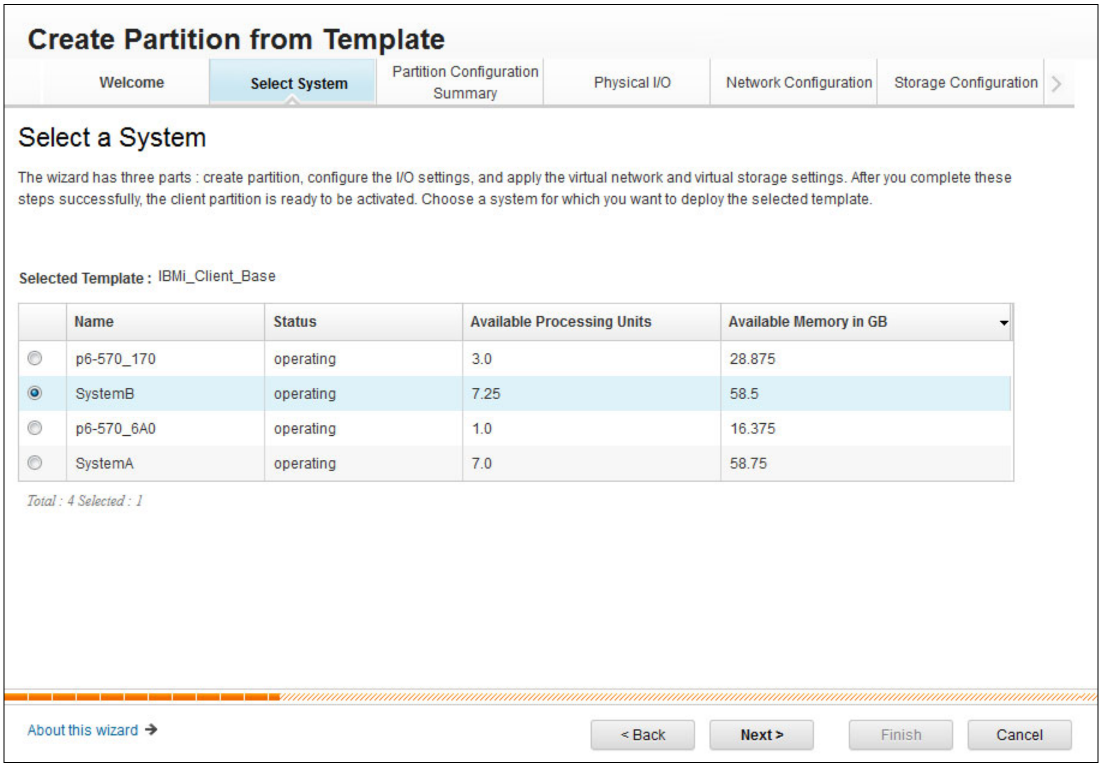
1. Choosing a template.
2. Naming the partition.
3. Assigning physical I/O resources
4. Configuring Network and Storage I/O.
5. Reviewing the configuration settings for the partition.

Learn More on Prerequisites.. ➔

Figure 2-90 Initial deployment wizard window

2. Click **Next** to move to the next tab.

3. In the Select System tab, select the managed system that you want to deploy with the selected template. For this example, SystemB is selected, as shown in Figure 2-91.



Create Partition from Template

Select a System

The wizard has three parts : create partition, configure the I/O settings, and apply the virtual network and virtual storage settings. After you complete these steps successfully, the client partition is ready to be activated. Choose a system for which you want to deploy the selected template.

Selected Template : IBMi_Client_Base

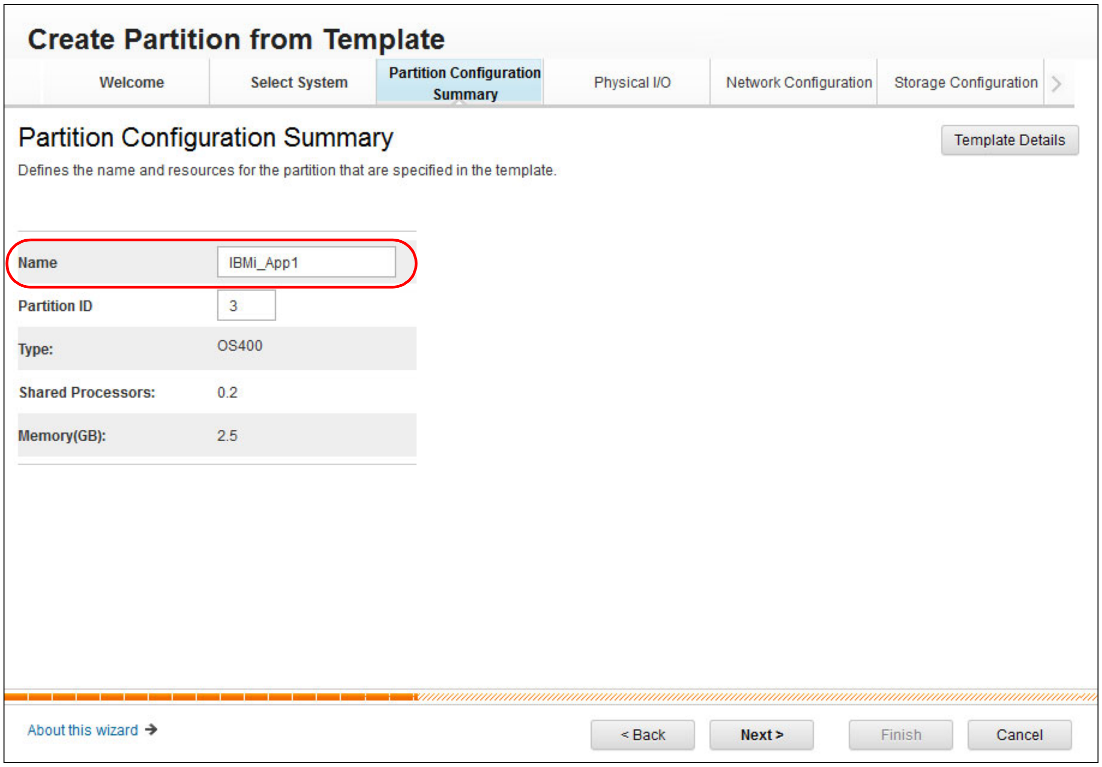
	Name	Status	Available Processing Units	Available Memory in GB
○	p6-570_170	operating	3.0	28.875
●	SystemB	operating	7.25	58.5
○	p6-570_6A0	operating	1.0	16.375
○	SystemA	operating	7.0	58.75

Total : 4 Selected : 1

Figure 2-91 Deployment: system

4. Click **Next** to move to the next tab.

In the Partition Configuration tab, enter the name of your logical partition, which at the completion of the wizard displays under the selected managed system in the work pane, as shown in Figure 2-92.



Create Partition from Template

Partition Configuration Summary

Defines the name and resources for the partition that are specified in the template.

Name	IBMi_App1
Partition ID	3
Type:	OS400
Shared Processors:	0.2
Memory(GB):	2.5

Figure 2-92   Deployment: Partition Configuration

This tab also displays the type of logical partition to be created and the Processor and Memory configurations that are specified by the template. In this case, the template deploys an IBM i logical partition with 0.2 shared processors and 2.5 GB of memory.

To verify the template configuration, click **Template Details** in the wizard window to view the template configuration, which displays the template details, but you cannot edit the template. If your template details must be edited, cancel the deployment wizard and edit your template, save the changes, and then restart the deployment wizard.

5. Click **Next** to move to the next tab.

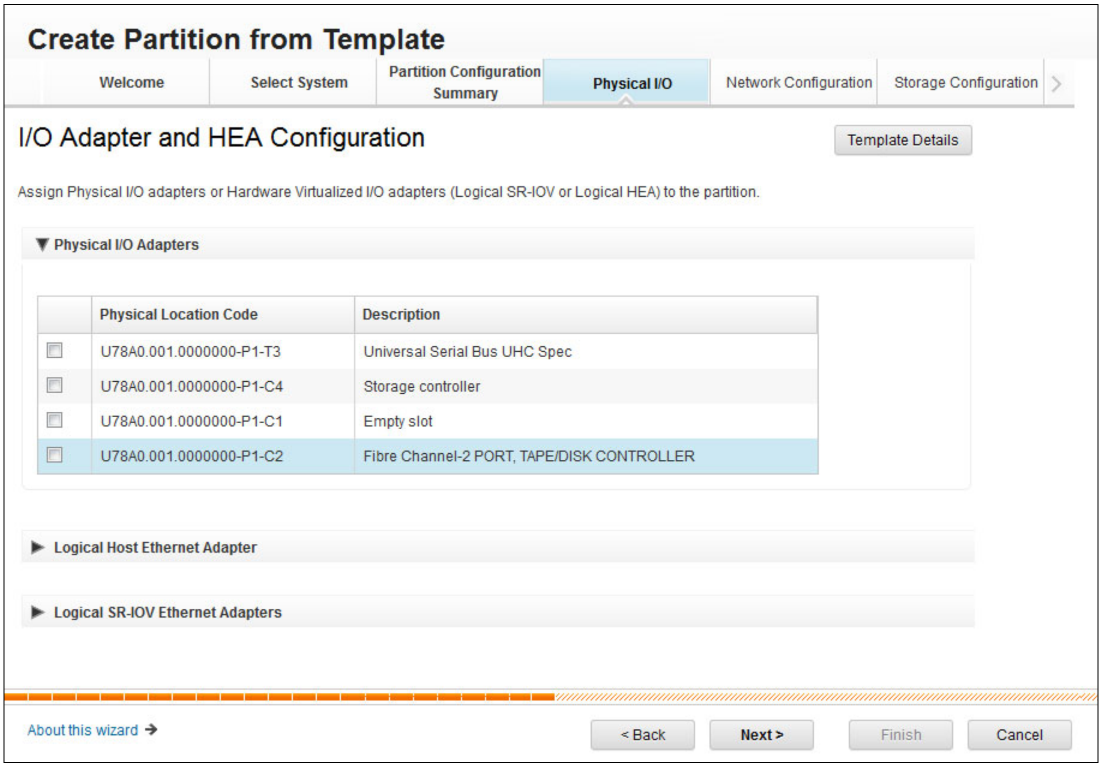
   The Physical I/O tab has three available options.

   – Physical I/O: Assign physical I/O to the logical partition.

   – Logical Host Ethernet Adapter: Assign a logical port on a HEA.

   – Logical SR-IOV Ethernet Adapters: Assign a logical port on an SR-IOV Ethernet Adapter.

Depending on your environment, expand the appropriate option and, as Figure 2-93 shows, select the required physical I/O resource that will be assigned to the partition as part of the logical partition deployment.



Create Partition from Template

I/O Adapter and HEA Configuration

Assign Physical I/O adapters or Hardware Virtualized I/O adapters (Logical SR-IOV or Logical HEA) to the partition.

▼ Physical I/O Adapters

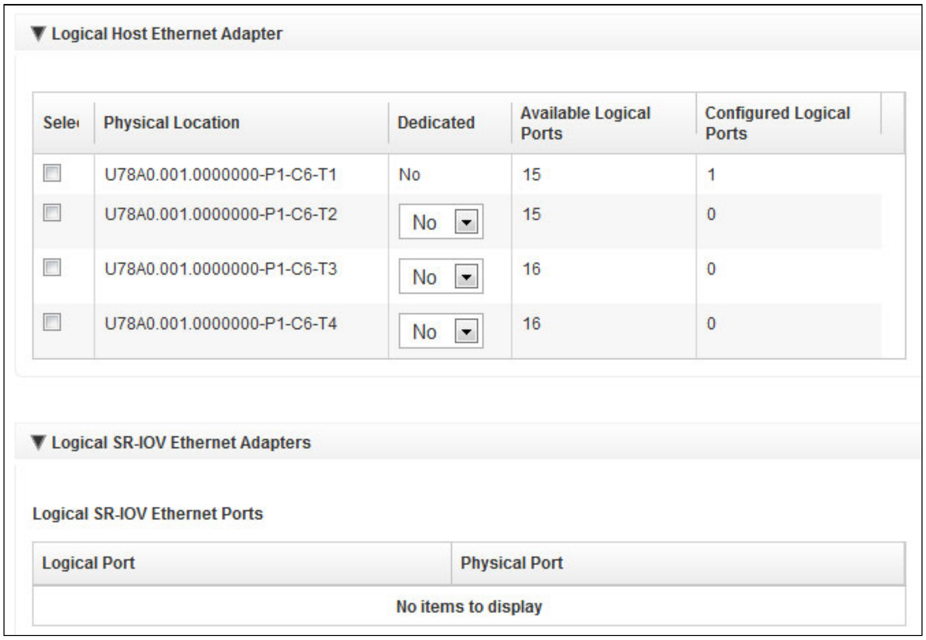
	Physical Location Code	Description
□	U78A0.001.0000000-P1-T3	Universal Serial Bus UHC Spec
□	U78A0.001.0000000-P1-C4	Storage controller
□	U78A0.001.0000000-P1-C1	Empty slot
□	U78A0.001.0000000-P1-C2	Fibre Channel-2 PORT, TAPE/DISK CONTROLLER

▶ Logical Host Ethernet Adapter

▶ Logical SR-IOV Ethernet Adapters

Figure 2-93 Deployment: Physical I/O

If your managed system does not have HEA or SR-IOV resources, expanding the options does not display any options. For the managed system that is selected in this example, an HEA resource exists, but no SR-IOV resource, as shown in Figure 2-94.



▼ Logical Host Ethernet Adapter

Selec	Physical Location	Dedicated	Available Logical Ports	Configured Logical Ports
□	U78A0.001.0000000-P1-C6-T1	No	15	1
□	U78A0.001.0000000-P1-C6-T2	No ▾	15	0
□	U78A0.001.0000000-P1-C6-T3	No ▾	16	0
□	U78A0.001.0000000-P1-C6-T4	No ▾	16	0

▼ Logical SR-IOV Ethernet Adapters

Logical SR-IOV Ethernet Ports

Logical Port	Physical Port
No items to display	

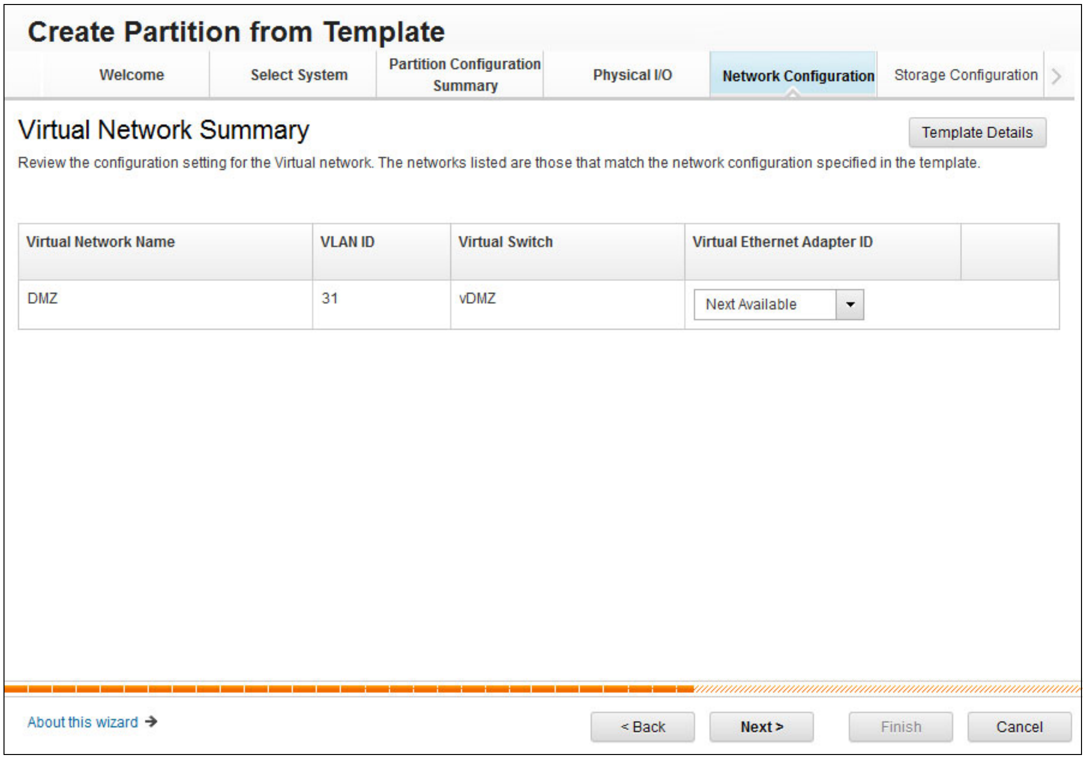
Figure 2-94 Deployment: Physical I/O additional

Modify the assigned resources to suit your environment.

6. Click **Next** to move to the next tab.

   In the Network Configuration tab, you see the virtual network that is specified by the template which is used for the logical partition deployment.

   Figure 2-95 shows that the template was *specified* to use a virtual network, named DMZ, by using the **Specify Virtual Networks in this Partition Template** item of the Virtual Networks menu of the template and completing the appropriate values.



Virtual Network Summary

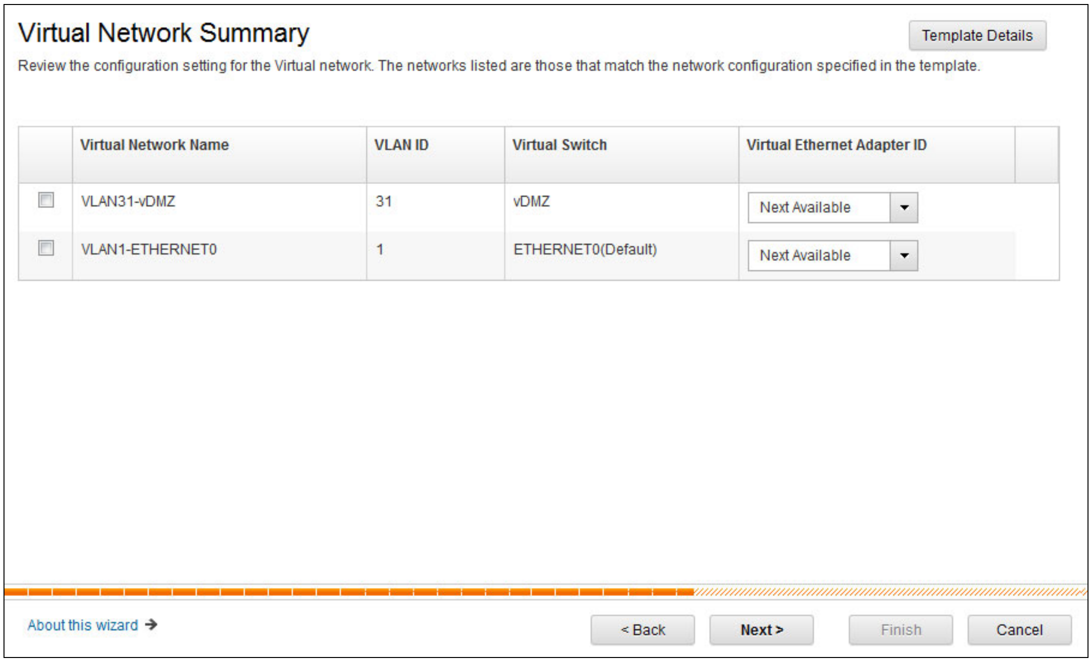
Review the configuration setting for the Virtual network. The networks listed are those that match the network configuration specified in the template.

Virtual Network Name	VLAN ID	Virtual Switch	Virtual Ethernet Adapter ID
DMZ	31	vDMZ	Next Available

Figure 2-95 Deployment: Network Configuration

If the template is specified with the **Choose Virtual Networks during Deployment** option, the wizard displays the available virtual networks on the managed system.

The wizard displays the available networks and selections for the logical partition requirements (Figure 2-96).



Virtual Network Summary

Review the configuration setting for the Virtual network. The networks listed are those that match the network configuration specified in the template.

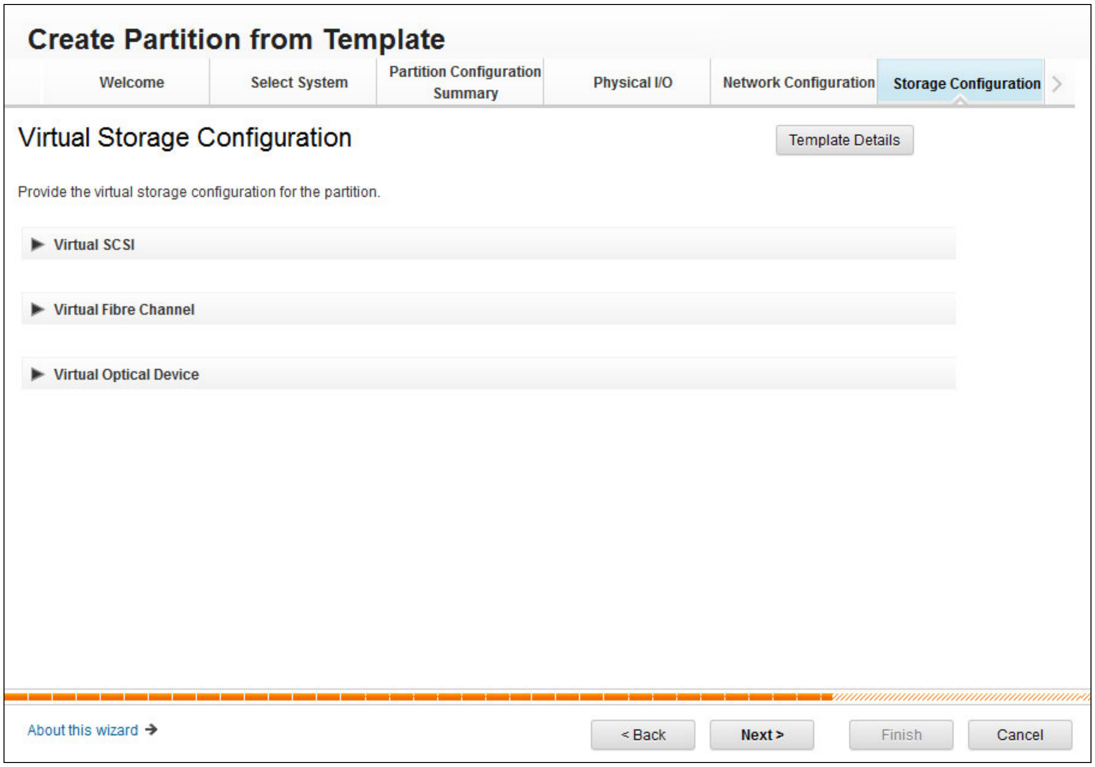
	Virtual Network Name	VLAN ID	Virtual Switch	Virtual Ethernet Adapter ID
□	VLAN31-vDMZ	31	vDMZ	Next Available ▾
□	VLAN1-ETHERNET0	1	ETHERNET0(Default)	Next Available ▾

Figure 2-96   Deployment: Virtual Network

7. Click **Next** to move to the next tab.

The Storage Configuration tab (Figure 2-97) has three options that are available for your virtual storage:

- Virtual SCSI
- Virtual Fibre Channel
- Virtual Optical Device



Create Partition from Template

Virtual Storage Configuration

Provide the virtual storage configuration for the partition.

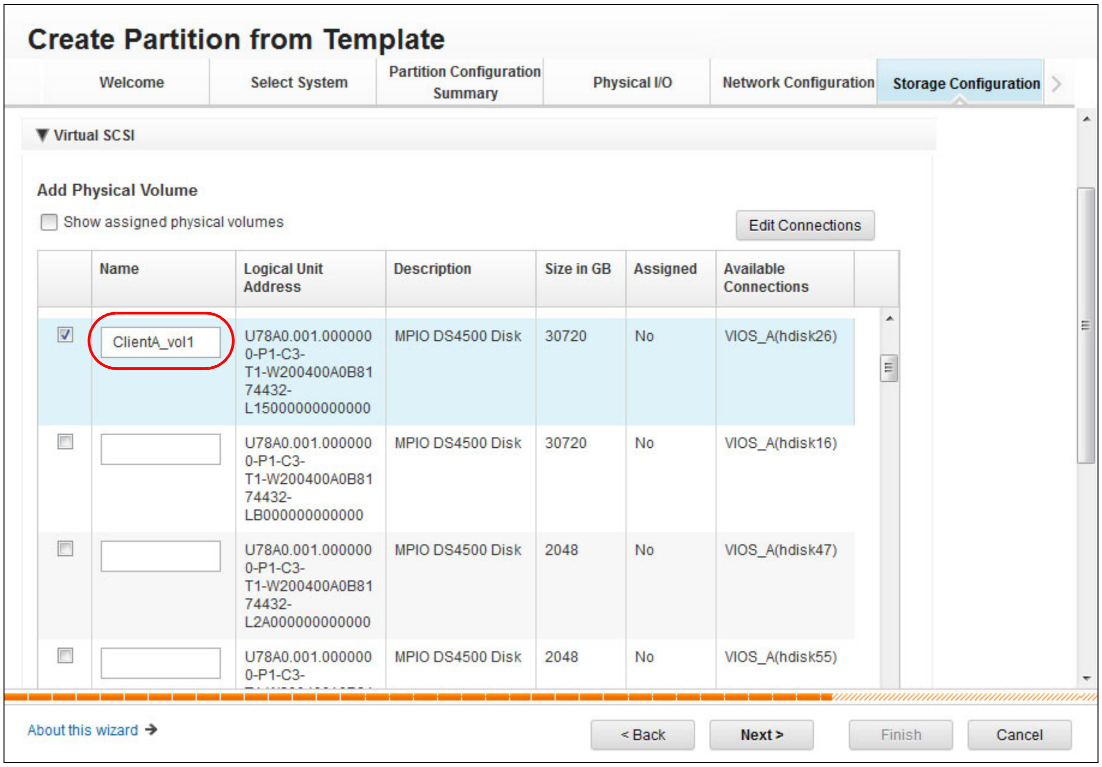
▶ Virtual SCSI

▶ Virtual Fibre Channel

▶ Virtual Optical Device

Figure 2-97 Deployment: Virtual Storage initial

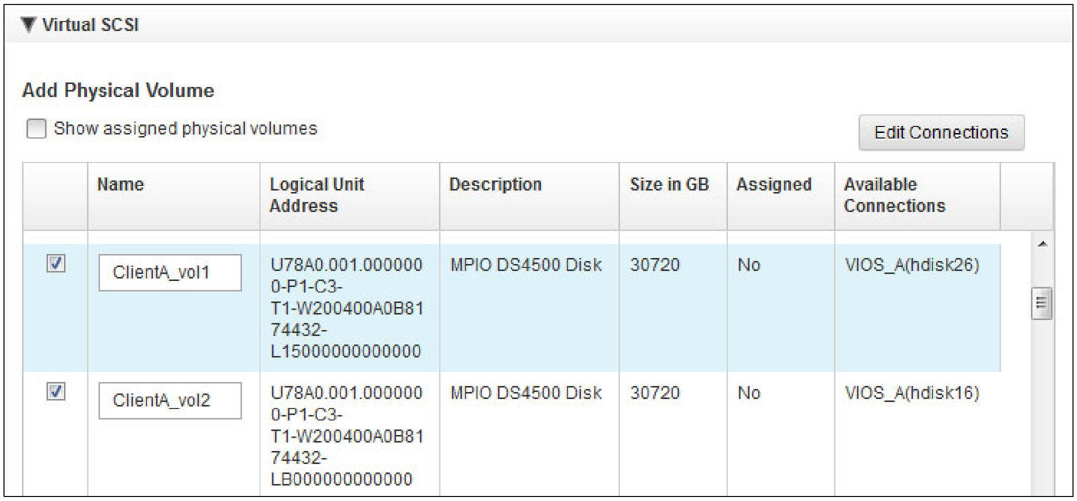
You can expand **Virtual SCSI** to assign physical volumes to your logical partition. Figure 2-98 shows volumes that are present and can be selected. Entering a volume name allows for multiple deployments to determine what volumes already are selected and to which logical partition they are assigned.



	Name	Logical Unit Address	Description	Size in GB	Assigned	Available Connections
☑	ClientA_vol1	U78A0.001.000000 0-P1-C3- T1-W200400A0B81 74432- L15000000000000	MPIO DS4500 Disk	30720	No	VIOS_A(hdisk26)
□		U78A0.001.000000 0-P1-C3- T1-W200400A0B81 74432- LB000000000000	MPIO DS4500 Disk	30720	No	VIOS_A(hdisk16)
□		U78A0.001.000000 0-P1-C3- T1-W200400A0B81 74432- L2A000000000000	MPIO DS4500 Disk	2048	No	VIOS_A(hdisk47)
□		U78A0.001.000000 0-P1-C3-	MPIO DS4500 Disk	2048	No	VIOS_A(hdisk55)

Figure 2-98 Deployment: Storage - Virtual SCSI

Selecting multiple volumes is supported, as shown in Figure 2-99.

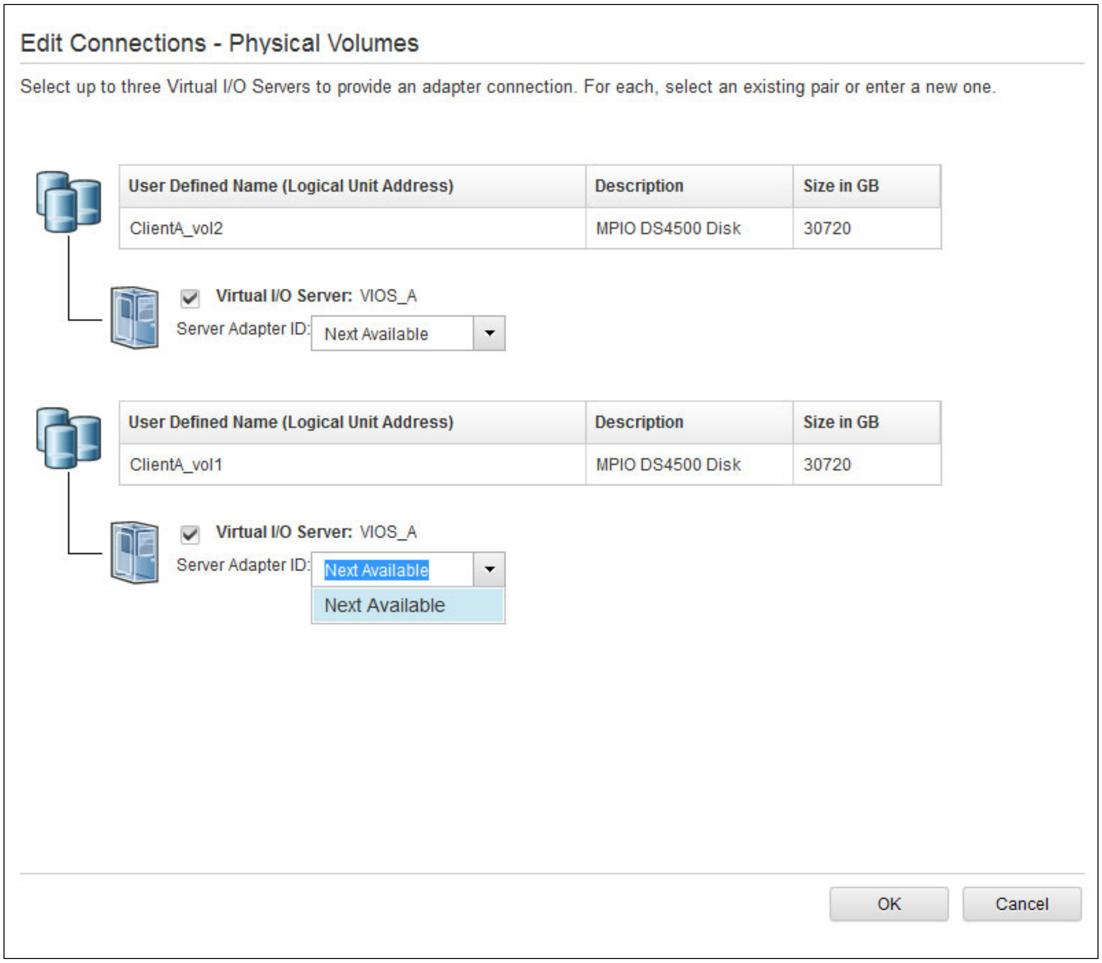


	Name	Logical Unit Address	Description	Size in GB	Assigned	Available Connections
☑	ClientA_vol1	U78A0.001.000000 0-P1-C3- T1-W200400A0B81 74432- L15000000000000	MPIO DS4500 Disk	30720	No	VIOS_A(hdisk26)
☑	ClientA_vol2	U78A0.001.000000 0-P1-C3- T1-W200400A0B81 74432- LB000000000000	MPIO DS4500 Disk	30720	No	VIOS_A(hdisk16)

Figure 2-99 Deployment: Storage - Multiple Volumes

8. Click **Edit Connections** in the wizard window.

9. The Edit Connections window opens (Figure 2-100). Use it to modify the virtual SCSI connections to the physical volumes that are specified, as shown in the figure.



Edit Connections - Physical Volumes

Select up to three Virtual I/O Servers to provide an adapter connection. For each, select an existing pair or enter a new one.

User Defined Name (Logical Unit Address)	Description	Size in GB
ClientA_vol2	MPIO DS4500 Disk	30720

☑ **Virtual I/O Server:** VIOS_A

Server Adapter ID: Next Available

User Defined Name (Logical Unit Address)	Description	Size in GB
ClientA_vol1	MPIO DS4500 Disk	30720

☑ **Virtual I/O Server:** VIOS_A

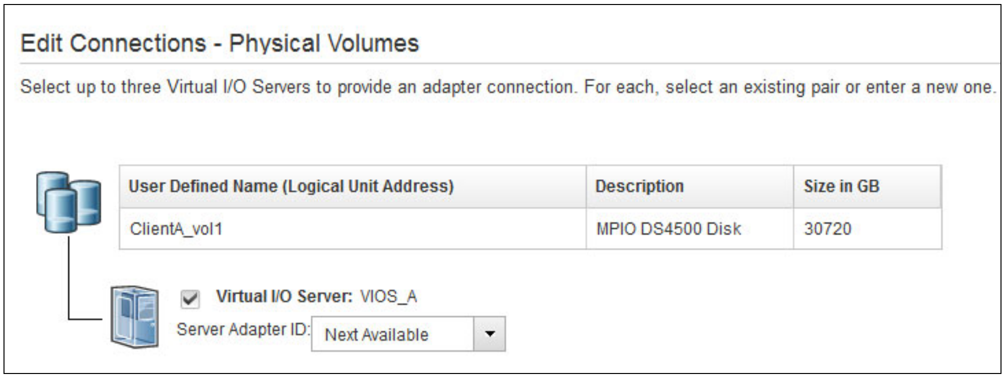
Server Adapter ID: Next Available

Figure 2-100 Deployment: Virtual SCSI connections - Multiple

If your managed system has multiple Virtual I/O Servers, you can select which VIOS you want for your virtual SCSI connections:

- Figure 2-99 on page 133 shows that multiple volumes were selected to be assigned to the logical partition upon deployment.
- Figure 2-100 shows that each volume has its *own* virtual SCSI connection, which might not be the configuration you want.

10. To associate multiple volumes with a single virtual SCSI connection, select only one volume at the time of deployment, as shown in Figure 2-101. After the logical partition is created, use the logical partition management functions to add the additional volumes to the created virtual SCSI connector.



Edit Connections - Physical Volumes

Select up to three Virtual I/O Servers to provide an adapter connection. For each, select an existing pair or enter a new one.

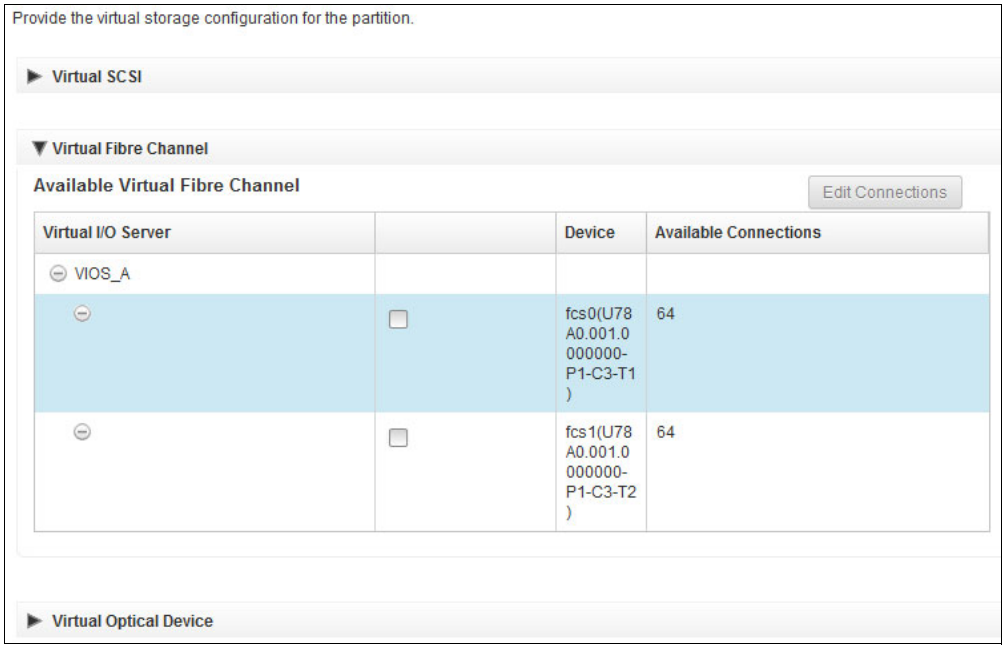
User Defined Name (Logical Unit Address)	Description	Size in GB
ClientA_vol1	MPIO DS4500 Disk	30720

☑ **Virtual I/O Server:** VIOS_A

Server Adapter ID: Next Available ▾

Figure 2-101 Deployment: Virtual SCSI Connections - Single

11. Expand **Virtual Fibre Channel** to view the available Fibre Channel adapters per VIOS, as shown in Figure 2-102.



Provide the virtual storage configuration for the partition.

▶ Virtual SCSI

▼ Virtual Fibre Channel

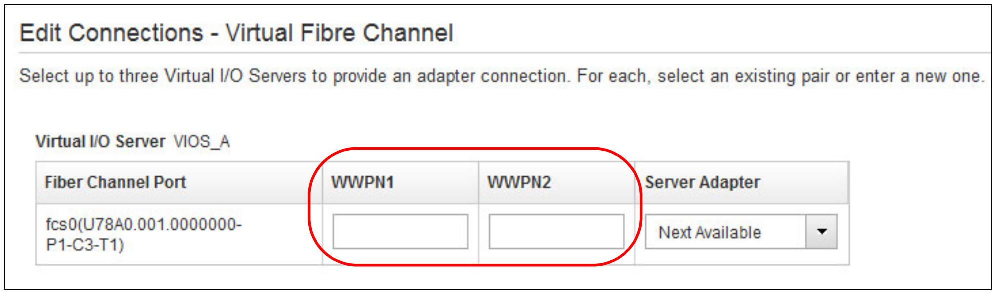
Available Virtual Fibre Channel

Virtual I/O Server		Device	Available Connections
⊖ VIOS_A			
⊖	□	fcs0(U78A0.001.0000000-P1-C3-T1)	64
⊖	□	fcs1(U78A0.001.0000000-P1-C3-T2)	64

▶ Virtual Optical Device

Figure 2-102 Deployment: Virtual Fibre Channel

12. You can select a Fibre Channel adapter and click **Edit Connections** to enter appropriate WWPN values manually. If the fields are blank (Figure 2-103), the managed system auto-generates the WWPN values.



Edit Connections - Virtual Fibre Channel

Select up to three Virtual I/O Servers to provide an adapter connection. For each, select an existing pair or enter a new one.

Virtual I/O Server VIOS_A

Fiber Channel Port	WWPN1	WWPN2	Server Adapter
fcs0(U78A0.001.0000000-P1-C3-T1)			Next Available

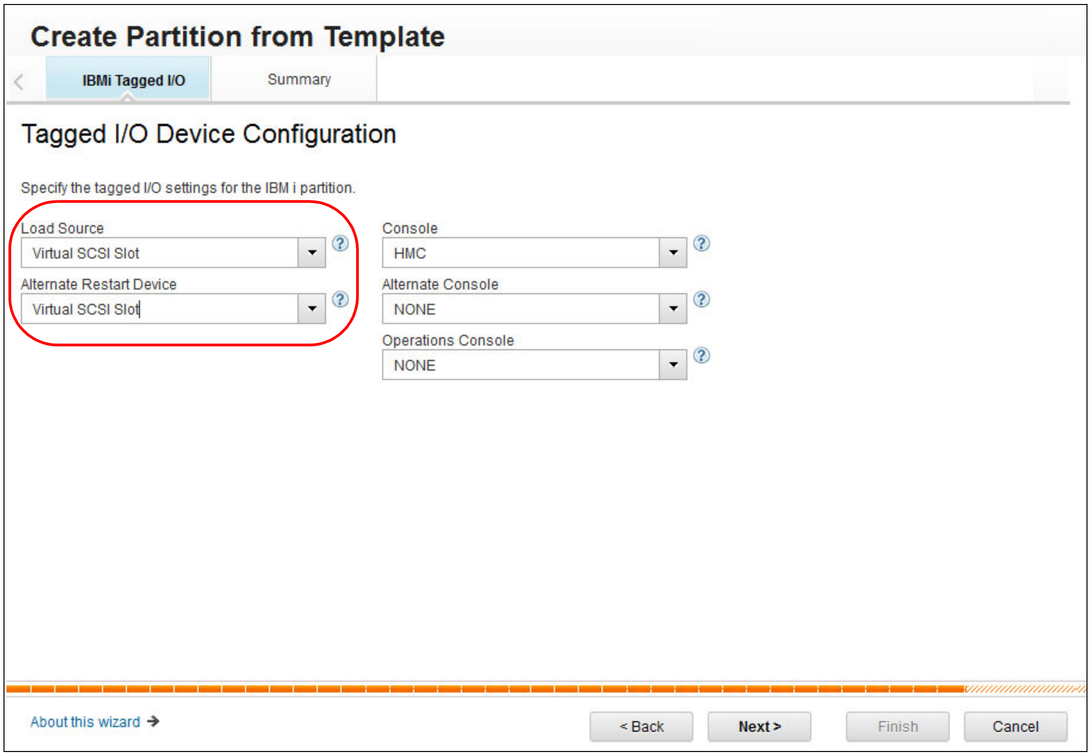
Figure 2-103 Virtual Fibre Channel connections

Expanding **Virtual Optical Drive** shows the available virtual optical devices, if they are present in your managed system. If they are present, create a connection to the virtual optical device.

13. Modify the virtual storage connections to suit your environment, and then click **Next** to move to the next tab.

14. For an IBM i logical partition, as part of the deployment, the Tagged I/O Device Configuration must be specified.

    While you are using the deployment wizard, if you specified virtual storage connections, you can use the drop-down menu to select **Virtual SCSI Slot** for the Load Source and Alternate Restart Devices fields, as shown in Figure 2-104.



Create Partition from Template

Tagged I/O Device Configuration

Specify the tagged I/O settings for the IBM i partition.

Load Source: Virtual SCSI Slot

Alternate Restart Device: Virtual SCSI Slot

Console: HMC

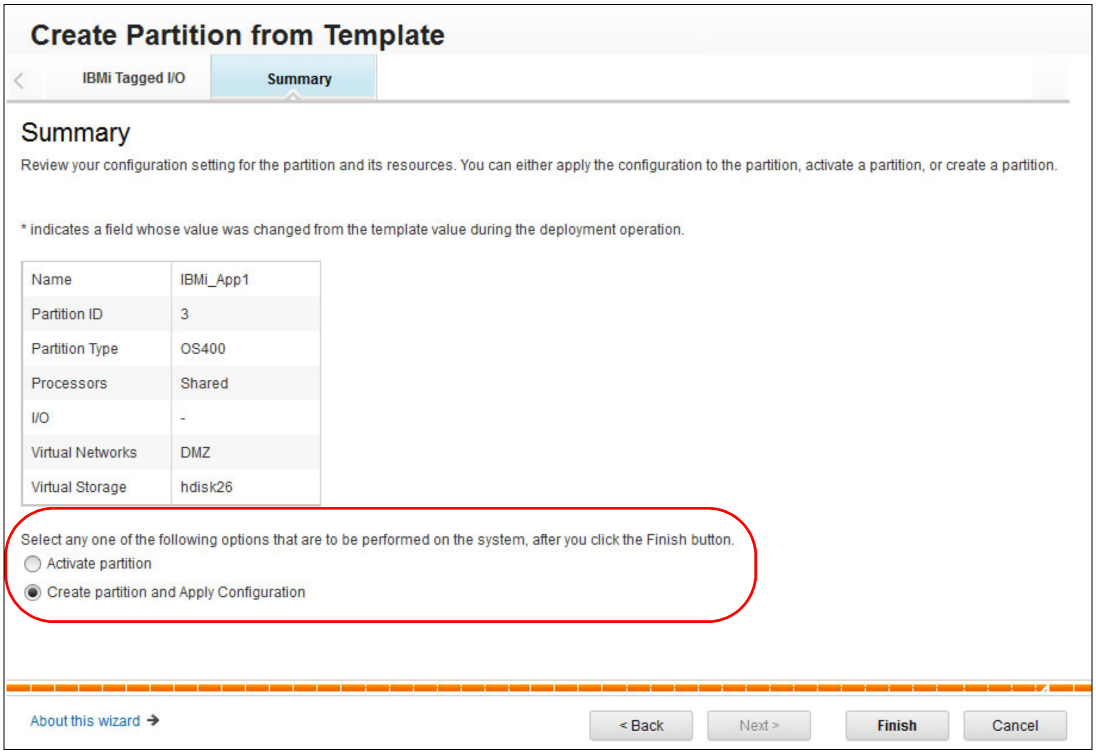
Alternate Console: NONE

Operations Console: NONE

Figure 2-104 IBM i Tagged I/O Device Configuration

15. Modify the Tagged I/O to suit your environment, and then click **Next** to move to the next tab.

The Summary tab (Figure 2-105) displays your selections and is the final opportunity if you want to go back and modify your settings *before* you start the deployment of the logical partition from the template. You can click **Back** to go back to the previous tabs and modify the setting in those tabs.



Create Partition from Template

Summary

Review your configuration setting for the partition and its resources. You can either apply the configuration to the partition, activate a partition, or create a partition.

* indicates a field whose value was changed from the template value during the deployment operation.

Name	IBMi_App1
Partition ID	3
Partition Type	OS400
Processors	Shared
I/O	-
Virtual Networks	DMZ
Virtual Storage	hdisk26

Select any one of the following options that are to be performed on the system, after you click the Finish button.

○ Activate partition

● Create partition and Apply Configuration

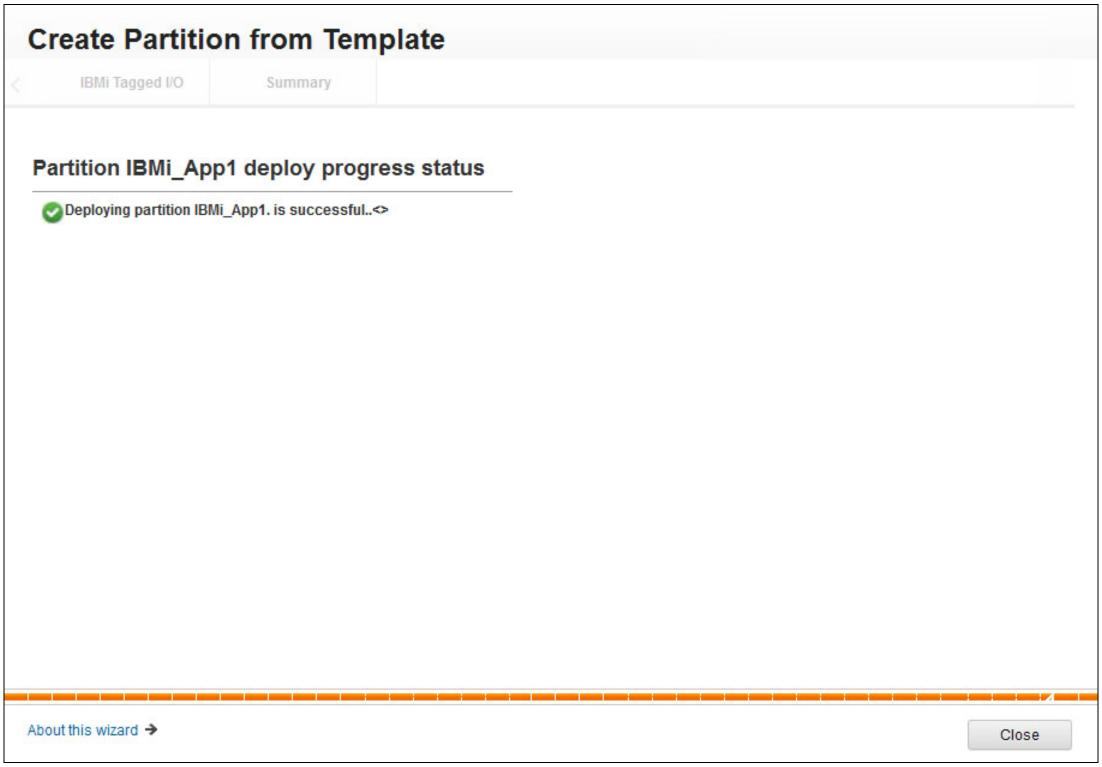
Figure 2-105 Deployment Summary tab

Use the remaining option, highlighted in the figure on this Summary tab to decide whether to activate the partition after deployment or to create the logical partition only after deployment.

If your logical partition has multiple volumes and you have not specified them as part of the template deployment wizard, create the partition and then modify the logical partition configuration by using the PowerVM Management functions.

16.Click **Finish** when you are ready to begin the deployment of your logical partition on to your managed system.

17. With a properly configured template and PowerVM environment, a successful deployment of your template can be achieved, as shown in Figure 2-106. Click **Close**.



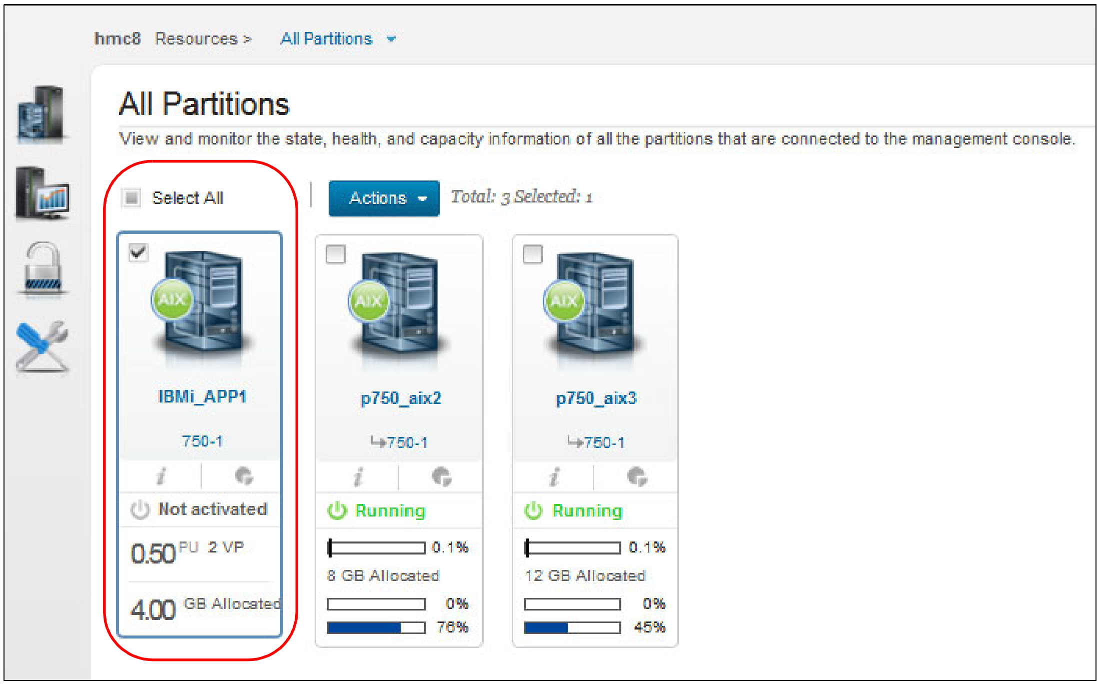
Create Partition from Template

Partition IBMi_App1 deploy progress status

Deploying partition IBMi_App1. is successful..<>

Figure 2-106 Deployment completed successfully

Select your managed system from the navigator pane of the HMC to now show the created logical partition that is based on the template configuration, as shown in Figure 2-107.



All Partitions

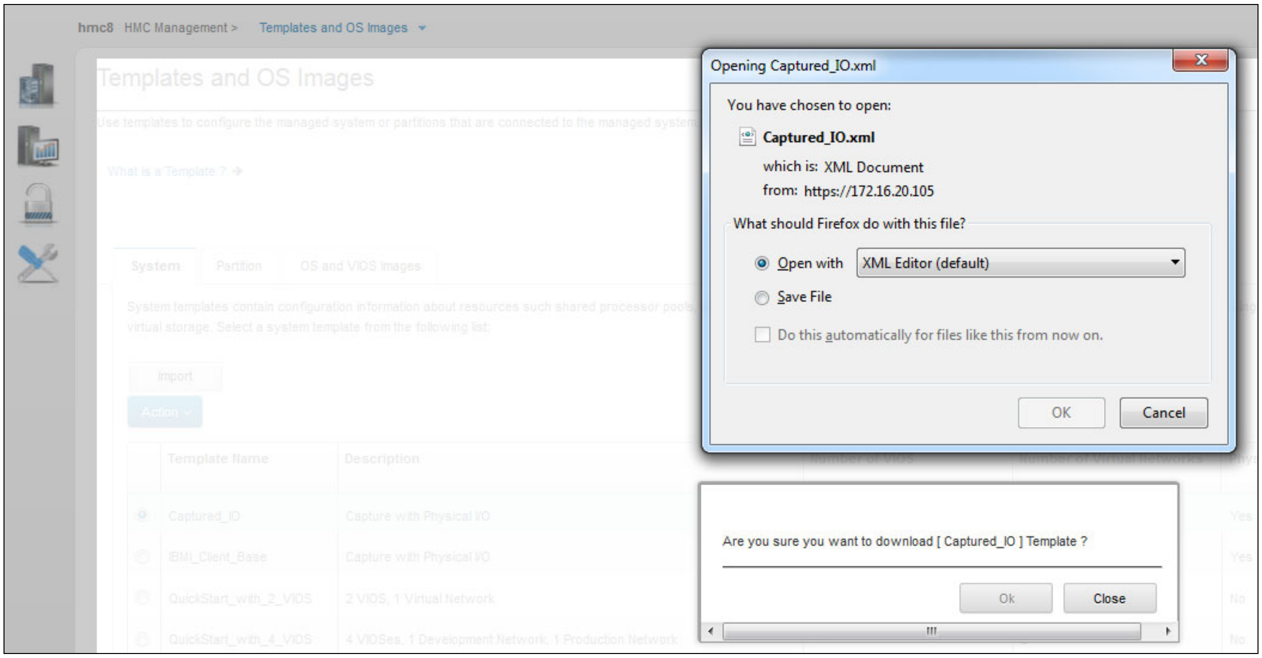
View and monitor the state, health, and capacity information of all the partitions that are connected to the management console.

Figure 2-107 Logical partition created in a managed system

2.6.5 Exporting templates

Included with the new template functions of HMC is the ability to export your partition template configuration.

To export your template, select your template in the Templates and OS Images, right-click your template, and select **Export**. The window that is shown in Figure 2-108 opens.



hmc8 HMC Management > Templates and OS Images

Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system

What is a Template ?

System | Partition | OS and VIOS Images

System templates contain configuration information about resources such shared processor pools, virtual storage. Select a system template from the following list:

Import

Action

	Template Name	Description
●	Captured_IO	Capture with Physical I/O
○	IBMi_Client_Base	Capture with Physical I/O
○	QuickStart_with_2_VIOS	2 VIOS, 1 Virtual Network
○	QuickStart_with_4_VIOS	4 VIOSes, 1 Development Network, 1 Production Network

Opening Captured_IO.xml

You have chosen to open:

Captured_IO.xml

which is: XML Document

from: https://172.16.20.105

What should Firefox do with this file?

● Open with XML Editor (default)

○ Save File

□ Do this automatically for files like this from now on.

OK Cancel

Are you sure you want to download [Captured_IO] Template ?

Ok Close

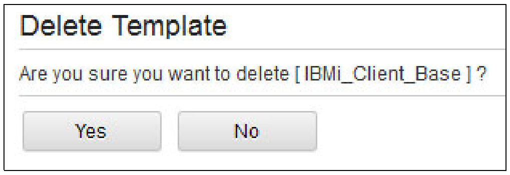
Figure 2-108 Export of a partition template

This function can be used to export your template configuration to another HMC that supports templates. To import the template, click **Import** in the Templates and OS Images in the other HMC.

This function also can be used as an off site type backup of your customized templates.

2.6.6 Deleting templates

Included with the new template functions of HMC V8.8.4.0 is the ability to delete your template configurations. To do so, select your template in the Templates and OS Images, right-click your template, and select **Delete**. The window that is shown in Figure 2-109 opens. To delete the template, click **Yes**.



Delete Template

Are you sure you want to delete [IBMi_Client_Base] ?

Yes No

Figure 2-109 Delete Template

2.7 Virtualization introduction

This section describes basic concepts of PowerVM and Virtualization in a Power Server environment.

2.7.1 PowerVM introduction

IBM PowerVM provides the industrial strength virtualization solution for IBM Power Systems servers. Based on more than a decade of evolution and innovation, PowerVM represents the state of the art in enterprise virtualization and is broadly deployed in production environments worldwide by most Power systems owners. The IBM Power systems family of servers includes proven workload consolidation platforms that help clients control costs while they improve overall performance, availability, and energy efficiency.

PowerVM can help eliminate under utilized servers because it is designed to pool resources and optimize their use across multiple application environments and operating systems. Through advanced virtual machine (VM) capabilities, a single VM can act as a separate IBM AIX, IBM i, or Linux operating environment, by using dedicated or shared system resources.

For more information about PowerVM, see *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940 and *IBM PowerVM Virtualization Managing and Monitoring*, SG24-7590.

Processor virtualization

PowerVM can automatically adjust pooled processor resources across multiple operating systems, borrowing capacity from idle VMs to handle high resource demands from other workloads.

Micro-Partitioning

IBM Micro-Partitioning supports multiple VMs per processor core and, depending upon the Power Systems model, can run up to 1000 VMs on a single server, each with its own processor resources.

Multiple Shared Processor Pools

Multiple Shared Processor Pools allow for the automatic nondisruptive balancing of processing power between VMs assigned to shared pools, resulting in increased throughput.

Shared Dedicated Capacity

Shared Dedicated Capacity allows for the “donation” of spared CPU cycle from dedicated processor VMs to a Shared Processor Pool. Because a dedicated VM maintains absolute priority for processor cycles, enabling this feature can increase system utilization without compromising the computing power for critical workloads.

Power Enterprise Pool

A Power Enterprise Pool is a group of enterprise systems that can share Mobile Capacity on Demand (CoD) processor and memory resources. With this you can flexible manage large workloads in a pool of systems and rebalance the resources to respond to business need.

For more information about Power Enterprise Pools, see *Power Enterprise Pools on IBM Power Systems*, REDP-5101.

Memory virtualization

With PowerVM, pooled memory resources can be adjusted across multiple operating systems, to handle high resource demands from other workloads.

Active Memory Sharing

IBM Active Memory Sharing (AMS) is a technology that can intelligently and dynamically reallocate memory from one VM to another for increased utilization, flexibility, and performance. AMS enables the sharing of a pool of physical memory among VMs on a server, helping to increase memory utilization and lower system costs. The memory is dynamically allocated among the VMs as needed to optimize the overall physical memory usage in the pool.

For more information about Active Memory Sharing, see *IBM PowerVM Virtualization Active Memory Sharing*, REDP-4470.

Active Memory Deduplication

Active Memory Deduplication is a powerful optimization feature that can be enabled when Active Memory Sharing is in use. This memory optimization intelligently detects and removes duplicate memory pages that are used between VMs and as a result reduces overall memory consumption.

I/O virtualization

PowerVM can automatically adjust pooled processor resources across multiple operating systems, borrowing capacity from idle VMs to handle high resource demands from other workloads.

Virtual I/O Server (VIOS)

The VIOS is a special purpose VM that can be used to virtualize I/O resources for AIX, IBM i, and Linux client VMs. The VIOS owns the resources that are shared with clients. A physical adapter that is assigned to the VIOS can be shared by one or more other VMs. The VIOS can reduce costs by eliminating the need for dedicated network adapters, disk adapter and disk drives, CD-ROMS, and tape adapters and tape drives in each client VM. With VIOS, client VMs can easily be created for test, development, or production purposes.

Shared Storage Pools

Shared Storage Pools (SSP) allows storage subsystems to be combined into a common pool of virtualized storage that can be shared by the Virtual I/O Server on multiple Power Systems. SSP supports capabilities such as thin provisioning, whereby VM storage is dynamically allocated and released as required, to improve overall storage resource utilization.

Virtual Fibre Channel

Virtual Fibre Channel, or N_Port ID Virtualization (NPIV), provides direct access to Fibre Channel adapters from multiple VMs, simplifying the deployment and management of Fibre Channel SAN environments.

Single root I/O virtualizaton (SR-IOV)

Single root I/O virtualization (SR-IOV) is a peripheral component interconnect express (PCIe) standard architecture that define extensions to PCIe specifications to enable multiple logical partitions running simultaneously within a system to share PCIe devices. The architecture defines virtual replicas of PCI functions known as virtual functions (VF). A logical partition can connect directly to an SR-IOV adapter VF without going though a virtual intermediary (VI) such as a Power Hypervisor or Virtual I/O Server. This provides for a low latency and lower CPU utilization alternative by avoiding a virtual intermediary.

Server virtualization

Server virtualization allows for the following key functions.

Live Partition Mobility (LPM)

LPM supports the movement of a running AIX, IBM i, or Linux VM from one Power Systems server to another without application downtime. This component helps to avoid application interruption for planned system maintenance, provisioning, and workload management. LPM can be used to simplify migration of operating environments to new servers temporarily or permanently.

Partition Suspend and Resume

The state of a partition can be suspended and resumed at a later time. The applicability and benefits of the suspend/resume feature include resource balancing and planned system outages for maintenance or upgrades. Lower priority or long running workloads can be suspended to free resources.

Partition Remote Restart

A logical partiton can be remotely restarted. Use this feature to recover the partitions quickly during a source server failure.

Partition simplified Remote Restart

The partition state and configuration data of a logical partition is automatically stored on each managing HMC. Any change to the partition configuration or profile is automatically synchronized with the data that is stored on the HMC.

Further virtualization features

Additional virtualization features are described in the following sections.

Active Memory Mirroring for Hypervisor

With active Memory Mirroring for Hypervisor, two identical copies of the system hypervisor of a managed system are maintained in memory always. But copies are simultaneously updated with any changes. If a memory failure occurs on the primary copy, the second copy is automatically called, eliminating platform outages due to uncorrectable errors in system hypervisor memory. Active Memory Mirroring for hypervisor is designed to ensure that system operations continues even in the unlikely event of an uncorrectable error that is occurring in main memory that is used by the system hypervisor.

Coherent Accelerator Processor Interface (CAPI)

With CAPI, an I/O adapter can be used as a coherent accelerator to participate in a memory coherency domain to accelerate system workloads.

Dynamic Platform Optimization

With Dynamic Platform Optimizer, you can dynamically optimize the placement of partitions. This function increases the processor-memory affinity of the partitions to improve the performance.

IBM i 5250 Application

With IBM i 5250 Application, you can run 5250 applications on the IBM i partitions of the managed system. The 5250 applications include all 5250 sessions (such as 5250 emulation, Telnet, and screen scrapers), interactive system monitors, and twin axial printer jobs.

2.7.2 Virtualization by using an HMC

With the HMC, you can control the virtualization of Power Systems servers (also called managed systems). The HMC uses a web-bossier-based interface or a command-line interface (CLI) to create and manage logical partitions (LPARs).

Logical partitions are a virtualized subset of the hardware resources of a physical system. An IBM Power System server can be partitioned into multiple logical partitions. Each logical partition can have a separate operating system: AIX, IBM i, or Linux.

Processor virtualization

The virtualization of physical processors in IBM Power Systems introduces an abstraction layer that is implemented within the IBM POWER® Hypervisor. The Power Hypervisor abstracts the physical processors and presents a set of virtual processors to the operating system within the micro-partitions on the system. A micro-partition can have a minimum of 0.05 (0.1 with POWER7 technology-based servers) of a processor up to the total processor capacity in the system. The granularity of processor entitlement is 0.01 of a processor, allowing entitlement to be precisely determined and configured.

In contrast, dedicated-processor logical partitions can be only allocated whole processors, so the maximum number of dedicated-processor logical partition in a system is equal to the number of physical activated processors.

Memory virtualization

IBM Power Systems provide *dedicated* memory allocation, and with two features (*Active Memory Sharing* and *Active Memory Expansion*) for memory virtualization, you can increase the flexibility and overall usage of physical memory:

- Dedicated

  The physical memory is distributed among the partitions.

- Active Memory Sharing (AMS)

  AMS enables the sharing of a pool of physical memory among AIX, IBM i and Linux partitions. The memory is dynamically allocated among the partitions as needed to optimize the overall physical memory usage in the pool.

- Active Memory Expansion (AME)

  AME is the ability to expand the memory that is available to an AIX partition beyond the amount of assigned physical memory. AME compresses memory pages to provide more memory capacity for a partition. Since the POWER7+ processor, a hardware accelerator is embedded in the processor chip for AIX memory compression. This offloads compression work from the processor and improves the overall performance.

Virtual I/O

Virtual I/O describes the ability to share physical I/O resources between partitions in the form of *virtual adapters* that are in the managed system.

Power Hypervisor for virtual I/O

The Power Hypervisor (PHYP) provides the interconnection for the partitions. To use the function of virtual I/O, a partition uses a virtual adapter as shown in Figure 2-110. The PHYP provides the partition with a view of an adapter that has the appearance of an I/O adapter, which might or might not correspond to a physical I/O adapter.

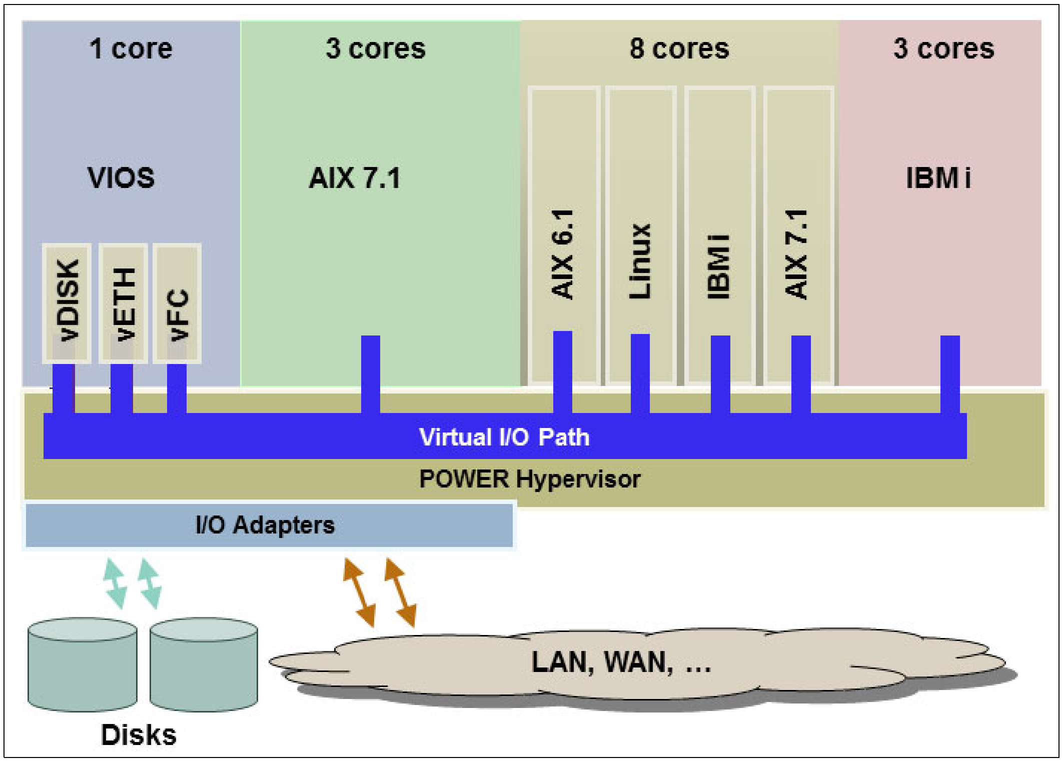


Figure 2-110 Role of PHYP for virtual I/O

Virtual I/O Server (VIOS)

The VIOS can link the physical resources to the virtual resources. By this linking, it provides virtual storage and Shared Ethernet Adapter capability to client logical partitions on the system. It allows physical adapters with attached disks on the VIOS to be shared by one or more client partitions.

VIOS mainly provides the following functions:

- Serves virtual SCSI devices to clients.
- Serves virtual Fibre Channel devices to clients.
- Provides Shared Ethernet Adapters for virtual Ethernet.

The VIOS is installed in its own logical partition. The VIOS partition is a special type of partition that is marked as such in the Create Logical Partitioning Wizard.

For further information about VIOS, see *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940.

Virtual Small Computer System Interface (virtual SCSI)

Virtual SCSI is based on a client/server relationship. A VIOS partition owns the physical resources and logical client partitions access the virtual SCSI resources that are provided by the VIOS partition. The VIOS partition has physically attached I/O devices and exports one or more of these devices to other partitions, as shown in Figure 2-111.

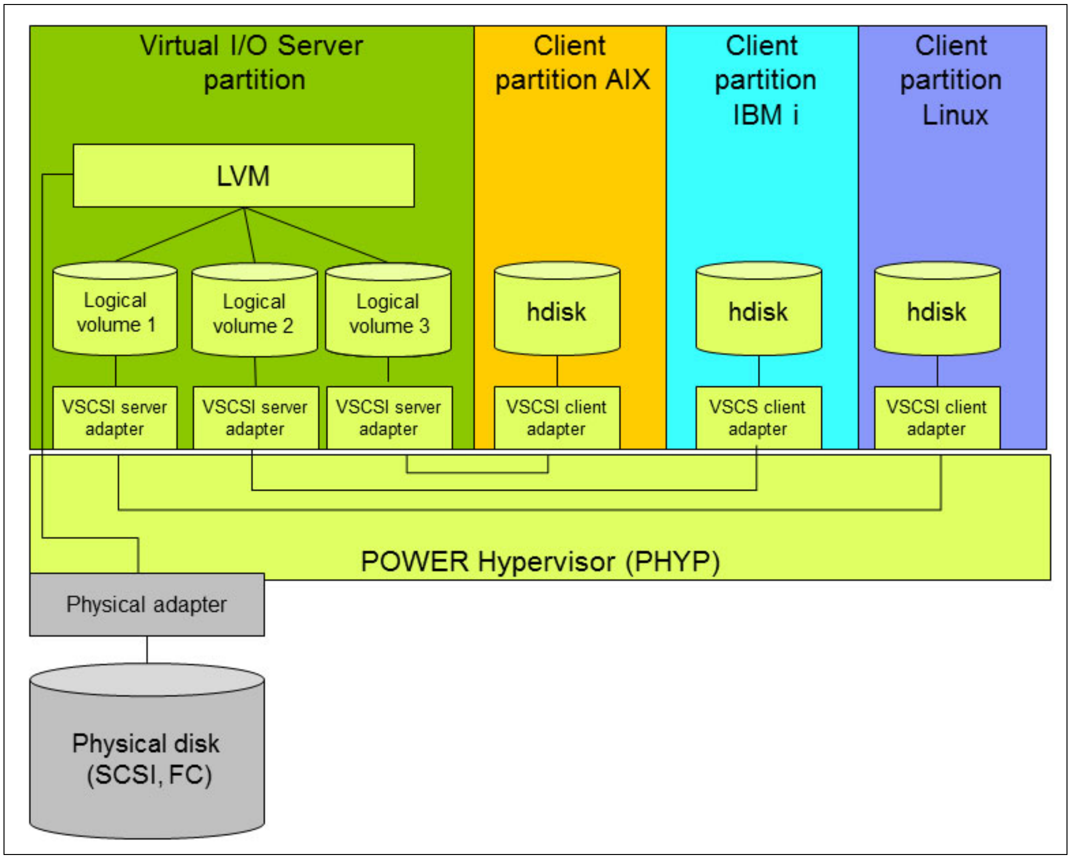


Figure 2-111 Virtual SCSI overview

Figure 2-111 shows that the virtual SCSI adapters on the server and the client are connected through the Hypervisor. The virtual SCSI adapter drives (server and client) communicate control data through the Hypervisor.

When data is transferred from the backing storage to the client partition, it is transferred to and from the clients data buffer by the DMA controller on the physical adapter by using redirected SCSI Remote Direct Memory Access (RDMA) Protocol. This facility enables the VIOS to securely target memory pages on the client to support virtual SCSI.

Virtual Fibre Channel

Just as with the virtual SCSI adapters, virtual Fibre Channel adapters (N_Port ID Virtualization (NPIV)), are based on a client/server relationship (Figure 2-112) and communicates control data through the Hypervisor.

On Power System server, Virtual Fibre Channel allows logical partitions to have dedicated N_Port IDs (WWN), giving the operating system a unique identity to the SAN. Virtual Fibre Channel is supported by AIX, IBM i, and Linux partitions.

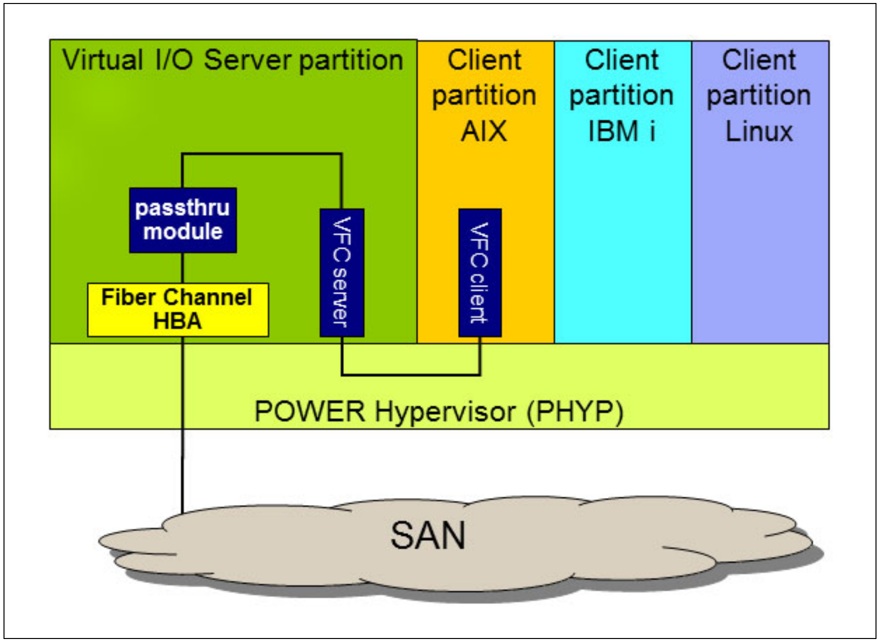


Figure 2-112 NPIV overview

Virtual Ethernet

Virtual Ethernet enables inter-partition communication without having physical network adapters that are assigned to each partition. Virtual Ethernet is a convenient and cost-saving option to enable partitions within a single system to communicate with one another through a virtual Ethernet LAN. These connections exhibit characteristics that are similar to physical high-bandwidth Ethernet connections and support multiple protocols (IPv4, IPv6, and Internet Control Message Protocol (ICMP)).

Virtual LAN (VLAN)

VLAN is a technology that is used for establishing virtual network segments on top of physical switch devices. Multiple VLAN logical devices can be configured on a single system, as shown in Figure 2-113. Each VLAN logical device constitutes an extra Ethernet adapter instance. These logical devices can be used to configure the same types of Ethernet IP interfaces as are used with physical Ethernet adapters.

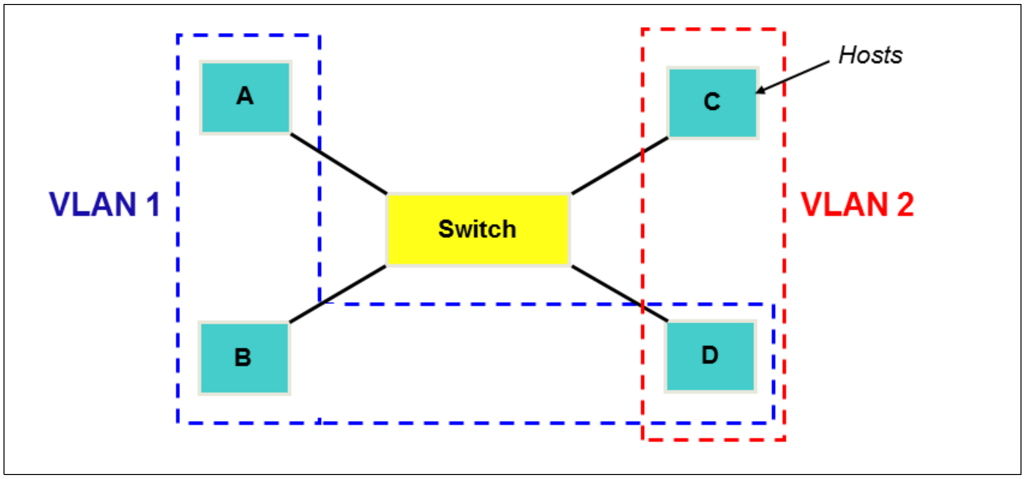


Figure 2-113 VLAN example of two VLANs

Virtual Ethernet connection

Virtual Ethernet connections use VLAN technology to ensure that partitions can access only data that is directed to them. The Power Hypervisor provides a virtual Ethernet switch function that is based on the IEEE 802.1Q VLAN standard that enables partition communication within the same servers, as shown in Figure 2-114. The connections are based on an implementation internal to the Hypervisor that moves data between partitions.

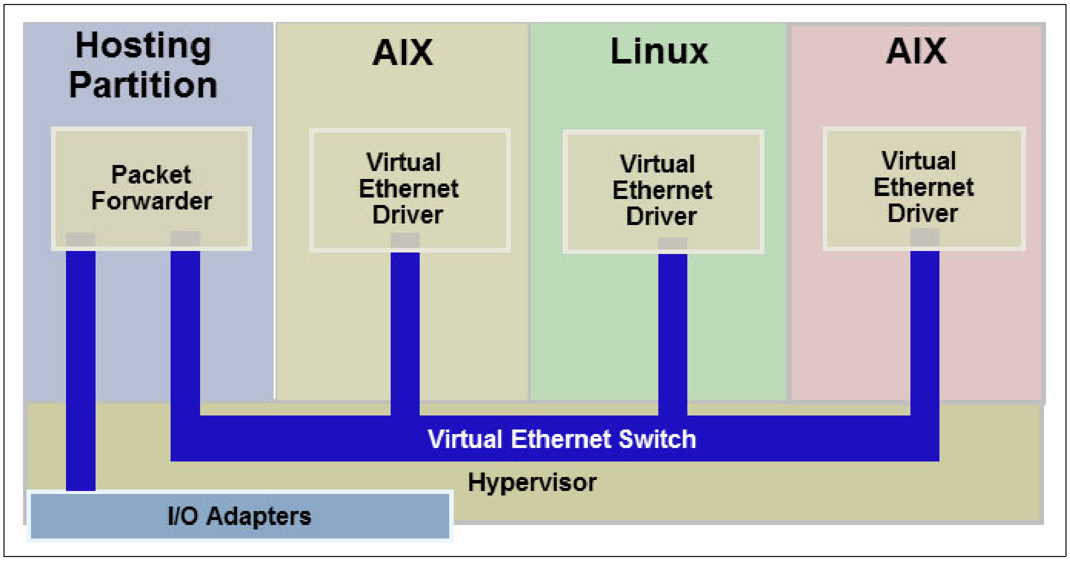


Figure 2-114 Virtual Ethernet connection

Shared Ethernet Adapter (SEA)

An SEA bridges external networks to internal networks. The SEA hosted in the VIOS partition acts as an OSI Layer 2 switch between the internal and external network.

Figure 2-115 shows the Shared Ethernet Adapter in a Virtual I/O Server that is used as a bridge between the virtual and physical Ethernet.

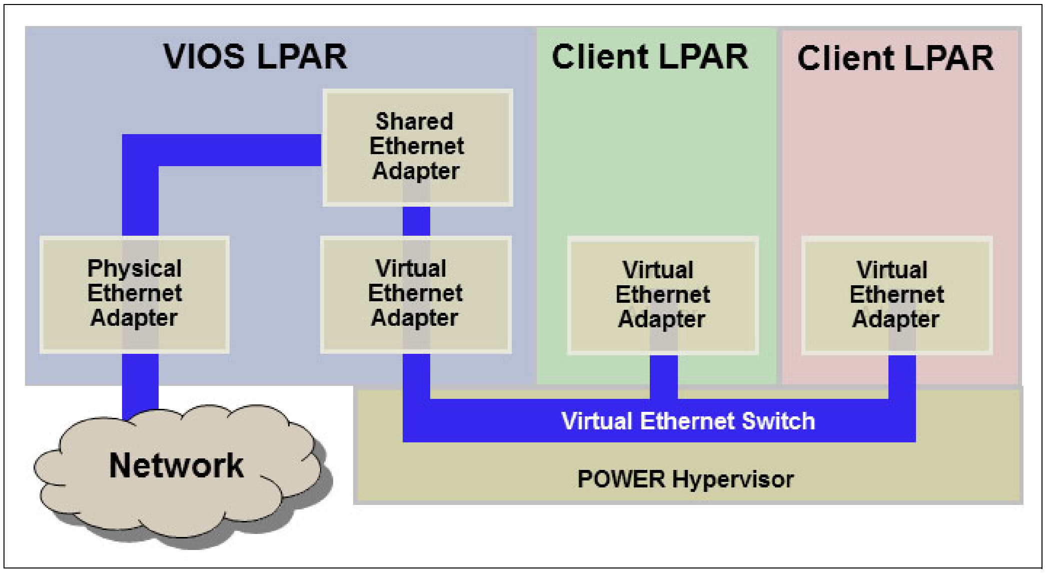


Figure 2-115 Shared Ethernet Adapter configuration

The bridge is transparent to the Internet Protocol (IP) layer. For example, when an IP host sends an IP datagram to another host on a network that is connected by a bridge, it sends the datagram directly to the host. The datagram crosses the bridge without the sending IP host being aware of it.

Live Partition Mobility (LPM)

With LPM, AIX, IBM i, and Linux partitions can be moved from one system to another. The mobility process transfers the system environment that includes the processor state, memory, attached virtual devices, and connected users.

You can use the HMC to move an active or inactive logical partition from one server to another:

- *Active partition mobility* moves AIX, IBM i, or Linux logical partitions while they are running, including the operating system and applications, from one system to another. The logical partition and the applications that run on that migrated partition do not need to be shut down.
- *Inactive partition mobility* moves a powered-off AIX, IBM i, or Linux logical partition from one system to another.

Because the HMC always moves the last activated profile, an inactive logical partition that has never been activated cannot be moved. For inactive partition mobility, you can either select the partition that is defined in the Hypervisor, or select the configuration data that is defined in the last activated profile on the source server.

Host Ethernet Adapter (HEA)

HEA is a physical Ethernet adapter that is integrated directly into the system bus on a managed system. HEAs offer high throughput, low latency, and virtualization support for Ethernet connections. HEAs are also known as Integrated Virtual Ethernet adapters (IVE adapters). Multiple logical partitions can connect directly to the HEA and use the HEA resources, This configuration allows these logical partitions to access external networks through the HEA without having to go through an Ethernet bridge (for example Shared Ethernet Adapter) or another logical partition (for example “Virtual I/O Server”).

2.8 Reliability, availability, and serviceability (RAS) on the HMC

The HMC is used for configuration, management, and maintenance of Power Systems. The HMC is considered to be part of the server firmware, so it is one of the resources that contributes to the system stability and normal operation.

2.8.1 Dual HMC and redundancy

You can configure a redundant HMC in a configuration in which dual HMC servers are connected to the service processors.

Using a redundant HMC configuration with your service processor setup requires a specific port configuration, as shown in Figure 2-116. In this configuration, each service processor connects to a network hub that is connected to each HMC. The network hubs that are connected to the service processors must remain in the *power-on* state.

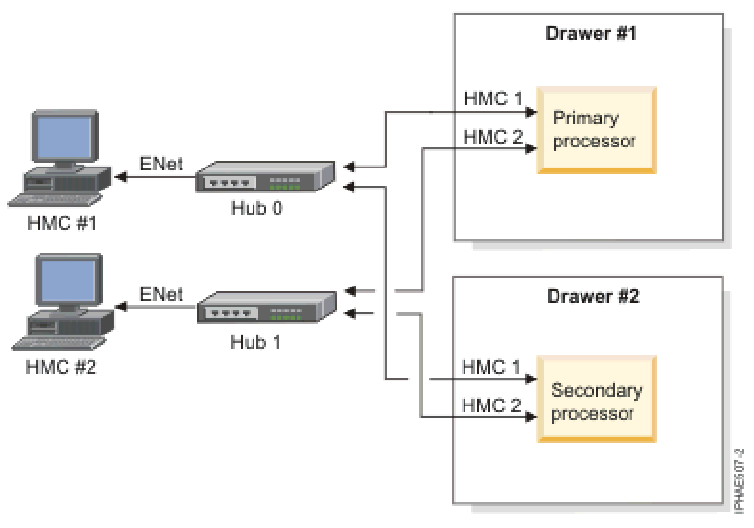


Figure 2-116 Dual HMC configuration on a private network

The HMC’s first Ethernet port should be configured to be a Dynamic Host Configuration Protocol (DHCP) server over a private network. By default, the service processor of a Power Server uses a DHCP client to request an IP address. This processor starts automatically when power is applied to the server or the service processor is reset. The service processor has two default IP addresses:

- 192.168.2.147 on HMC1 port
- 192.168.3.147 on HMC2 port

Always turn on the HMC first, then the server, during setup. This procedure allows for an IP address to be available for the service processor, by which the HMC can also discover the servers on its private service network, as shown in Figure 2-117.

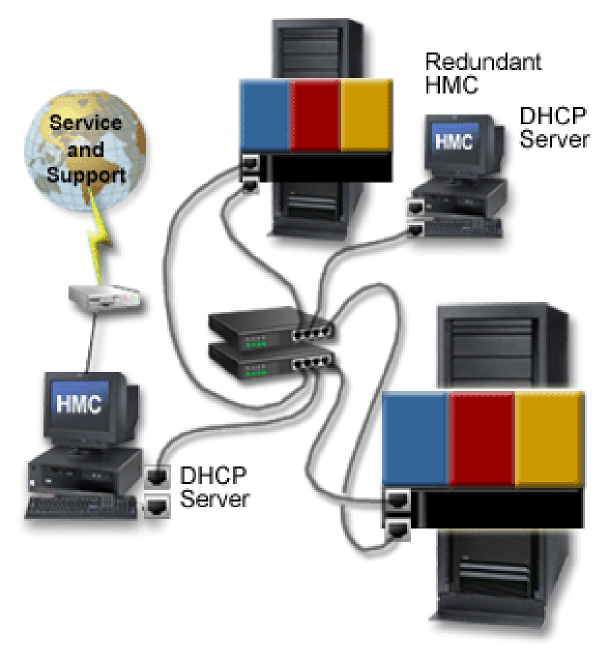


Figure 2-117   Dual HMC physical connections

This setup should also be done for virtual HMCs based on KVM or VMware Hosts. For information about configuring the network settings of an HMC, see 4.1.2, “Configuring the HMC network settings” on page 260.

Redundant remote HMC

A redundant remote HMC configuration is common. When clients have multiple sites or a disaster recovery site, they can use their second HMC in the configuration remotely over a switched network, as illustrated in Figure 2-118. The second HMC can be local, or it can be at a remote location. Use a different IP subnet for each HMC.

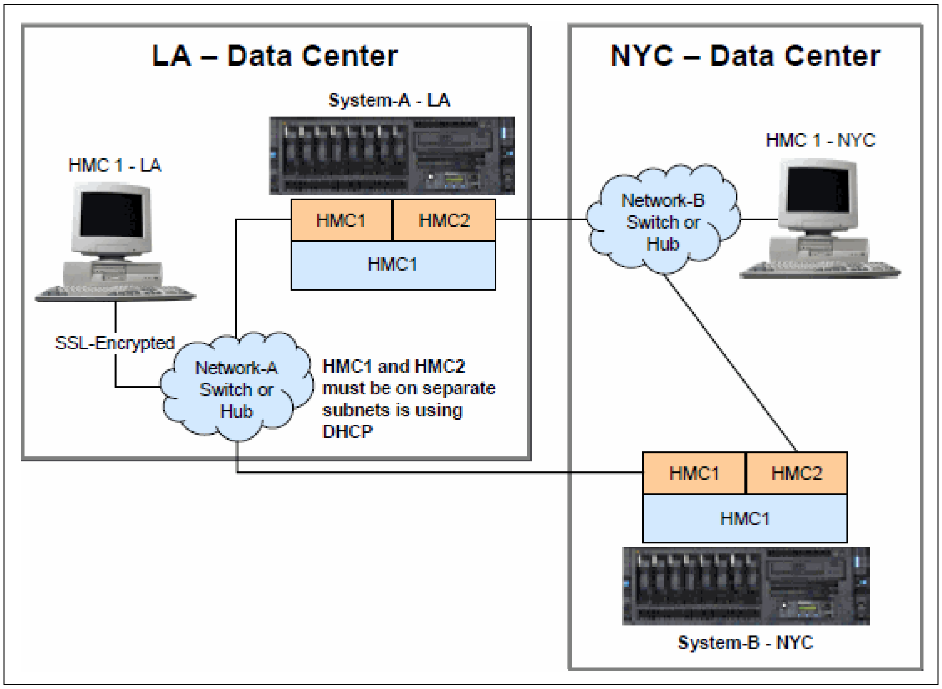


Figure 2-118 Example of redundant remote HMC

Redundant HMC configuration considerations

In a redundant HMC configuration, both HMCs are fully active and always accessible, enabling you to do management tasks from either HMC at any time. There is no primary or backup designation.

Consider the following points:

- Because authorized users can be defined independently for each HMC, determine whether users of one HMC should be authorized on the other. If so, the user authorization should be set up separately on each HMC.
- Because both HMCs provide Service Focal Point and Service Agent functions, connect only one of the HMCs to the Internet and enable its Service Agent. To prevent redundant service calls, do not enable the Service Agent on both HMCs.
- Perform software maintenance separately on each HMC, at separate times, so that there is no interruption in accessing HMC function. This maintenance allows one HMC to run at the new fix level, although the other HMC can continue to run at the previous fix level. However, the preferred practice is to upgrade both HMCs to the same fix level as soon as possible.

The basic design of a HMC eliminates the possible operation conflicts that are issued from two HMCs in a redundant HMC configuration. A locking mechanism that is provided by the service processor allows interoperation in a parallel environment. This allows the HMC to temporarily take exclusive control of the interface, effectively locking out the other HMC. Usually, this locking is held only for the short duration of time that it takes to complete an operation, after which the interface is available for further commands.

Both HMCs are automatically notified of any changes that occur in the managed systems, so the result of commands that are issued by one HMC are visible in the other. For example, if you choose to activate a partition from one HMC, you observe the partition going to the Starting and Running states on both HMCs.

The locking between HMCs does not prevent users from running commands that might seem to be in conflict with each other. For example, if the user on one HMC activates a partition, and a short time later a user on the other HMC selects to power off the system, the system turns off. Effectively, any sequence of commands that you can do from a single HMC is also allowed when it comes from redundant HMCs.

For this reason, an important consideration is to be careful how you use this redundant capability to avoid such conflicts. You might choose to use them in a primary and backup role, even though the HMCs are not restricted in that way. The interface-locking between two HMCs is automatic, usually of short duration, and most console operations wait for the lock to release without requiring user intervention.

However, if one HMC experiences a problem while in the middle of an operation, manually releasing the lock might be necessary. HMC 2 can be used to disconnect HMC 1. When an HMC is disconnected, all locks that are owned by the HMC are reset. To do this process, any `hmcsuperadmin` user can run the **Disconnect Another HMC GUI** task on HMC 2 against HMC1. This task can be done only from the graphical interface. A corresponding command-line version of this task is not available.

When you run two HMCs to the same server, also be careful with long-running functions because they might be affected if they are not completed before an extra function is run on the second HMC.

Considering the previous information, many good reasons exist to use the redundant HMC configuration. This list is not exhaustive:

- Redundancy of critical configuration information
- Ability to apply maintenance to an HMC while the other is available for production management functions
- Reduced risk of no HMC available
- Knowing that while running a long running command against one system, being able to use the second HMC to do functions on another system without waiting
- Continuos Performance Monitor data on one HMC

2.8.2 RAID 1 protection

Redundant Array of Independent Disks (RAID) is an industry-wide implementation of methods to store data on multiple physical disks to enhance the availability of that data. Since HMC V7R760, the HMC supports RAID 1.

RAID 1

Since HMC model 7042-CR7 and later models, by default, two hard disk drives are included with RAID 1 configured. RAID 1 is also offered on both the 7042-CR6 and the 7042-CR7 as an MES upgrade option. RAID 1 uses data mirroring. Two physical drives are combined into an array, and data is striped across the array. The first half of a stripe is the original data. The second half is a mirror of the data, but is written to the other drive in the RAID 1 array. RAID 1 requires two physical drives, enabling data redundancy.

Setting up RAID 1 protection

For configuring RAID 1 on a 7042-CR6 or 7042-CR7, see the IBM Redpaper™ publication *Converting Hardware Management Console (HMC) 7042-CR6 or 7042-CR7 Models to RAID1*, REDP-4909.

On a 7042-CR8 and 7042-CR9, RAID 1 is already configured with two hard drives with RAID 1 by default, unless you removed the additional hard disk drive (HDD) for the order in the ordering system.

For VMware and KVM Hosts, use a Hardware RAID 1 configuration on the system you use. For instructions of how to set up Hardware RAID 1, see your system documentation.

Rebuilding a RAID 1 array (HMC models only)

If a disk in the RAID 1 array of your HMC fails, it must be replaced. For instructions about replacing a drive, see the problem determination and service guide for your HMC model.

To rebuild a RAID 1 array on the HMC, complete the following steps:

1. Power on or restart the HMC.
2. When the system prompt is displayed, press the F1 key to access the Setup Utility.
3. In the System Setting window, use the up or down arrow keys to highlight **Storage** and then press Enter.
4. In the Storage window, use the up or down arrow keys to highlight **LSI MegaRAID Configuration Utility** and then press Enter.
5. In the Configuration Options window, use the up or down arrow keys to highlight **Drive Management** and then press Enter.
6. In the Select Drive Options window, press Enter. Use the up or down arrow keys to highlight the drive that is listed as **Unconfigured Bad** and then press Enter.
7. In the Select Drive Operations window, use the up or down arrow keys to highlight **Make Unconfigure Good** and then press Enter.
8. In the Success window, use the up or down arrow keys to Highlight **OK** and then press Enter.
9. In the Select Drive Operations window, use the up or down arrow keys to highlight **Assign Global Hot spare Drive** and then press Enter.
10. In the success window, use the up or down arrow keys to highlight **OK**, and then press Enter. The rebuild operation starts.
11. From the Setup menu, press the Esc key repeatedly to exit the Setup Utility.
12. In the Exit Setup window, press the Y key to save the changes and to exit the Setup Utility.
13. The HMC starts and the rebuild operation continues to run until it is complete.

3

Installation upgrade and updates

This chapter provides an overview of various methods to install, upgrade, and update the Hardware Management Console (HMC).

This chapter describes the following topics:

- DVD and ISO image installations
- Virtual appliances installations
- HMC Install Wizard
- HMC update
- HMC upgrade to a new software level

From an installation perspective, HMC V8R8.4.0 offers various types of installation over various platforms. The physical HMC requires either a network or a DVD installation. The KVM and VMWare virtual machines (VM) can be installed either with an ISO image or with a VM image.

For the network installation method, see Appendix E, “Preboot Execution Environment” on page 587. For more details about the HMC network installation, see the following web page:

http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/home.html

If you use a DVD on a physical HMC or an ISO image on a VMware or KVM, you must go through the complete HMC installation wizard. After you boot from your chosen source, the menus used for initial installation and configuration are exactly the same for a DVD or ISO image installation.

The V8R8.4.0 and later versions of the HMC can be installed into a virtual machine that is running on an x86 Hypervisor.

The virtual HMC (vHMC) provides images in two extra formats to allow for quick deployment of the vHMC on either ESXi or KVM hypervisors. If you chose the VM deployment method, you avoid the installation steps and go directly to the configuration wizard.

A feature of the vHMC is the Activation Engine, which allows you to preconfigure the HMC Console by passing configuration information to the HMC at the first boot of the HMC, when using these images.

3.1 DVD and ISO image installations

You can install by using either a DVD or an ISO image file. For a physical HMC (or bare metal) installation, you must use a DVD media which can be ordered from the web, or a DVD you have burnt with a downloaded ISO image file. The exact same ISO image can be burnt on a DVD or used as a boot image from a VM.

HMC upgrade and recovery media can be ordered and downloaded from IBM Fix Central:

http://www.ibm.com/support/fixcentral

The three instances for DVD or ISO installation on an HMC are as follows:

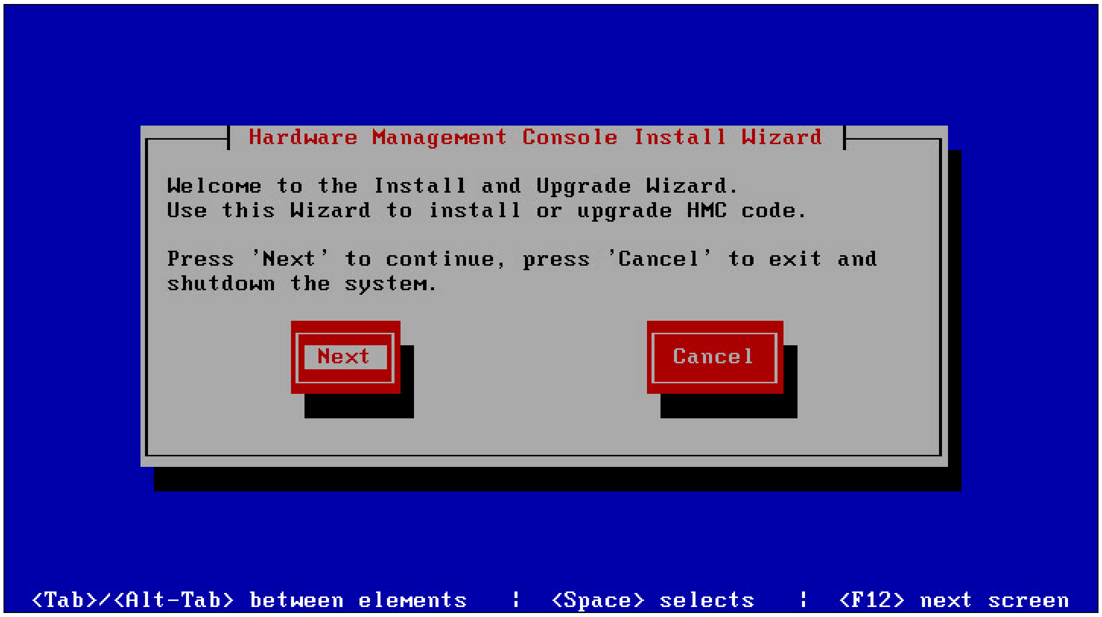
- Bare metal or physical machine installation
- VMware installation
- KVM installation

3.1.1 Physical HMC installation

Complete the following steps to install a physical HMC with the HMC recovery media:

1. Insert the HMC upgrade and recovery media DVD into the HMC drive, and boot the HMC. Depending on your BIOS setup, you may have to press the appropriate function key to explicitly choose to boot from the DVD.

   The HMC console now shows the initial HMC Install Wizard panel (Figure 3-1).



```
Hardware Management Console Install Wizard

Welcome to the Install and Upgrade Wizard.
Use this Wizard to install or upgrade HMC code.

Press 'Next' to continue, press 'Cancel' to exit and
shutdown the system.

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Figure 3-1 HMC Install Wizard

2. Proceed with the HMC Install Wizard. The installation instructions are described in 3.3, “HMC Install Wizard” on page 223.

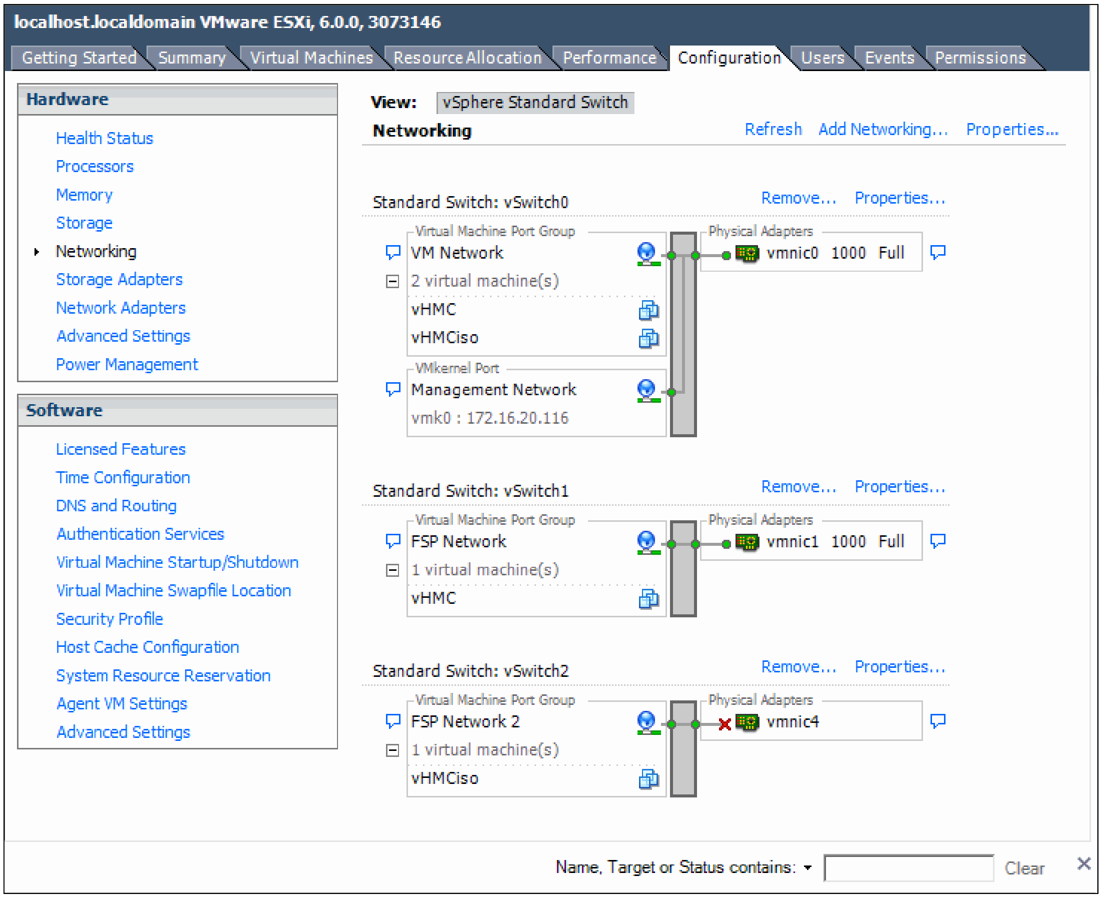
3.1.2 VMware installation

This section describes the steps to boot an HMC ISO image on VMware, with the vSphere client. You may use different steps with vCenter.

> **Note:** Prior to start any VM setup, upload the HMC ISO image file on the VMware server. There are options to start the virtual machine and upload the ISO image file from the vSphere client, but it would not be kept for any other deployment. Uploading the ISO image and having it available in a repository saves time for future deployments.

Before starting the HMC installation, the VMware server must be prepared with the proper network bridging setup. A minimum of one Network Interface Card (NIC) is required for your network. Nevertheless, on Power Servers and HMC installations, having a NIC for the service processor network and a NIC for the open network are common.

The following installation example has two separate physical NICs. One NIC is dedicated to the service processor network, and one to the open network (Figure 3-2).



localhost.localdomain VMware ESXi, 6.0.0, 3073146

View: vSphere Standard Switch

Networking

Standard Switch: vSwitch0

Virtual Machine Port Group: VM Network — 2 virtual machine(s): vHMC, vHMCiso

VMkernel Port: Management Network — vmk0 : 172.16.20.116

Physical Adapters: vmnic0 1000 Full

Standard Switch: vSwitch1

Virtual Machine Port Group: FSP Network — 1 virtual machine(s): vHMC

Physical Adapters: vmnic1 1000 Full

Standard Switch: vSwitch2

Virtual Machine Port Group: FSP Network 2 — 1 virtual machine(s): vHMCiso

Physical Adapters: vmnic4

Figure 3-2 VMware Networking Switch configuration

> **Important:** Having two HMCs used as Dynamic Host Configuration Protocol (DHCP) server on the same service processor network is not supported. Be careful about the switch bridging and do not have multiple HMCs with a DHCP server on the same service processor network.

To proceed with the HMC installation, complete the following steps:

1. From the main vSphere panel, press Ctrl+N, or right-click **New Virtual Machine** (Figure 3-3).

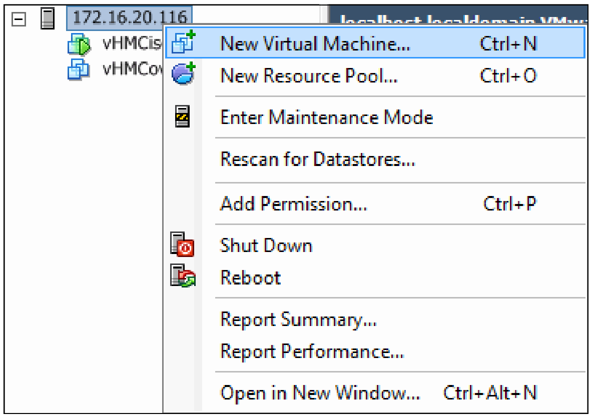
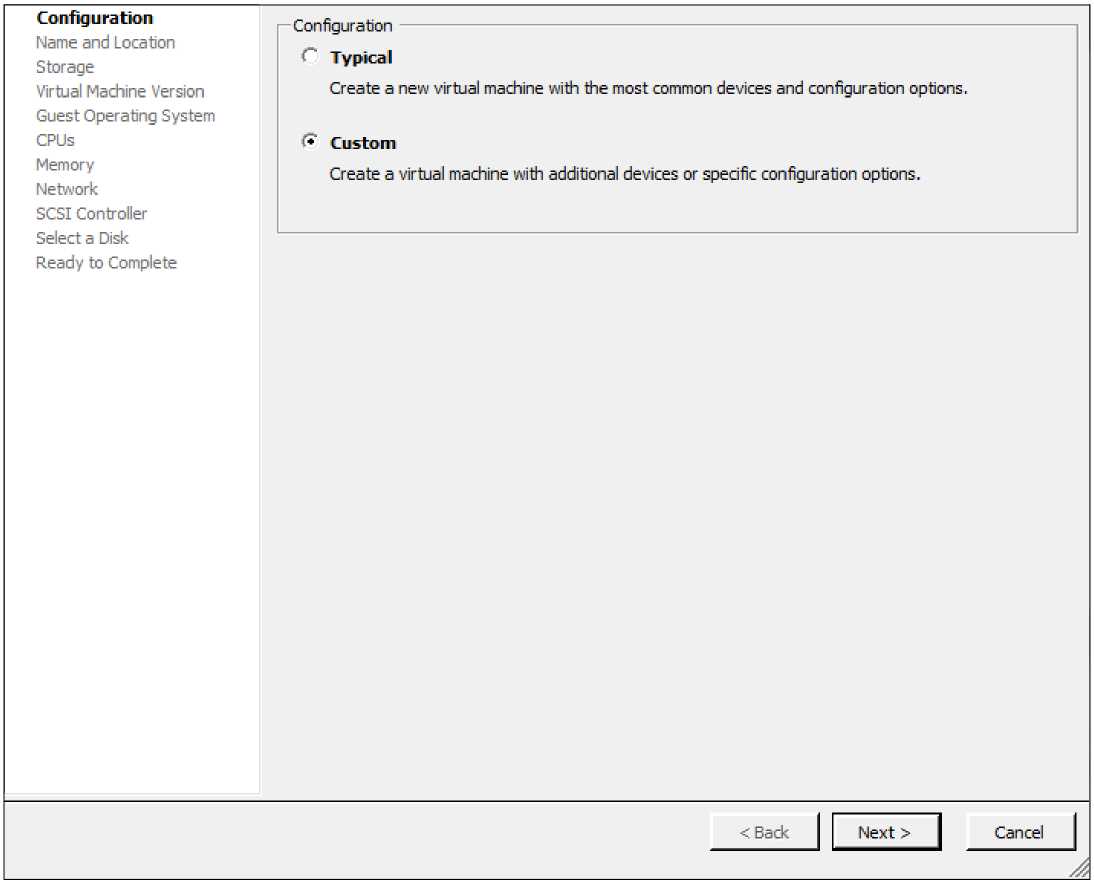


Figure 3-3 Create a new VM in vSphere

2. On the Configuration panel, choose **Custom** and click **Next** (Figure 3-4).



Configuration

○ **Typical**

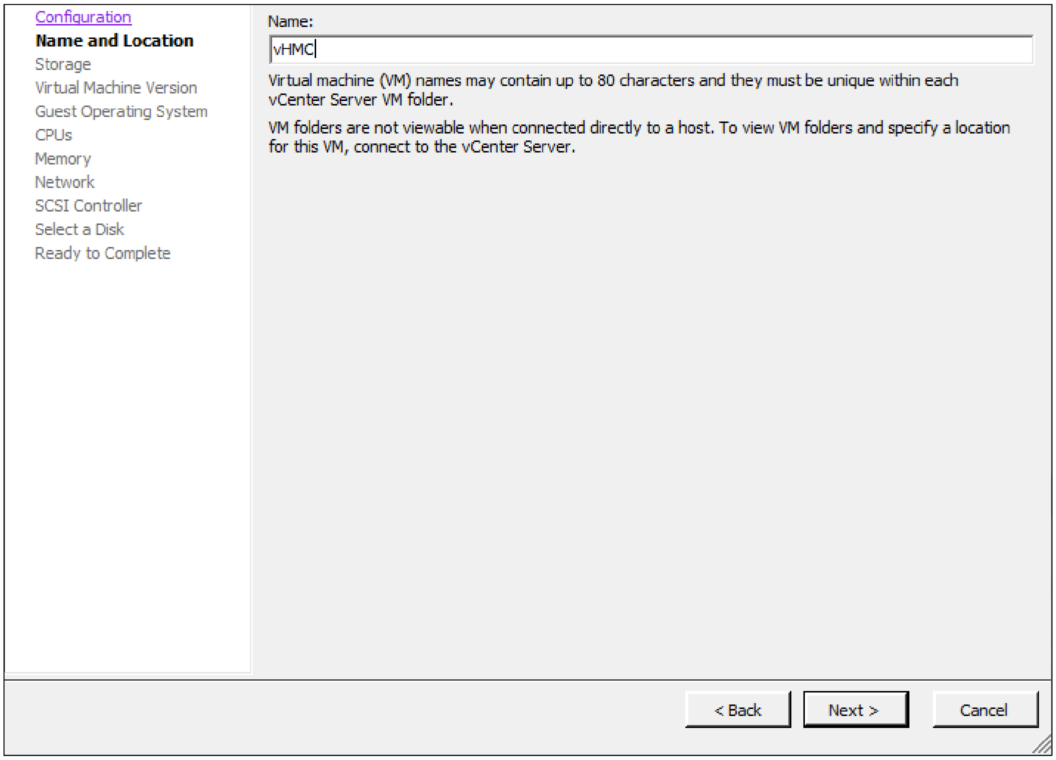
Create a new virtual machine with the most common devices and configuration options.

● **Custom**

Create a virtual machine with additional devices or specific configuration options.

Figure 3-4 Use custom type configuration

3. On the Name and Location panel (Figure 3-5), type in a name of your choice for your VM, and click **Next**.



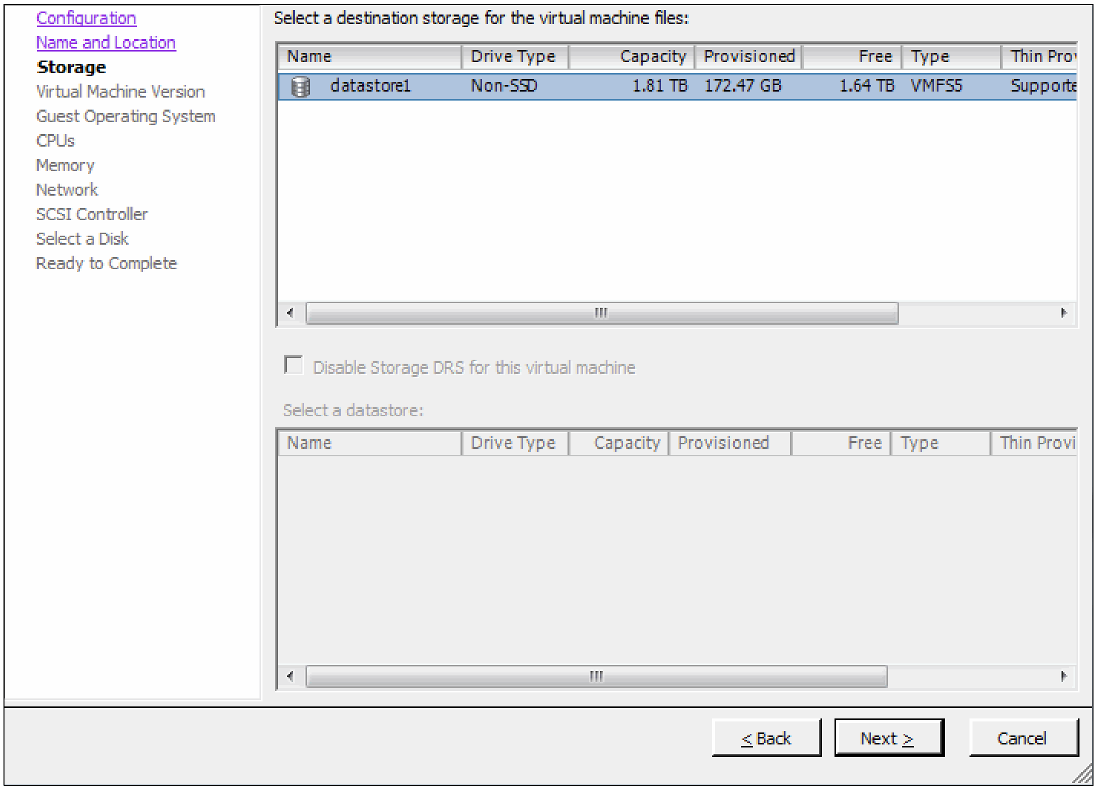
Name: vHMC

Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder.

VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.

Figure 3-5 Name and Location panel

4. Select the appropriate storage datastore (Figure 3-6) and click **Next**.



Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1	Non-SSD	1.81 TB	172.47 GB	1.64 TB	VMFS5	Supporte

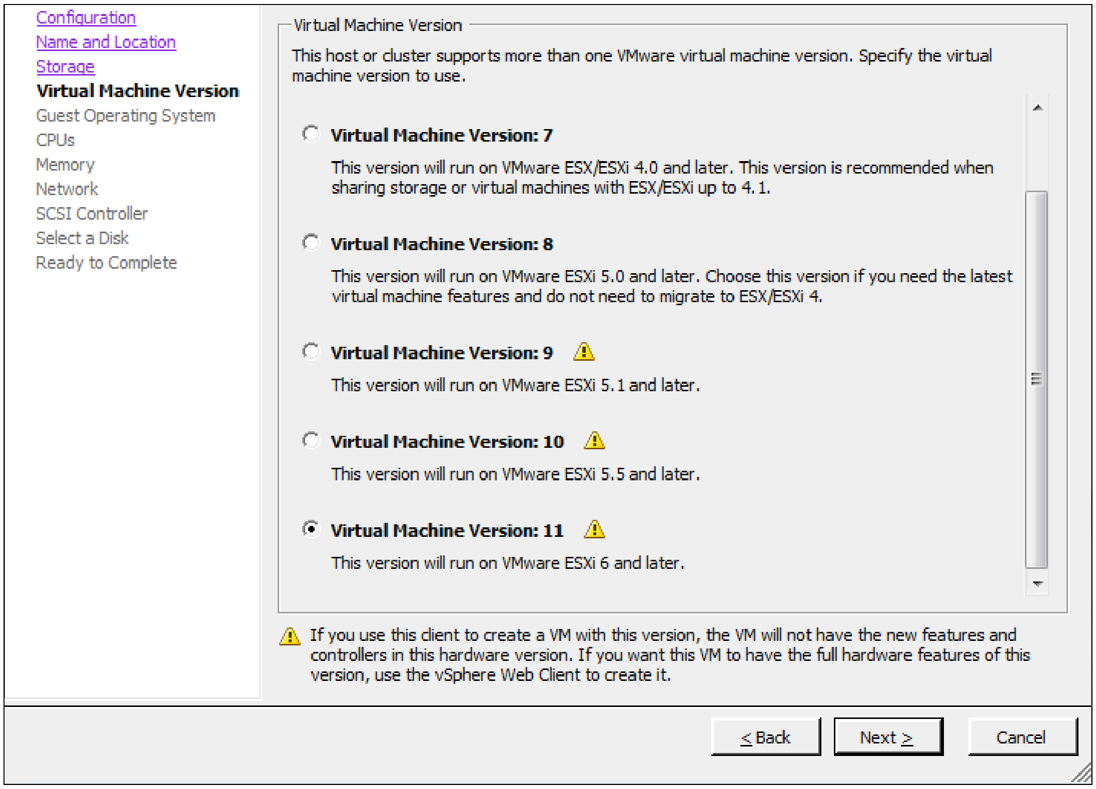
□ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi

Figure 3-6 Select the storage datastore

5. Select the version appropriate to your VMware ESXi version in the Virtual Machine Version panel (Figure 3-7), and then click **Next**.



Virtual Machine Version

This host or cluster supports more than one VMware virtual machine version. Specify the virtual machine version to use.

○ **Virtual Machine Version: 7**

This version will run on VMware ESX/ESXi 4.0 and later. This version is recommended when sharing storage or virtual machines with ESX/ESXi up to 4.1.

○ **Virtual Machine Version: 8**

This version will run on VMware ESXi 5.0 and later. Choose this version if you need the latest virtual machine features and do not need to migrate to ESX/ESXi 4.

○ **Virtual Machine Version: 9** ⚠

This version will run on VMware ESXi 5.1 and later.

○ **Virtual Machine Version: 10** ⚠

This version will run on VMware ESXi 5.5 and later.

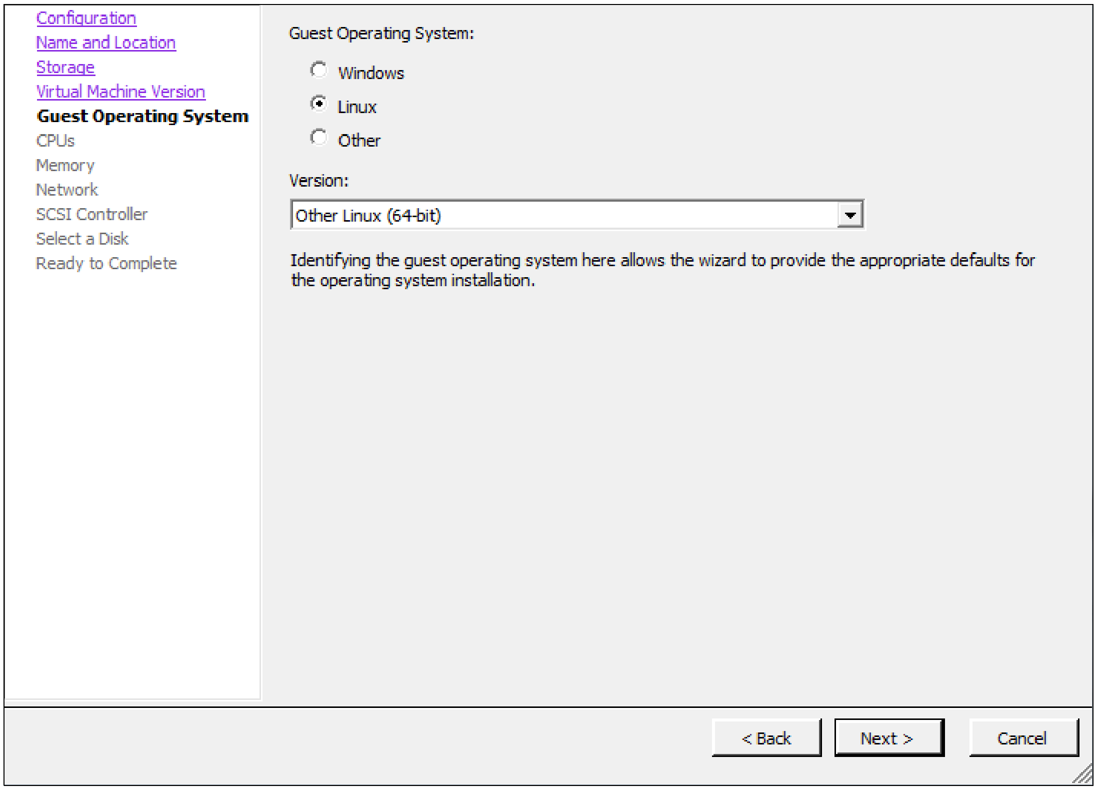
● **Virtual Machine Version: 11** ⚠

This version will run on VMware ESXi 6 and later.

⚠ If you use this client to create a VM with this version, the VM will not have the new features and controllers in this hardware version. If you want this VM to have the full hardware features of this version, use the vSphere Web Client to create it.

Figure 3-7 Virtual machine version selection

6. For the Guest Operating System (Figure 3-8), select **Linux**. Then select **Other Linux (64-Bit)** or **Red Hat Linux 6.3 (64-Bit)** from the Version list. Click **Next**.



Guest Operating System:

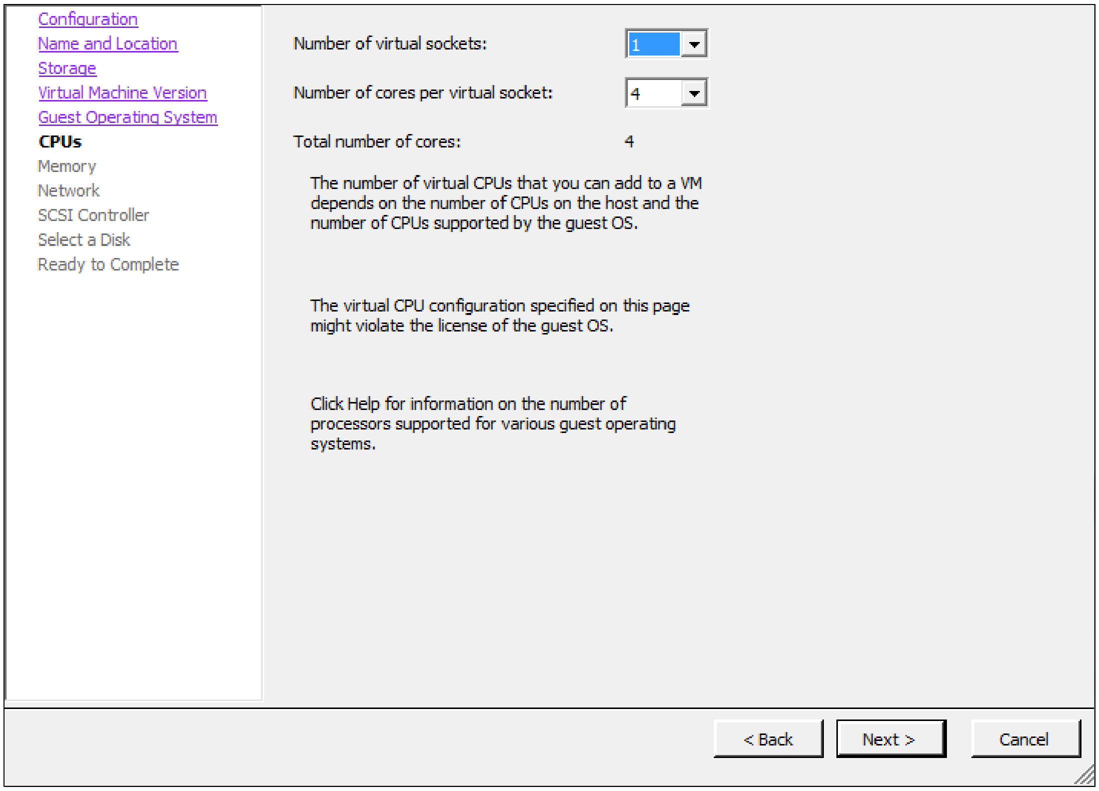
○ Windows
● Linux
○ Other

Version: Other Linux (64-bit)

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Figure 3-8 Guest Operating System version

7. In the CPUs panel (Figure 3-9), select the number of virtual sockets and cores and click **Next**. In this example, the choice is 4 cores.



Number of virtual sockets: 1

Number of cores per virtual socket: 4

Total number of cores: 4

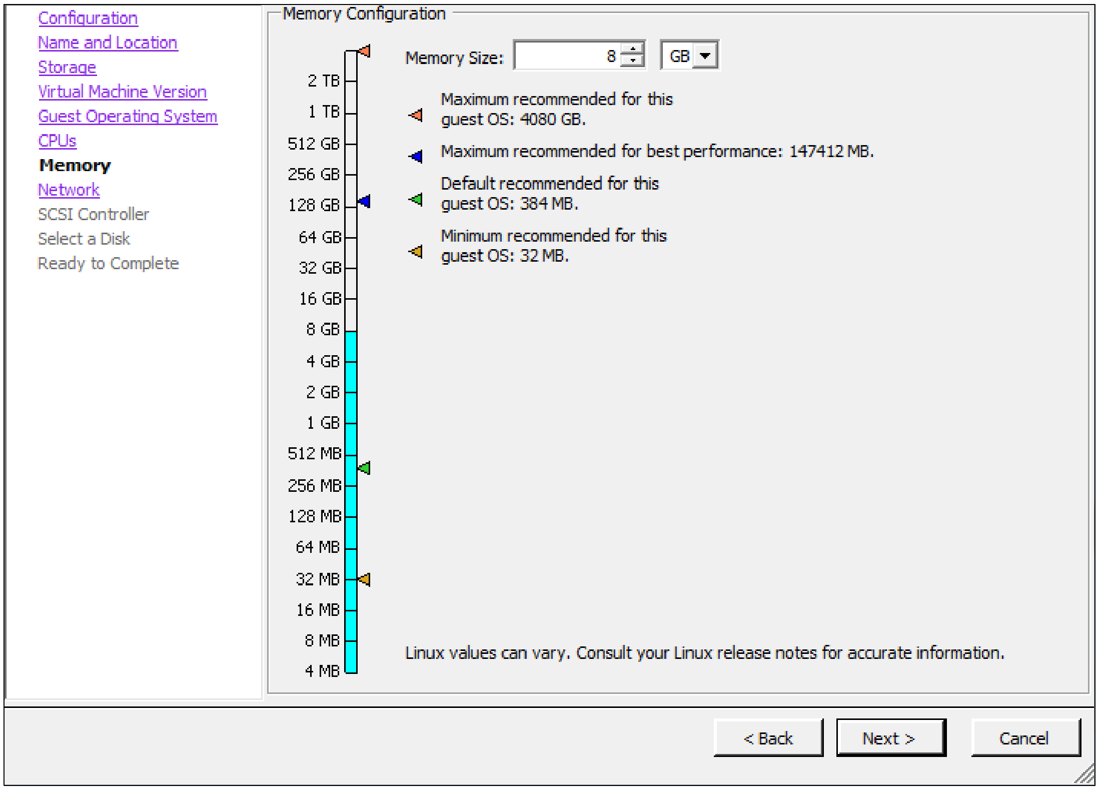
The number of virtual CPUs that you can add to a VM depends on the number of CPUs on the host and the number of CPUs supported by the guest OS.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

Click Help for information on the number of processors supported for various guest operating systems.

Figure 3-9 Select the appropriate number of cores

8. In the Memory panel (Figure 3-10), specify the amount of memory you need and click **Next**. In this example, the size is set to 8 GB.



Memory Size: 8 GB

Maximum recommended for this guest OS: 4080 GB.

Maximum recommended for best performance: 147412 MB.

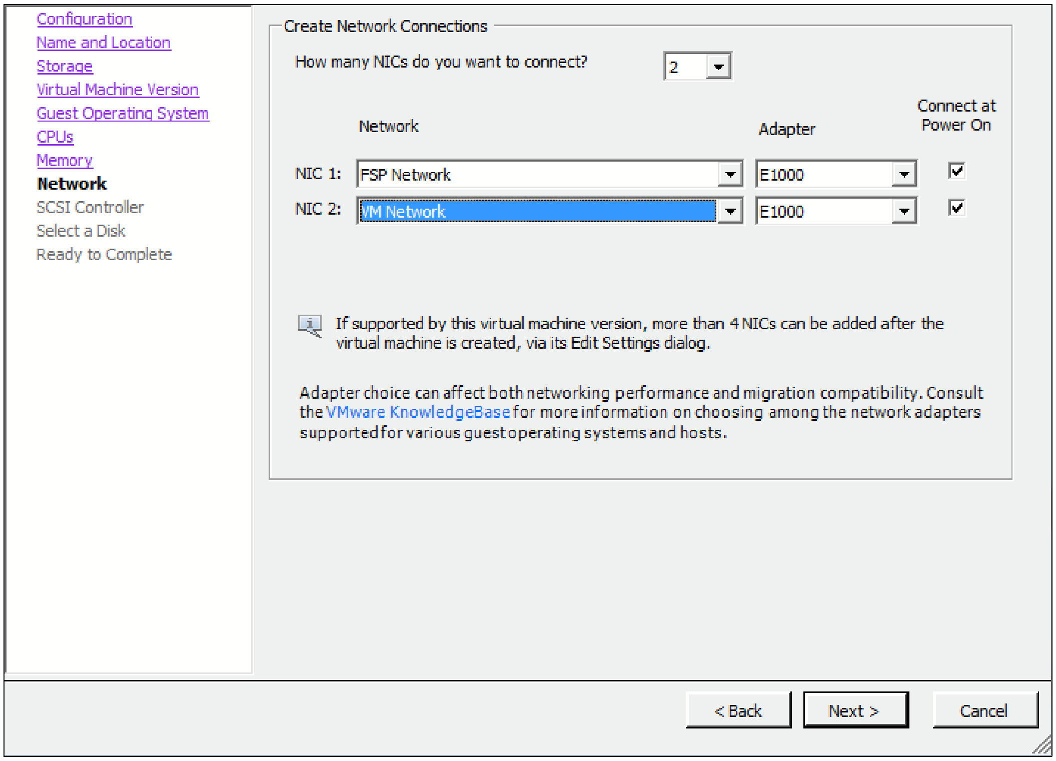
Default recommended for this guest OS: 384 MB.

Minimum recommended for this guest OS: 32 MB.

Linux values can vary. Consult your Linux release notes for accurate information.

Figure 3-10 Memory panel

9. In the Network panel (Figure 3-11), choose the number of virtual adapters and assign each of them to the network switch to match your configuration, depending on whether you plan to have an service processor network or not. Click **Next**.



Create Network Connections

How many NICs do you want to connect? 2

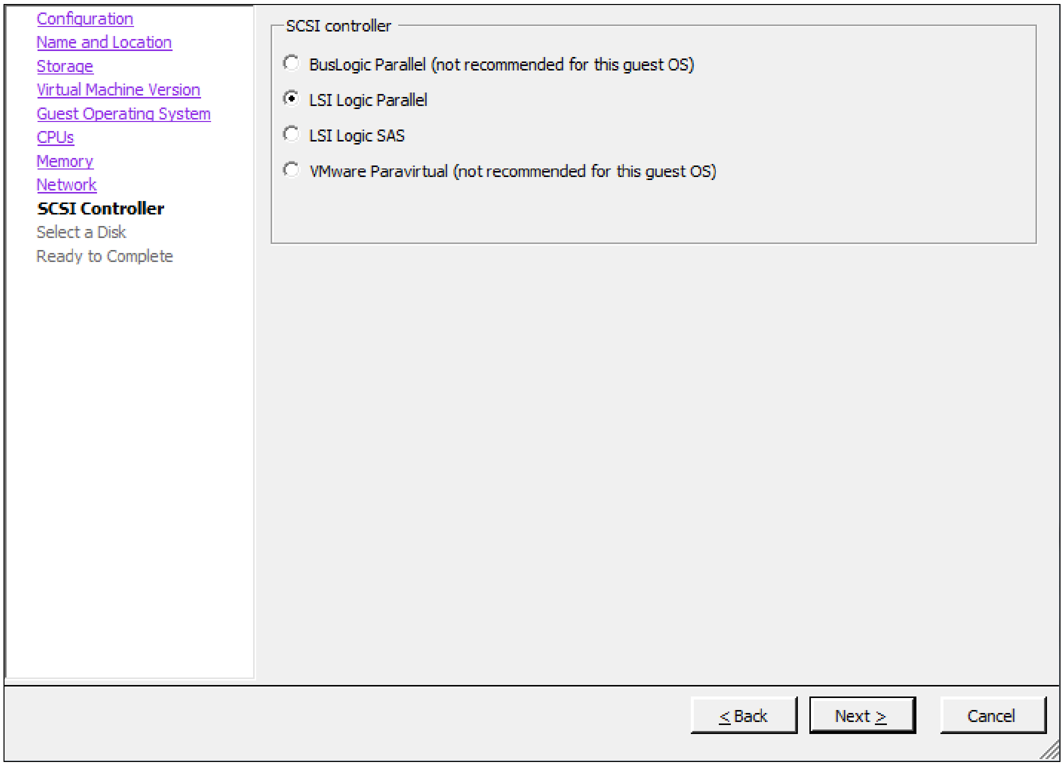
	Network	Adapter	Connect at Power On
NIC 1:	FSP Network	E1000	☑
NIC 2:	VM Network	E1000	☑

If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog.

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

Figure 3-11 Network selection panel

10. In the SCSI Controller panel (Figure 3-12), select the appropriate controller for your VM, and click **Next**.



SCSI controller

○ BusLogic Parallel (not recommended for this guest OS)

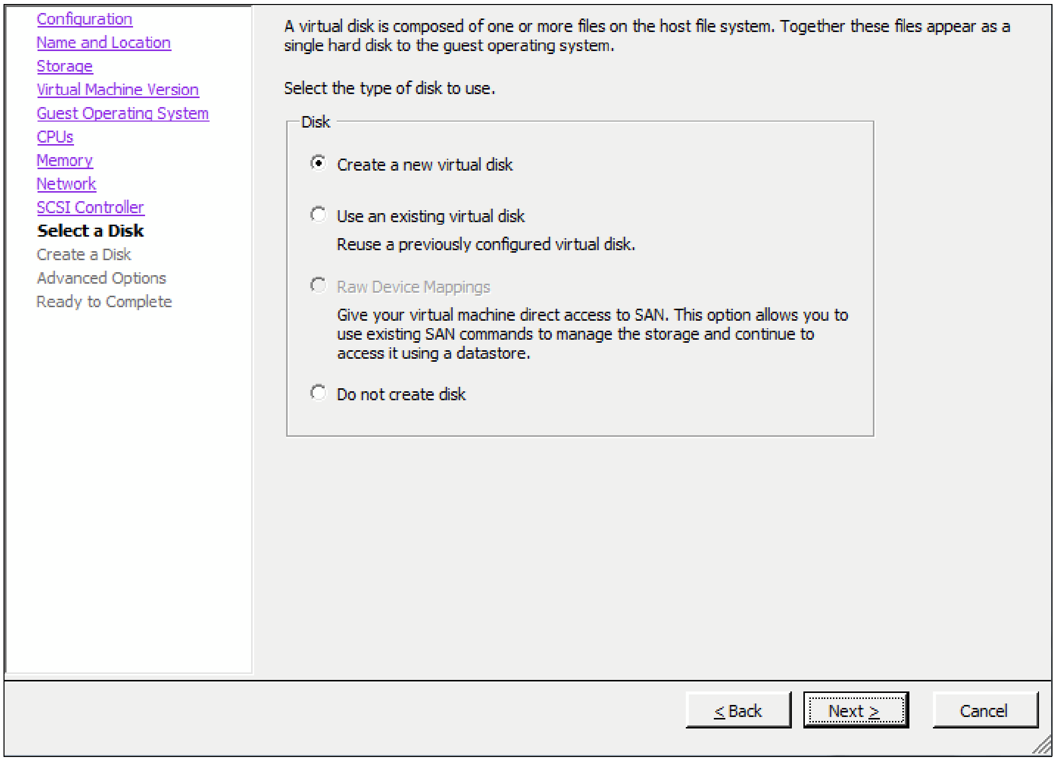
● LSI Logic Parallel

○ LSI Logic SAS

○ VMware Paravirtual (not recommended for this guest OS)

Figure 3-12 SCSI Controller panel

11.In the Select a Disk panel (Figure 3-13), select **Create a new virtual disk** and click **Next**.



A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

● Create a new virtual disk

○ Use an existing virtual disk

Reuse a previously configured virtual disk.

○ Raw Device Mappings

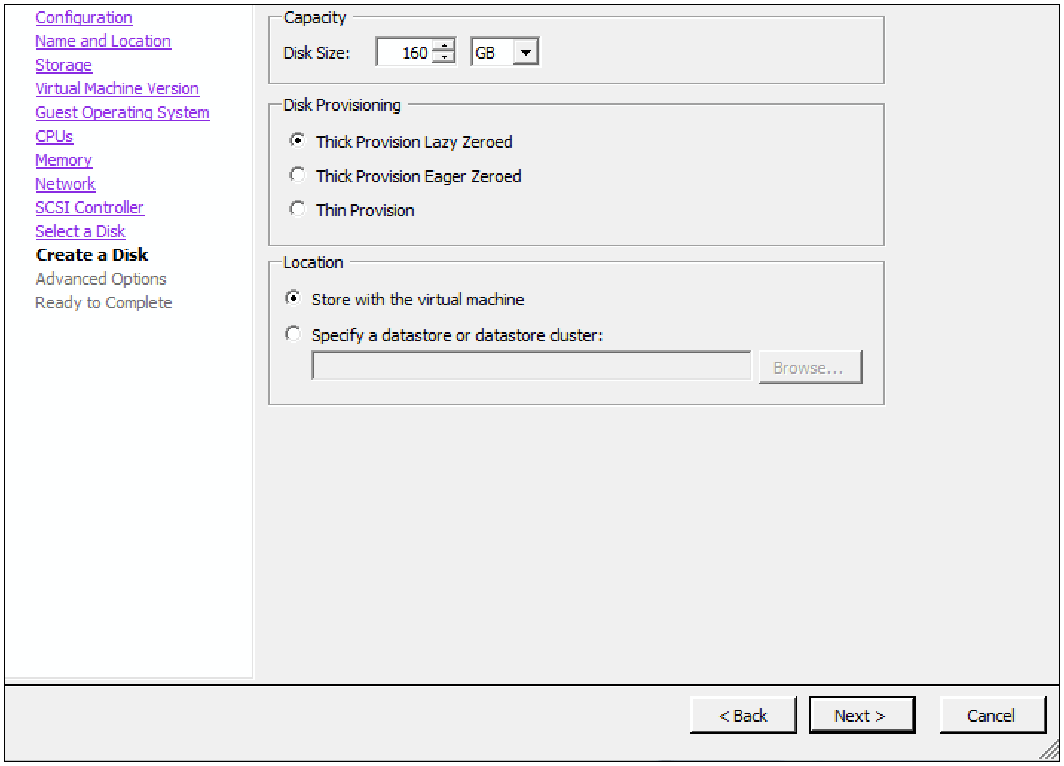
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

○ Do not create disk

Figure 3-13 Disk creation panel

12. In the Create a Disk panel (Figure 3-14), choose your disk size, and click **Next**.

    A minimum of 120 GB is required. Nevertheless, if you plan to use the performance capacity monitoring you might need to have the disk size approximately 700 GB. The disk must have the proper size before installation. It cannot be resized after the installation.



Capacity

Disk Size: 160 GB

Disk Provisioning

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

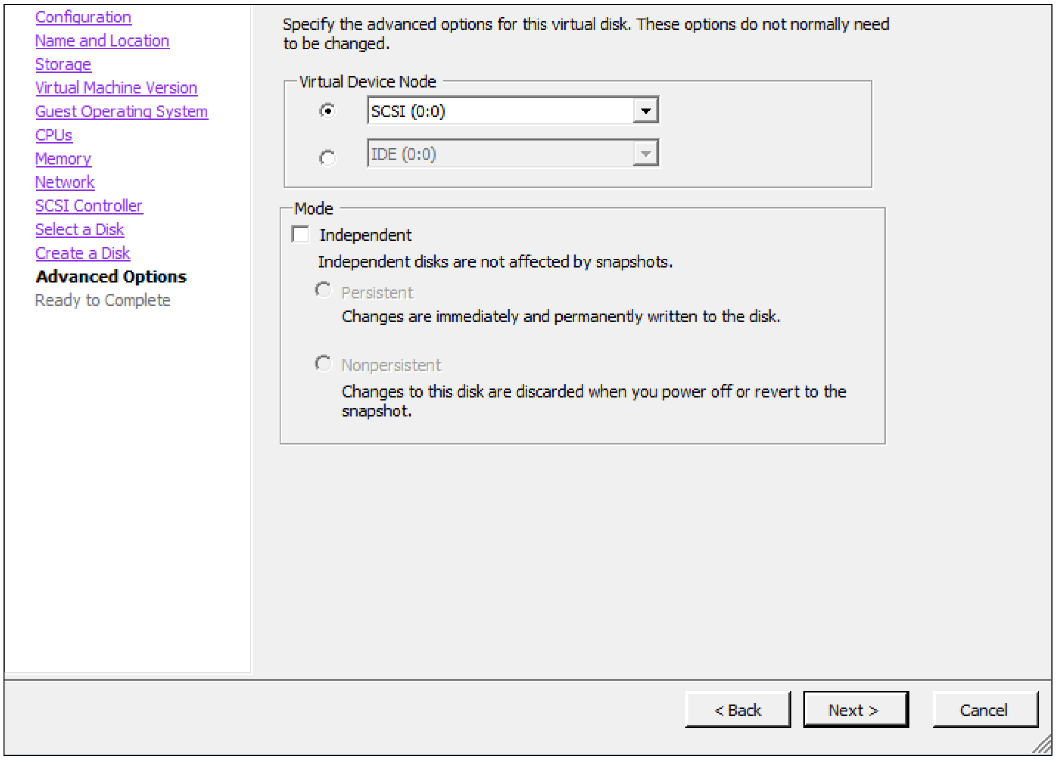
Location

● Store with the virtual machine

○ Specify a datastore or datastore cluster:

Figure 3-14 Choice of disk type and size

13. In the Advanced Options panel (Figure 3-15), click **Next** to proceed.



Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node

● SCSI (0:0)

○ IDE (0:0)

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

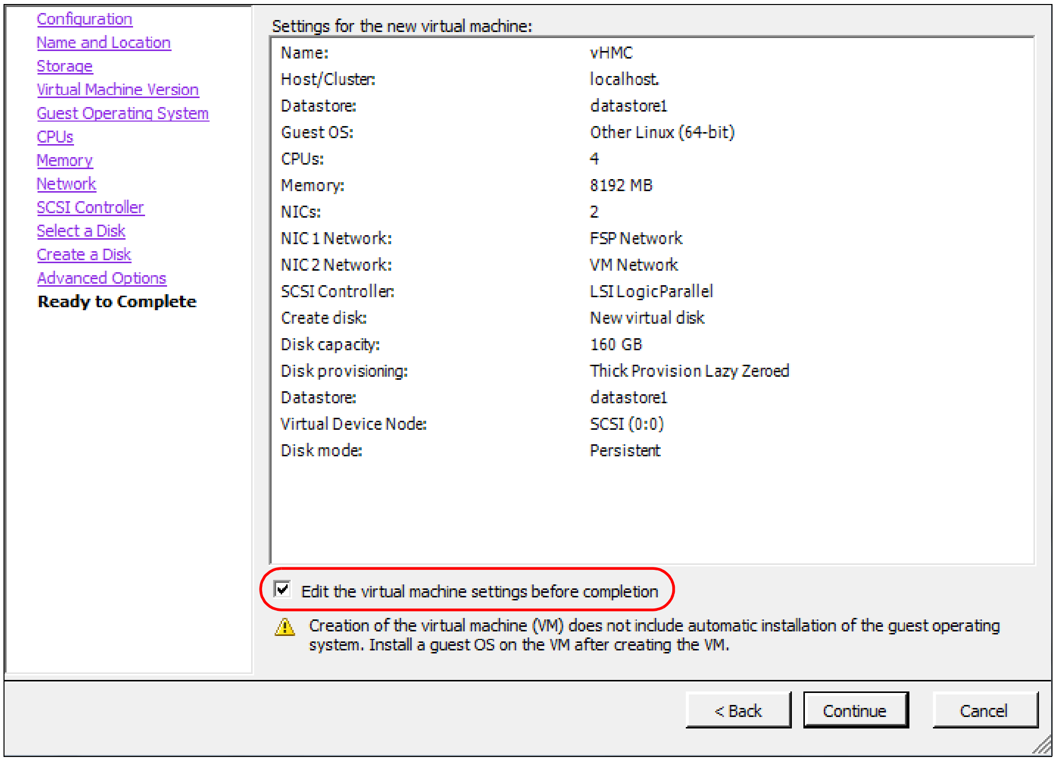
Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

Figure 3-15 Advanced Options panel

14. The Ready to Complete panel (Figure 3-16) lists the VM settings. You must edit the VM settings in order to connect an ISO image to boot from, then click **Continue** to create the vHMC VM.



Settings for the new virtual machine:

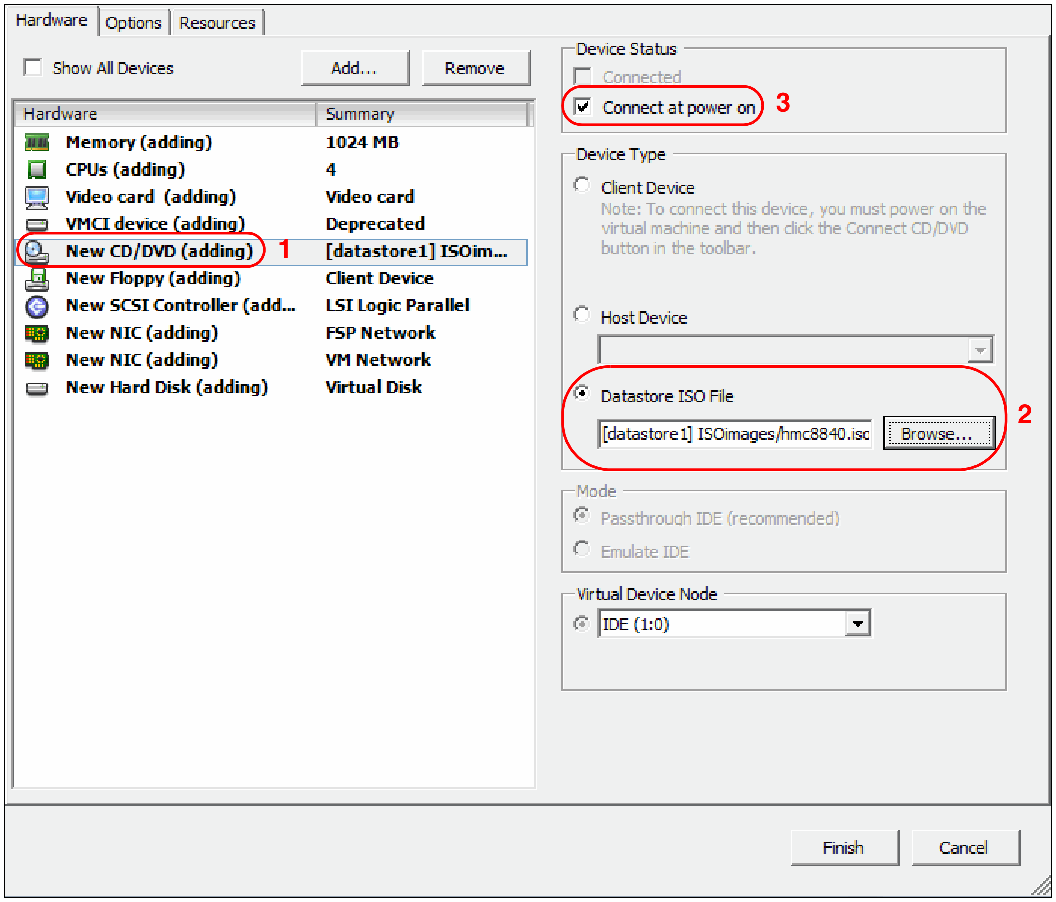
Name:	vHMC
Host/Cluster:	localhost.
Datastore:	datastore1
Guest OS:	Other Linux (64-bit)
CPUs:	4
Memory:	8192 MB
NICs:	2
NIC 1 Network:	FSP Network
NIC 2 Network:	VM Network
SCSI Controller:	LSI LogicParallel
Create disk:	New virtual disk
Disk capacity:	160 GB
Disk provisioning:	Thick Provision Lazy Zeroed
Datastore:	datastore1
Virtual Device Node:	SCSI (0:0)
Disk mode:	Persistent

☑ Edit the virtual machine settings before completion

⚠ Creation of the virtual machine (VM) does not include automatic installation of the guest operating system. Install a guest OS on the VM after creating the VM.

Figure 3-16 Ready to complete the VM

15. In the Virtual Machine Properties panel (Figure 3-17), select the **New CD/DVD** option in the left pane, and select the **Connect at power on** check box. Then, select the **Datastore ISO file** button and browse your directories to locate the HMC ISO image, which was previously uploaded on the VMware server. Click **Finish** to proceed.



□ Show All Devices

Hardware	Summary
Memory (adding)	1024 MB
CPUs (adding)	4
Video card (adding)	Video card
VMCI device (adding)	Deprecated
New CD/DVD (adding)	[datastore1] ISOim...
New Floppy (adding)	Client Device
New SCSI Controller (add...	LSI Logic Parallel
New NIC (adding)	FSP Network
New NIC (adding)	VM Network
New Hard Disk (adding)	Virtual Disk

Device Status

□ Connected

☑ Connect at power on

Device Type

○ Client Device

Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar.

○ Host Device

● Datastore ISO File

[datastore1] ISOimages/hmc8840.isc

Mode

● Passthrough IDE (recommended)

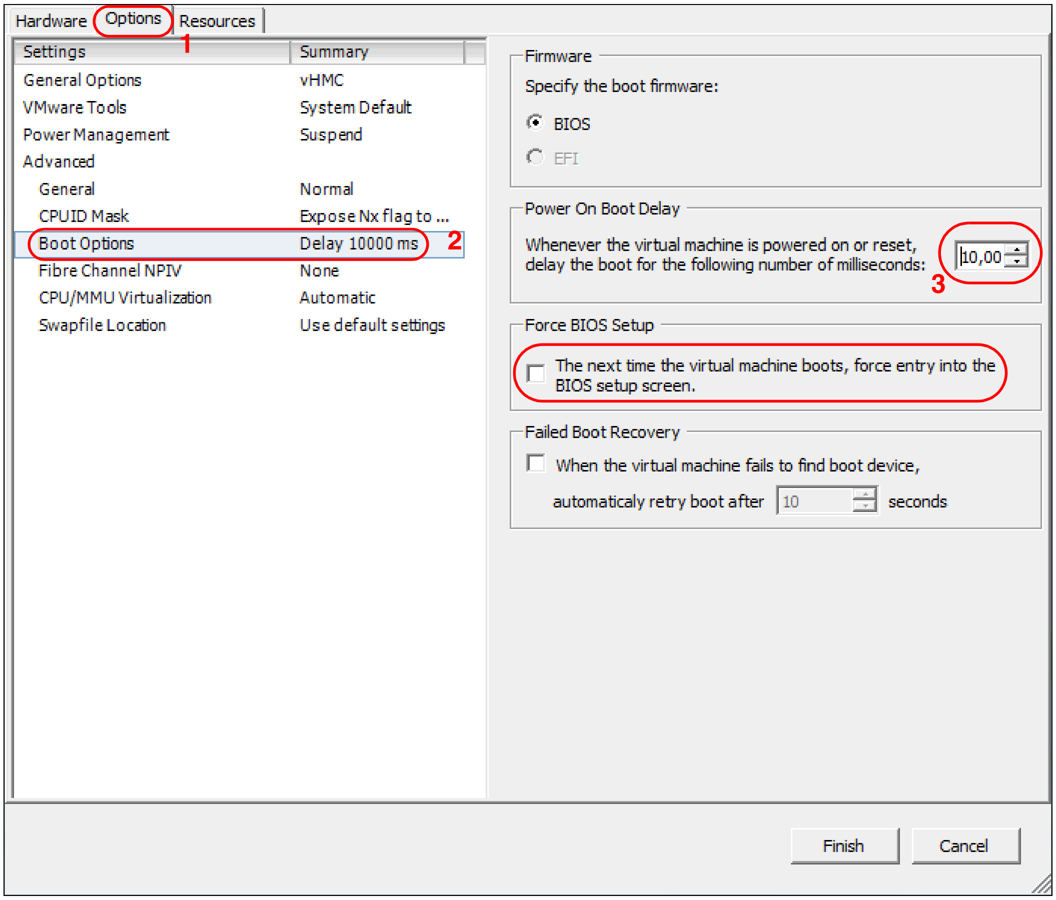
○ Emulate IDE

Virtual Device Node

● IDE (1:0)

Figure 3-17 Choose an ISO image file

16. You may also add delays during the boot phase of the VM, in order to be sure you boot from the virtual DVD drive. To do this, select the **Options** tab (Figure 3-18), and change the Power On Boot Delay value. Click **Finish** to create the VM. You also have an option in the same panel to force the VM to enter the BIOS on the next boot, and change the boot list order.



Settings	Summary
General Options	vHMC
VMware Tools	System Default
Power Management	Suspend
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Boot Options	Delay 10000 ms
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Firmware

Specify the boot firmware:

● BIOS

○ EFI

Power On Boot Delay

Whenever the virtual machine is powered on or reset, delay the boot for the following number of milliseconds: 10,00

Force BIOS Setup

□ The next time the virtual machine boots, force entry into the BIOS setup screen.

Failed Boot Recovery

□ When the virtual machine fails to find boot device,

automaticaly retry boot after 10 seconds

Figure 3-18 Add a boot delay

17. After the VM is created, you can start and boot from the ISO image file. You can open a console, as shown in Figure 3-19.

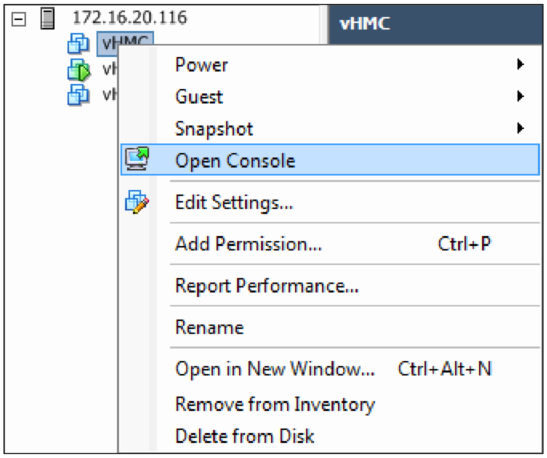


Figure 3-19 Open the VM's console

18. When the console is open (Figure 3-20), click **Power On** icon (green triangle), and click in the console display to interact with the VM. The HMC Install Wizard is now available.

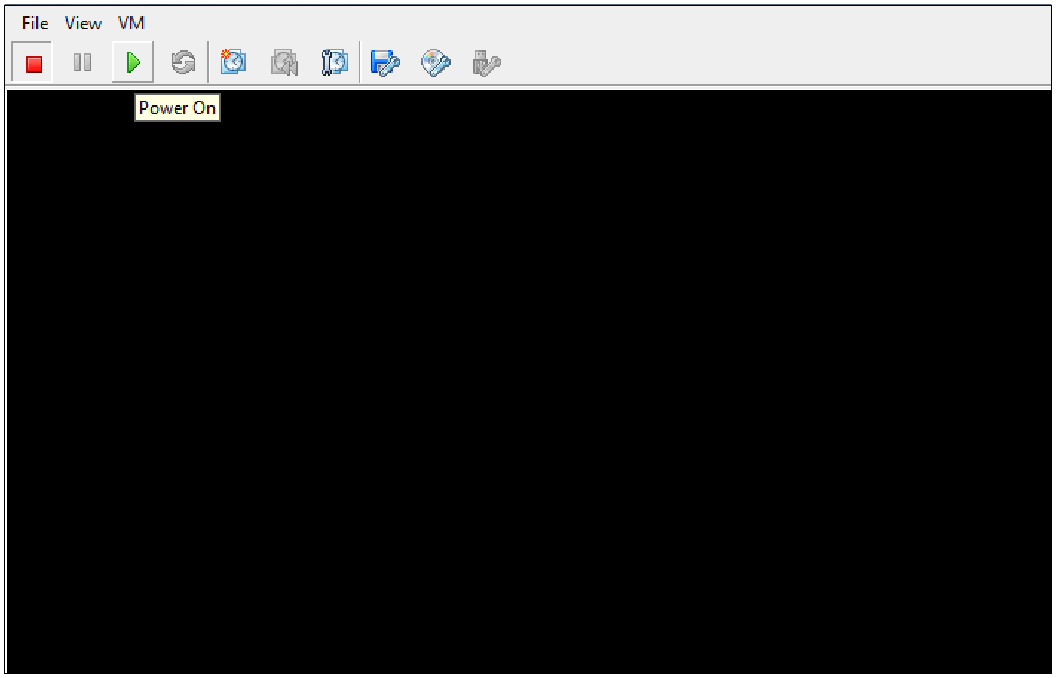
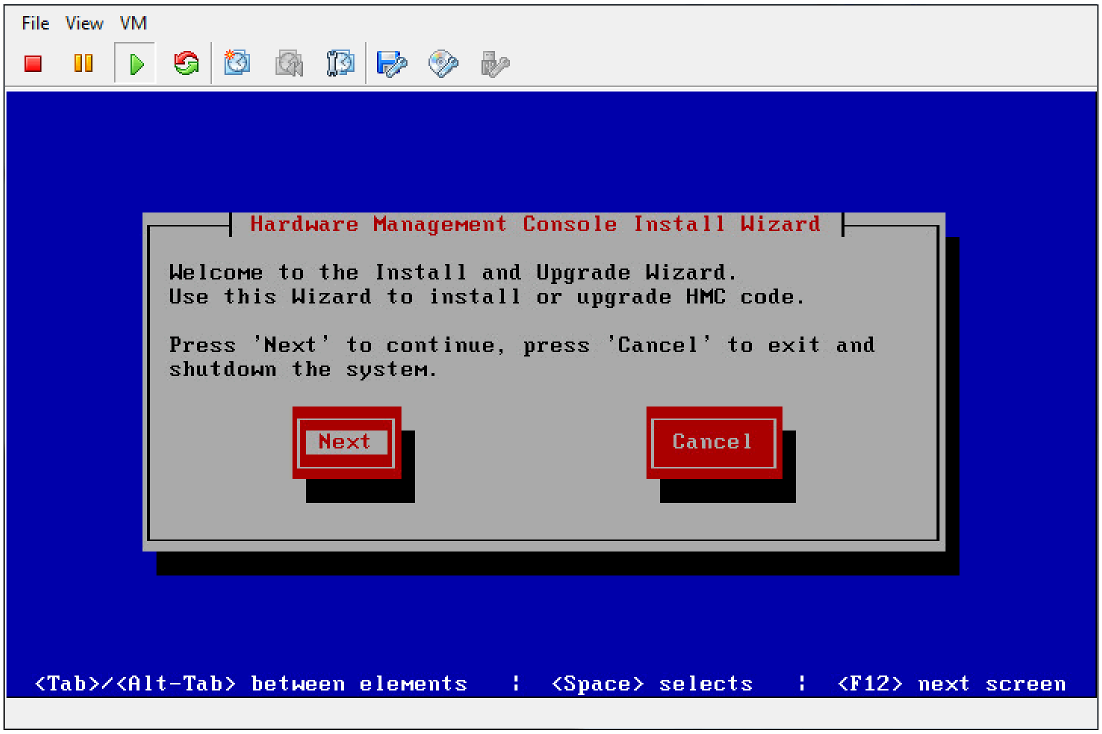


Figure 3-20 Power On the VMware VM

After it is booted, the VM console displays the HMC Install Wizard (Figure 3-21).



```
Hardware Management Console Install Wizard

Welcome to the Install and Upgrade Wizard.
Use this Wizard to install or upgrade HMC code.

Press 'Next' to continue, press 'Cancel' to exit and
shutdown the system.

        Next                    Cancel

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Figure 3-21 HMC Install Wizard

The ISO installation method is exactly the same as for KVM, or bare metal HMC. See 3.3, “HMC Install Wizard” on page 223, and proceed with the HMC installation and configuration.

> **Important:** The installation of the VMware tools for Linux is not supported on the virtual HMC.

3.1.3 KVM installation

The steps to install an HMC ISO image on KVM are described next. The steps use the command line and the *virt-manager* graphic tool. You may use different steps only from the command line.

On the KVM server, use the following command to create a directory, and upload the ISO image there:

```
mkdir -p /var/lib/libvirt/images/ISO
```

Example of a KVM bridge configuration

Before starting the virtual HMC installation, the KVM must have network bridges configured.

A minimum of one NIC is required for your network. Nevertheless, on Power Server and HMC installations, it is common to have a NIC for the service processor network and a NIC for the open network.

In the next installation example, KVM runs on a Red Hat Enterprise Linux 7.1 (RHEL) server. This configuration example provides of a simple dual NIC KVM configuration. For the KVM deployment shown in this chapter, the physical server has two separate physical NICs connected:

- One NIC is dedicated to the service processor network.
- A second NIC is dedicated to the Open network.

To configure a simple dual bridged configuration, complete the following steps:

1. Check the current TCP/IP configuration. Example 3-1 shows the NICs and IP with the **`ip`** command before adding the Ethernet bridges. It shows that the open network used to the KVM server is `172.16.20.115` on the `enp26s0` interface. No IP address is specified on the second `enp27s0` interface. The `enp26s0` interface is used for the open network, and the `enp27s0` interface for the service processor network.

   Example 3-1   NICs IP status before configuring the bridges

   ```
   [root@kvm1 ~]# ip a
   1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
       link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
       inet 127.0.0.1/8 scope host lo
          valid_lft forever preferred_lft forever
       inet6 ::1/128 scope host
          valid_lft forever preferred_lft forever
   2: enp26s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
       link/ether 00:1a:64:a1:ef:ca brd ff:ff:ff:ff:ff:ff
       inet 172.16.20.115/22 brd 172.16.23.255 scope global enp26s0
          valid_lft forever preferred_lft forever
       inet6 fe80::21a:64ff:fea1:efca/64 scope link
          valid_lft forever preferred_lft forever
   3: enp27s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
       link/ether 00:1a:64:a1:ef:cb brd ff:ff:ff:ff:ff:ff
   ```

```
6: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 52:54:00:27:4d:8c brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
7: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN
qlen 500
    link/ether 52:54:00:27:4d:8c brd ff:ff:ff:ff:ff:ff
```

2. Use the **brctl** (KVM Ethernet bridge administration) command to show the status of the bridges (Example 3-2). Only the default KVM NAT interface is present.

Example 3-2 KVM bridges status

```
[root@kvm1 ~]# brctl show
bridge name     bridge id               STP enabled     interfaces
virbr0          8000.525400274d8c       yes             virbr0-nic
```

Before adding the network bridges to the KVM configuration the IP configuration for enp26s and enp27s is shown in Example 3-3.

Example 3-3 Ethernet interfaces network definitions

```
[root@kvm1 ~]# cat /etc/sysconfig/network-scripts/ifcfg-enp26s0
TYPE="Ethernet"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
NAME="enp26s0"
UUID="933ea7dc-b58d-43b3-b22c-6687529044f3"
DEVICE="enp26s0"
ONBOOT="yes"
IPADDR="172.16.20.115"
PREFIX="22"
GATEWAY="172.16.20.1"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
IPV6_PRIVACY="no"

[root@kvm1 ~]# cat /etc/sysconfig/network-scripts/ifcfg-enp27s0
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=enp27s0
UUID=3327d1c8-1517-4e25-b84d-f7b540bd07e1
DEVICE=enp27s0
ONBOOT=no
```

Use the following steps to create the network bridges and reconfigure the default TCP/IP connection:

1. Use the **brctl addb** command to create the network bridges (Example 3-4). You can then add the physical NIC interfaces to the bridges, with the **brctl addif** commands Finally, the **brctl show** command shows the status of the bridges and their corresponding interfaces.

   Example 3-4 Add network

   ```
   [root@kvm1 ~]# brctl addbr br0
   [root@kvm1 ~]# brctl addbr br1
   [root@kvm1 ~]# brctl addif br0 enp26s0
   [root@kvm1 ~]# brctl addif br1 enp27s0
   [root@kvm1 ~]# brctl show
   bridge name     bridge id               STP enabled     interfaces
   br0             8000.001a64a1efca       no              enp26s0
   br1             8000.001a64a1efcb       no              enp27s0
   virbr0          8000.525400274d8c       yes             virbr0-nic
   ```

   Important: If you need to create a bridge over your default interface, you must do it from the server’s console, otherwise it breaks the connection.

2. After the bridges are created, change the interface configuration files in the `/etc/sysconfig/network-scripts` directory for the `enp26s0` interface by adding the `BRIDGE` definition, as shown in Example 3-5.

   Example 3-5 /etc/sysconfig/network-scripts/ifcfg-enp26s0 file

   ```
   TYPE=Ethernet
   NM_CONTROLLED=no
   BOOTPROTO=none
   IPV4_FAILURE_FATAL=no
   IPV6INIT=no
   NAME=enp26s0
   UUID=933ea7dc-b58d-43b3-b22c-6687529044f3
   DEVICE=enp26s0
   ONBOOT=yes
   BRIDGE=br0
   ```

3. Create a `br0` interface (Example 3-6). You might notice that the default TCP/IP address `172.16.20.115` and default gateway information are now moved to the `br0` interface.

   Example 3-6 /etc/sysconfig/network-scripts/ifcfg-br0 file

   ```
   DEVICE=br0
   BOOTPROTO=none
   IPV6INIT=no
   ONBOOT=yes
   TYPE=Bridge
   NM_CONTROLLED=no
   DEFROUTE=yes
   DEVICE=br0
   ONBOOT=yes
   IPADDR=172.16.20.115
   PREFIX=22
   GATEWAY=172.16.20.1
   ```

4. Also change the interface configuration files in the `/etc/sysconfig/network-scripts` directory for the `enp27s0` interface adding the `BRIDGE` definition, as shown in Example 3-7.

Example 3-7 /etc/sysconfig/network-scripts/ifcfg-enp27s0

```
TYPE=Ethernet
NM_CONTROLLED=no
BOOTPROTO=none
IPV4_FAILURE_FATAL=no
IPV6INIT=no
NAME=enp27s0
UUID=3327d1c8-1517-4e25-b84d-f7b540bd07e1
DEVICE=enp27s0
ONBOOT=yes
BRIDGE=br1
```

5. Create a `br1` interface, as shown in Example 3-8. You do not have to set a TCP/IP address on this interface, because it will be used as a DHCP network for the service processors.

Example 3-8 /etc/sysconfig/network-scripts/ifcfg-br1 file

```
DEVICE=br1
BOOTPROTO=none
IPV6INIT=no
ONBOOT=yes
TYPE=Bridge
NM_CONTROLLED=no
```

6. After you modify the interface definitions, reboot the server to be sure the configuration is properly working. The configuration is now similar to Example 3-9.

Example 3-9 TCP/IP configuration example

```
[root@kvm1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp26s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master br0 state UP qlen
1000
    link/ether 00:1a:64:a1:ef:ca brd ff:ff:ff:ff:ff:ff
    inet6 fe80::21a:64ff:fea1:efca/64 scope link
       valid_lft forever preferred_lft forever
3: enp27s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master br1 state UP qlen
1000
    link/ether 00:1a:64:a1:ef:cb brd ff:ff:ff:ff:ff:ff
    inet6 fe80::21a:64ff:fea1:efcb/64 scope link
       valid_lft forever preferred_lft forever
4: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:1a:64:a1:ef:ca brd ff:ff:ff:ff:ff:ff
    inet 172.16.20.115/22 brd 172.16.23.255 scope global br0
       valid_lft forever preferred_lft forever
    inet6 fe80::21a:64ff:fea1:efca/64 scope link
       valid_lft forever preferred_lft forever
5: br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:1a:64:a1:ef:cb brd ff:ff:ff:ff:ff:ff
    inet6 fe80::21a:64ff:fea1:efcb/64 scope link
       valid_lft forever preferred_lft forever
```

```
6: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 52:54:00:27:4d:8c brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
7: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN
qlen 500
    link/ether 52:54:00:27:4d:8c brd ff:ff:ff:ff:ff:ff
```

KVM ISO installation

After you make the simple KVM configuration, you can proceed with the HMC ISO file installation; use the following steps:

1. Create a storage pool directory and disk to host the VM using the commands in Example 3-10.

   Example 3-10 Create storage pool and disk in KVM

   ```
   [root@kvm1 ~]# mkdir -p /var/lib/libvirt/images/vHMC1
   cd /var/lib/libvirt/images/vHMC1
   [root@kvm1 vHMC1]# qemu-img create -f raw vHMC1.img 160G
   Formatting 'vHMC1.img', fmt=raw size=171798691840
   ```

2. You can now open the graphical Virtual Machine Manager to proceed with the VM configuration by using the **virt-manager** command. Click **File** → **New Virtual Machine** (Figure 3-22).

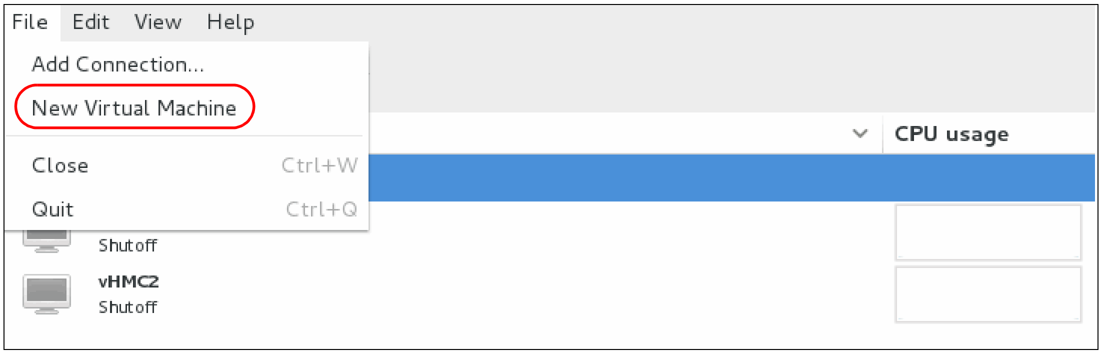
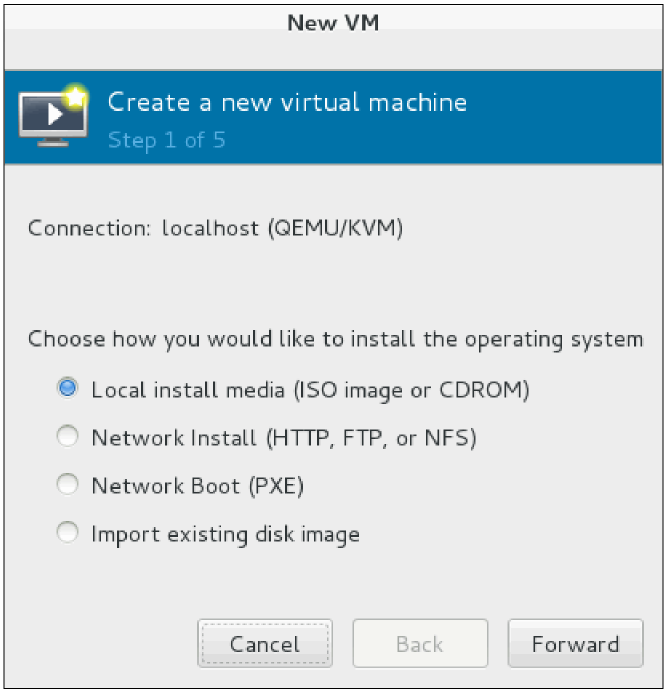


Figure 3-22 Virtual Machine Manager main panel

3. In the New VM panel (Figure 3-23), select **Local install media**, and then click **Forward**.



New VM

Create a new virtual machine
Step 1 of 5

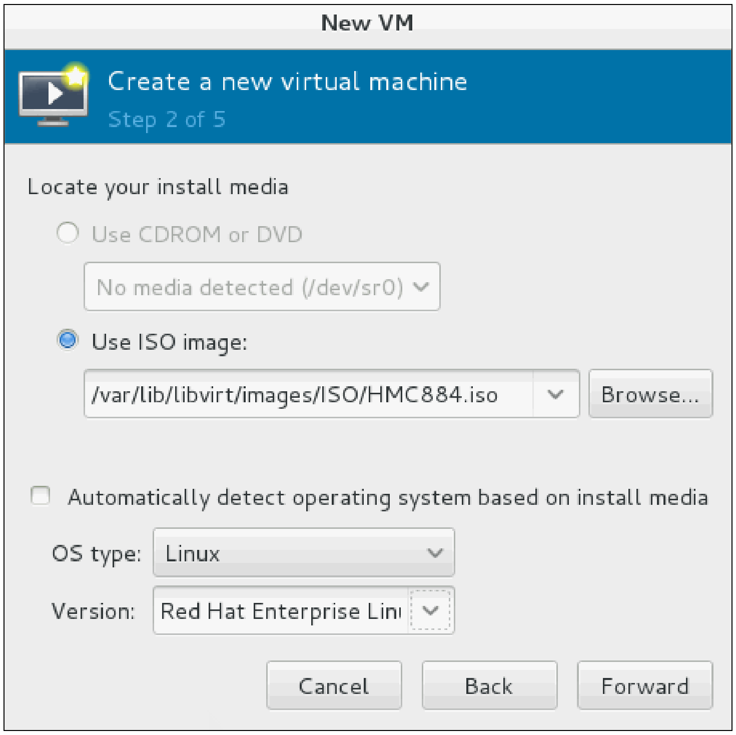
Connection: localhost (QEMU/KVM)

Choose how you would like to install the operating system

- ● Local install media (ISO image or CDROM)
- ○ Network Install (HTTP, FTP, or NFS)
- ○ Network Boot (PXE)
- ○ Import existing disk image

Figure 3-23 New VM panel

4. In the *Step 2 of 5* panel (Figure 3-24), click **Browse** to locate the ISO image previously uploaded in the ISO storage pool. Deselect the **Automatically detect the operating system** check box and then specify the Linux OS and RHEL 6.3 version. Click **Forward**.



New VM

Create a new virtual machine
Step 2 of 5

Locate your install media

○ Use CDROM or DVD

No media detected (/dev/sr0)

● Use ISO image:

/var/lib/libvirt/images/ISO/HMC884.iso

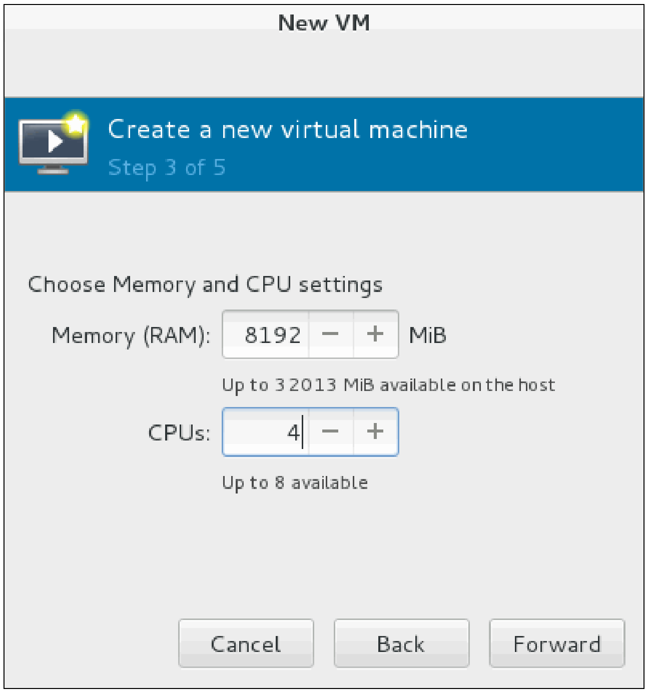
□ Automatically detect operating system based on install media

OS type: Linux

Version: Red Hat Enterprise Lin

Figure 3-24 Locate an ISO image

5. In the next panel (Figure 3-25), specify memory and CPU settings. This example specifies 8 GB of memory and 4 CPUs. Click **Forward** to proceed to the next step.



New VM

Create a new virtual machine

Step 3 of 5

Choose Memory and CPU settings

Memory (RAM): 8192 MiB

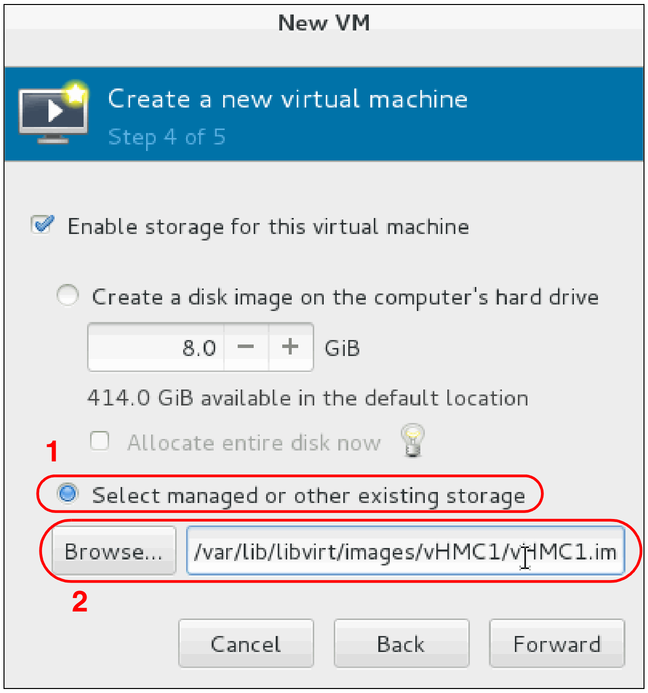
Up to 32013 MiB available on the host

CPUs: 4

Up to 8 available

Figure 3-25 Choose memory and CPU settings

6. In the next panel (Figure 3-26), choose **Select managed or other existing storage**, and click **Browse** to locate the `/var/lib/libvirt/images/vHMC1/vHMC1.img` file created in the initial step. Then, click **Forward**.



New VM

Create a new virtual machine

Step 4 of 5

☑ Enable storage for this virtual machine

○ Create a disk image on the computer's hard drive

8.0 GiB

414.0 GiB available in the default location

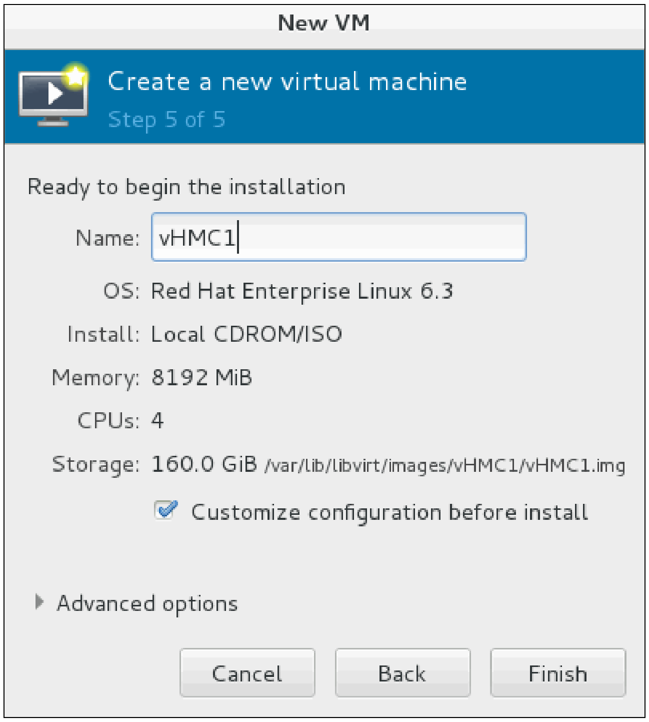
□ Allocate entire disk now

● Select managed or other existing storage

Browse... /var/lib/libvirt/images/vHMC1/vHMC1.im

Figure 3-26 Locate the disk image file in the storage pool

7. In the next panel (Figure 3-27), specify a name for the VM, select **Customize configuration before install**, and click **Finish.**



Ready to begin the installation

Name: vHMC1

OS: Red Hat Enterprise Linux 6.3

Install: Local CDROM/ISO

Memory: 8192 MiB

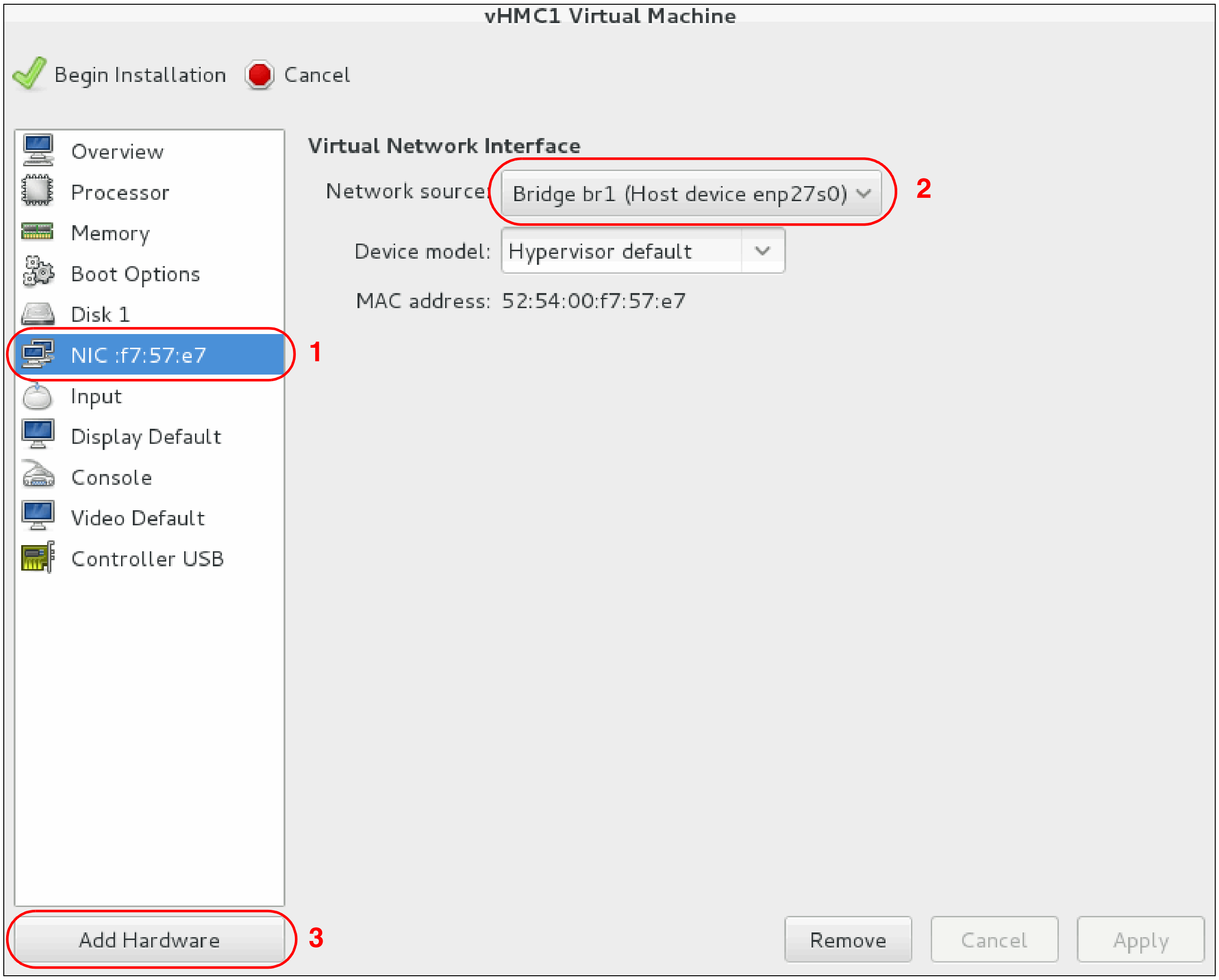
CPUs: 4

Storage: 160.0 GiB /var/lib/libvirt/images/vHMC1/vHMC1.img

☑ Customize configuration before install

Figure 3-27 Select name for the VM

8. In the VM customization panel (Figure 3-28), select the NIC in the left pane, and be sure it is assigned to the service processor network bridge (br1). Click **Add Hardware** to set up a second NIC.


vHMC1 Virtual Machine

Virtual Network Interface

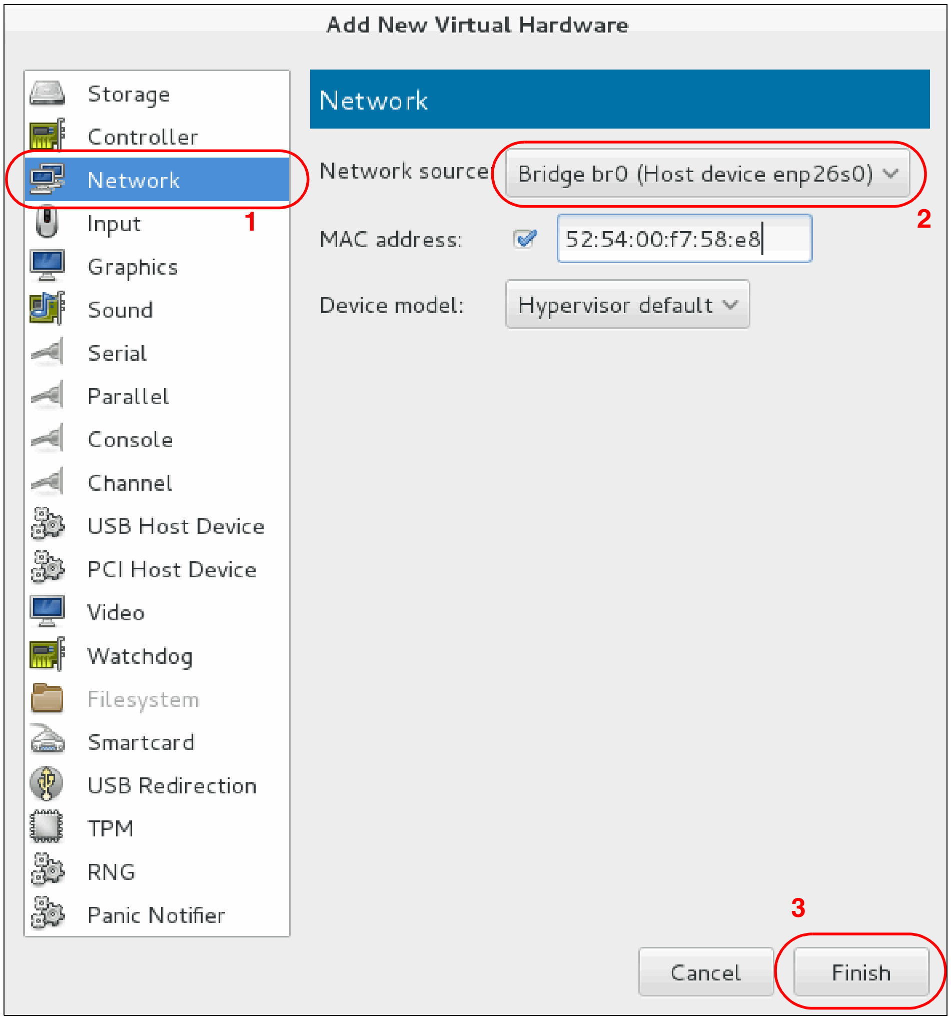
Network source: Bridge br1 (Host device enp27s0)

Device model: Hypervisor default

MAC address: 52:54:00:f7:57:e7

Figure 3-28 Check first NIC to be on bridge br1

9. Add a second NIC to the VM, as shown in Figure 3-29. Select **Network** in the left pane and select the open network bridge (br0). Click **Finish**.



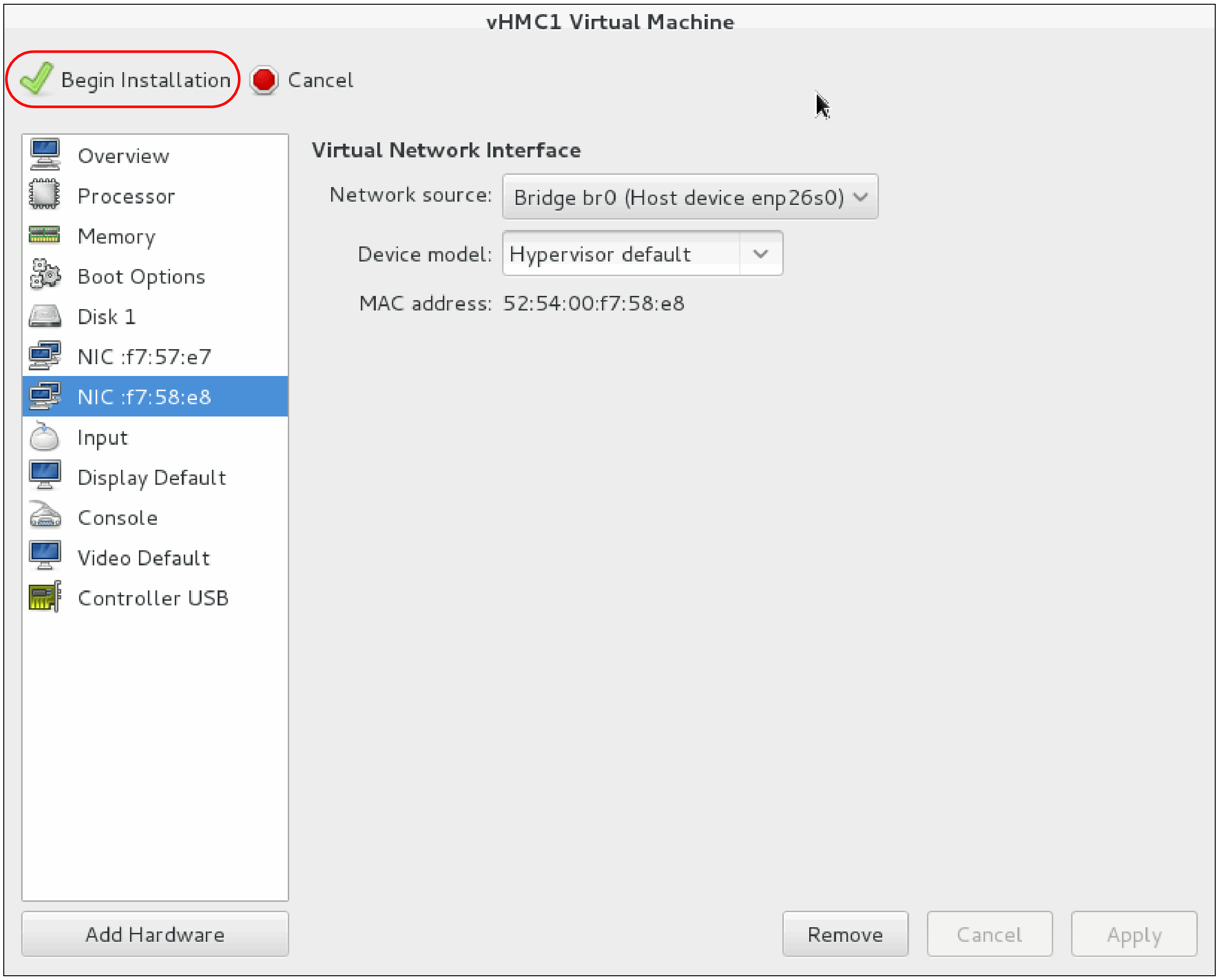
Network source: Bridge br0 (Host device enp26s0)

MAC address: ☑ 52:54:00:f7:58:e8

Device model: Hypervisor default

Figure 3-29 Add a second NIC

10. In the next panel you can now click **Begin Installation** (Figure 3-30).



vHMC1 Virtual Machine

Virtual Network Interface

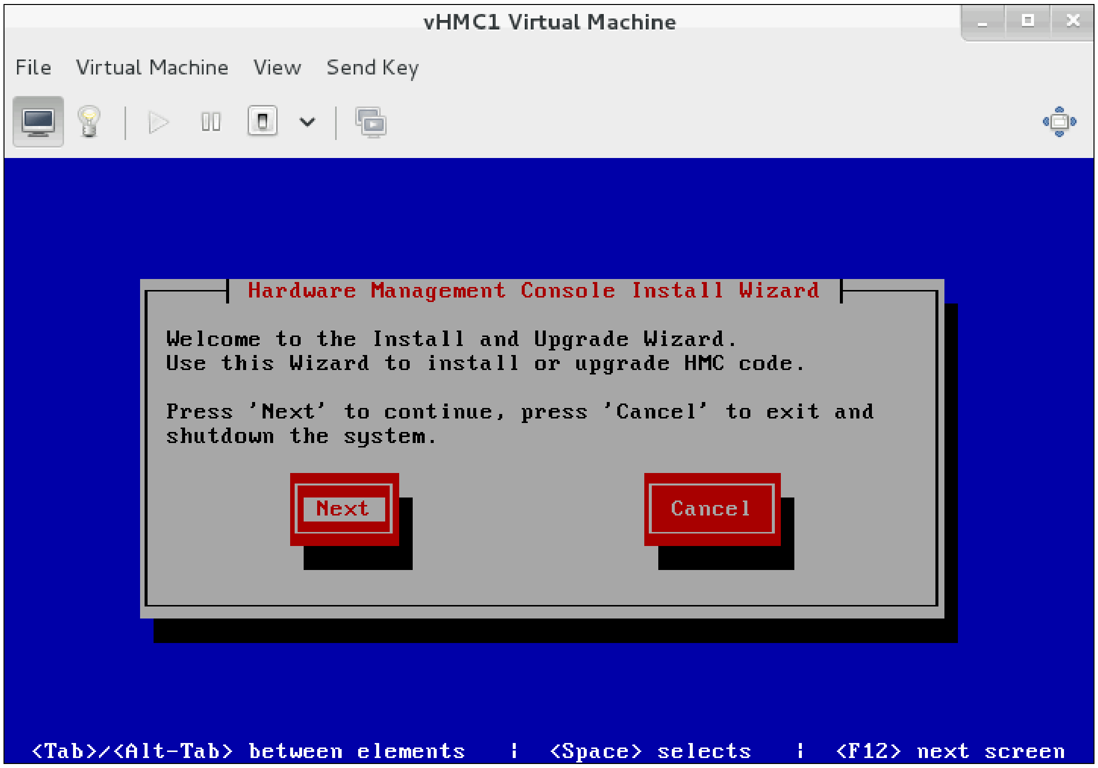
Network source: Bridge br0 (Host device enp26s0)

Device model: Hypervisor default

MAC address: 52:54:00:f7:58:e8

Figure 3-30 Begin Installation

After booting, the VM console shows the HMC Install Wizard (Figure 3-31).



```
Hardware Management Console Install Wizard

Welcome to the Install and Upgrade Wizard.
Use this Wizard to install or upgrade HMC code.

Press 'Next' to continue, press 'Cancel' to exit and
shutdown the system.

        Next                    Cancel

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Figure 3-31 HMC Install Wizard

11. The ISO installation method is exactly the same as for KVM, or bare metal HMC. See the 3.3, “HMC Install Wizard” on page 223 to continue with the HMC installation and customization.

3.2 Virtual appliances installations

This section covers the KVM and VMware virtual appliances installation.

3.2.1 VMware virtual appliance deployment

This section describes a simple vHMC appliance deployment on a VMware sever. You must have previously uploaded the `VMware_vHMC_installation_file_name.tgz` either on the workstation where you run the vSphere client or on an FTP server.

In this example, the `VMware_vHMC_installation_file_name.tgz` file was extracted on an AIX Linux server in the `/download/code/HMC8/HMC884/VMware` directory with the following command:

```
gunzip -c VMwareimage.tar.gz|tar -xvf -
```

The following steps describe an example of a simple vHMC deployment on VMware:

1. Verify that you are running with VMWARE ESXi 5.5 or later.
2. From the vSphere client user interface, deploy an Open Virtualization Format (OVF) template, as shown in Figure 3-32.

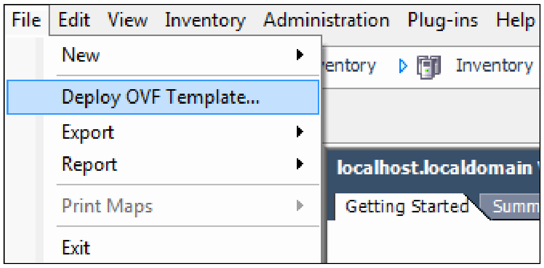
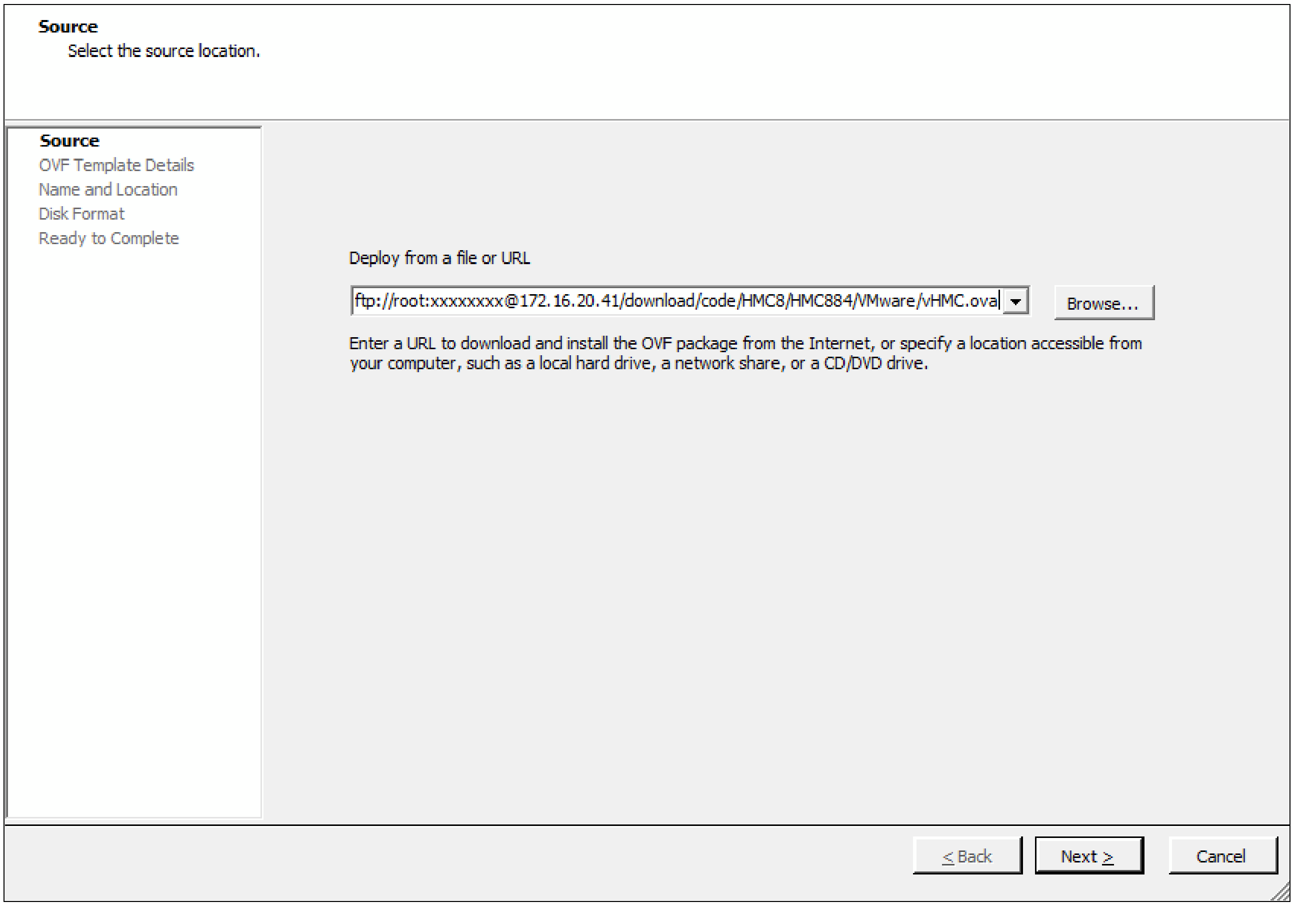


Figure 3-32 Deploy OVF template

3. You are prompted to browse to the OVA file location as shown in Figure 3-33. The default is to browse for an OVA file located on the workstation running the vSphere client. In this example, the deployment location uses a URL including the user and password:

   `ftp://root:xxxxxxxx@172.16.20.41/download/code/HMC8/HMC884/VMware/vHMC.ova`

   Where `xxxxxxxx` must be replaced with the actual password. Click **Next** to continue.



Source
Select the source location.

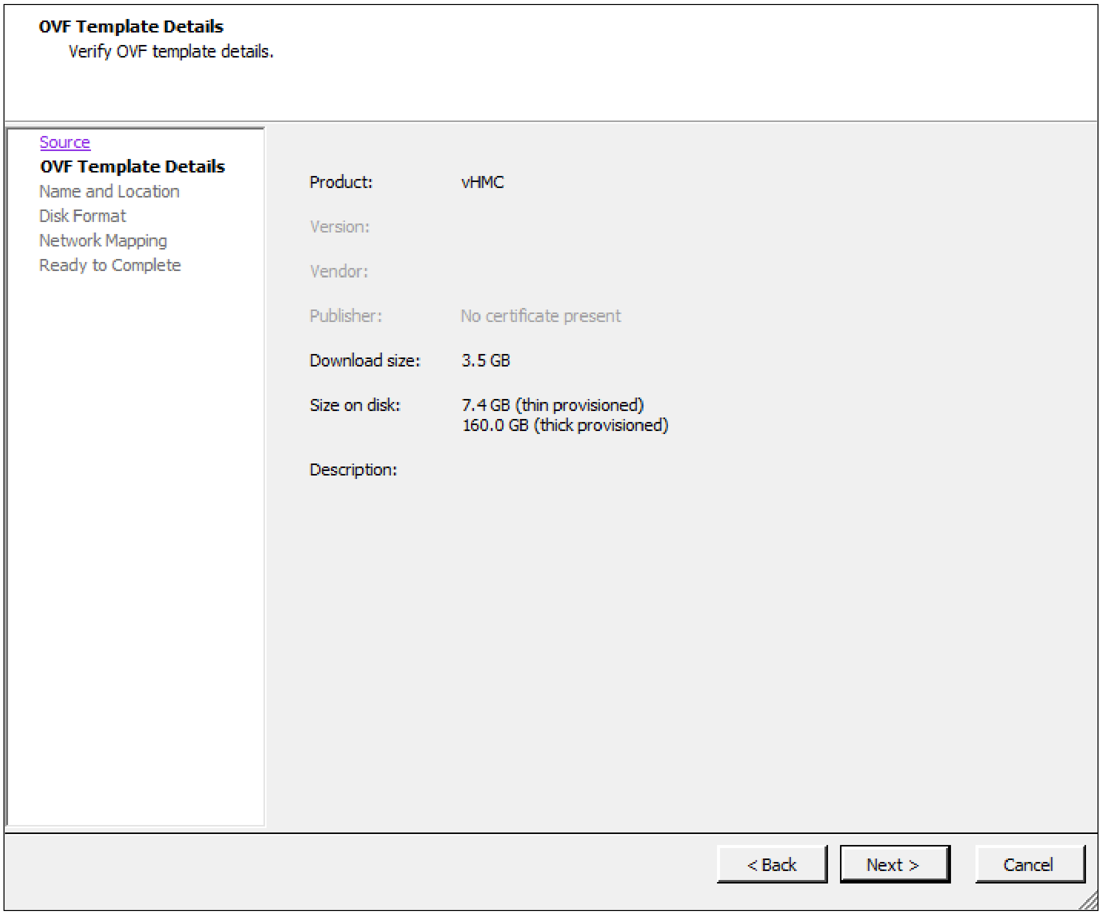
Deploy from a file or URL

ftp://root:xxxxxxxx@172.16.20.41/download/code/HMC8/HMC884/VMware/vHMC.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Figure 3-33 Deploy from a file or URL

4. On the OVF Details panel (Figure 3-34), click **Next**.



OVF Template Details
Verify OVF template details.

Product: vHMC

Version:

Vendor:

Publisher: No certificate present

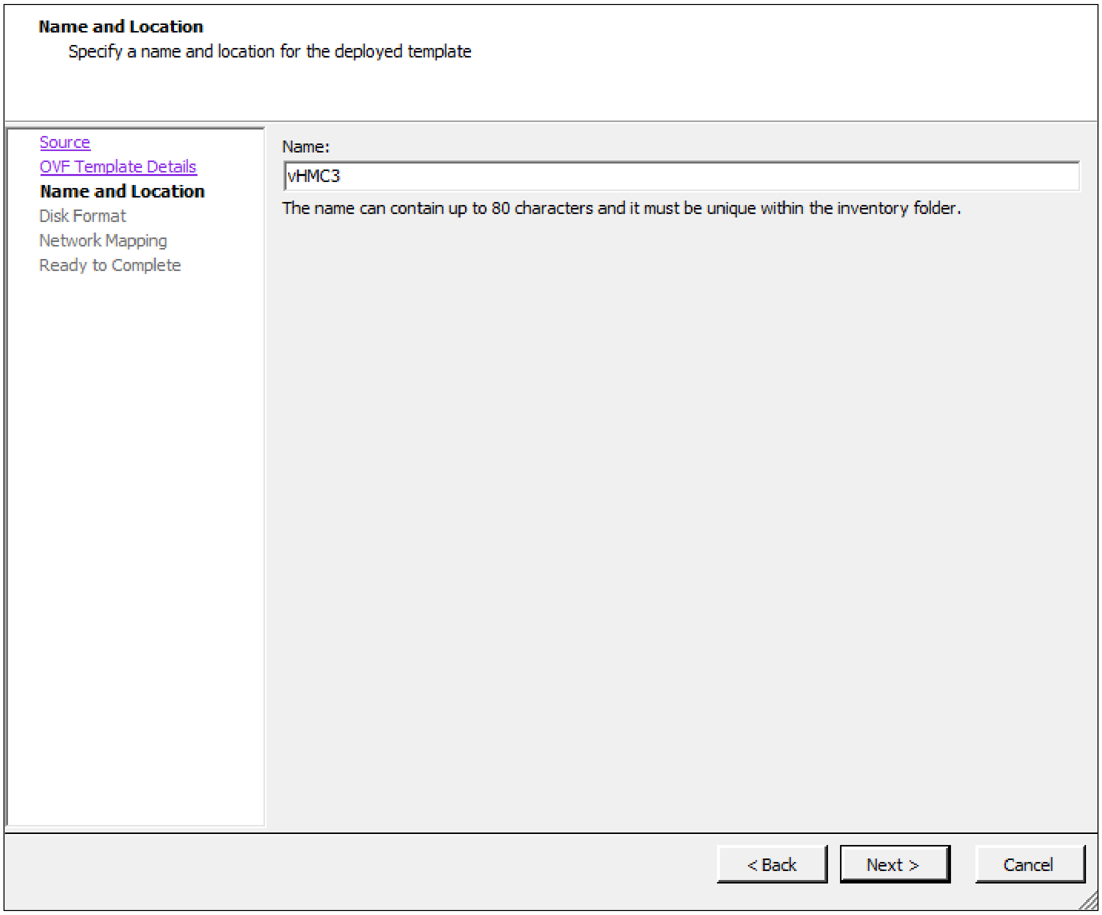
Download size: 3.5 GB

Size on disk: 7.4 GB (thin provisioned)
160.0 GB (thick provisioned)

Description:

Figure 3-34 OVF Template Details

5. In OVF Name and Location panel (Figure 3-35), enter a VM name, and click **Next**.



Name and Location

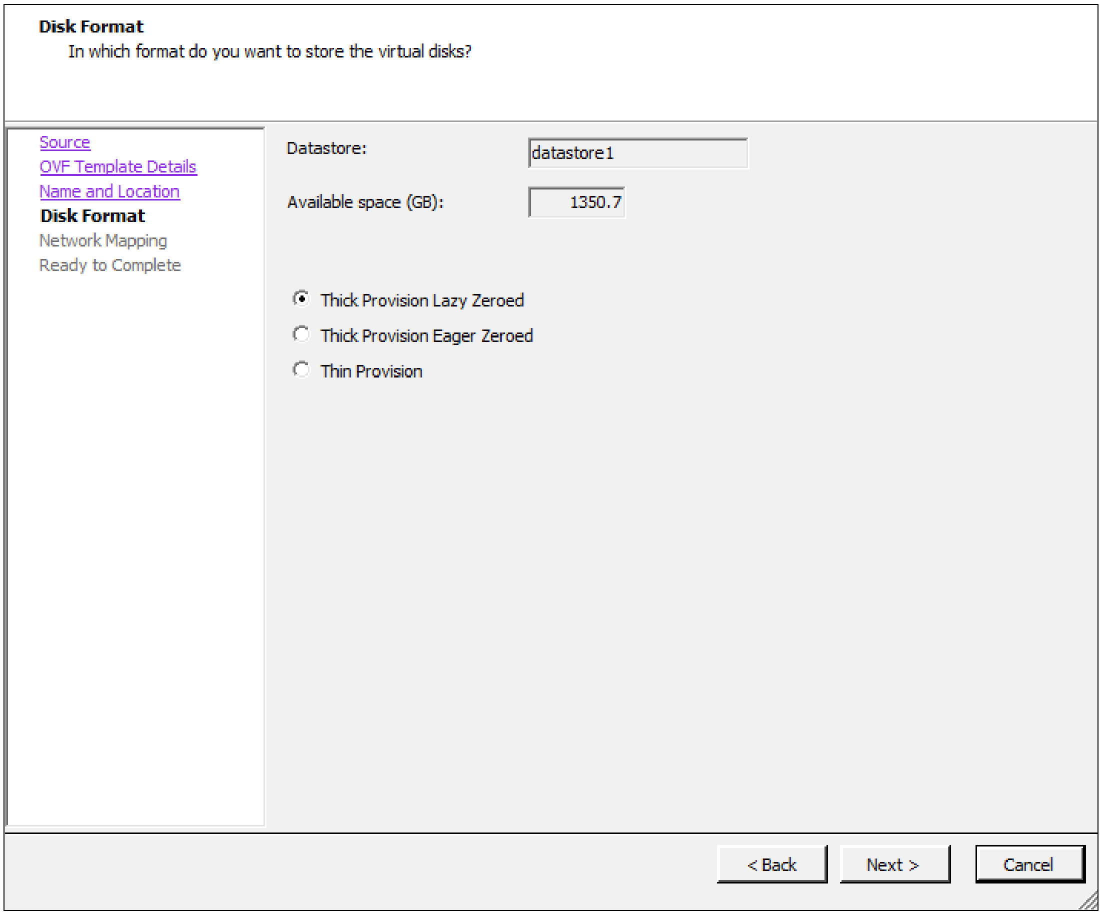
Specify a name and location for the deployed template

Name:
vHMC3

The name can contain up to 80 characters and it must be unique within the inventory folder.

Figure 3-35 Name and location for the vHMC

6. In the Disk Format panel (Figure 3-36), keep the default and click **Next**.



Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1

Available space (GB): 1350.7

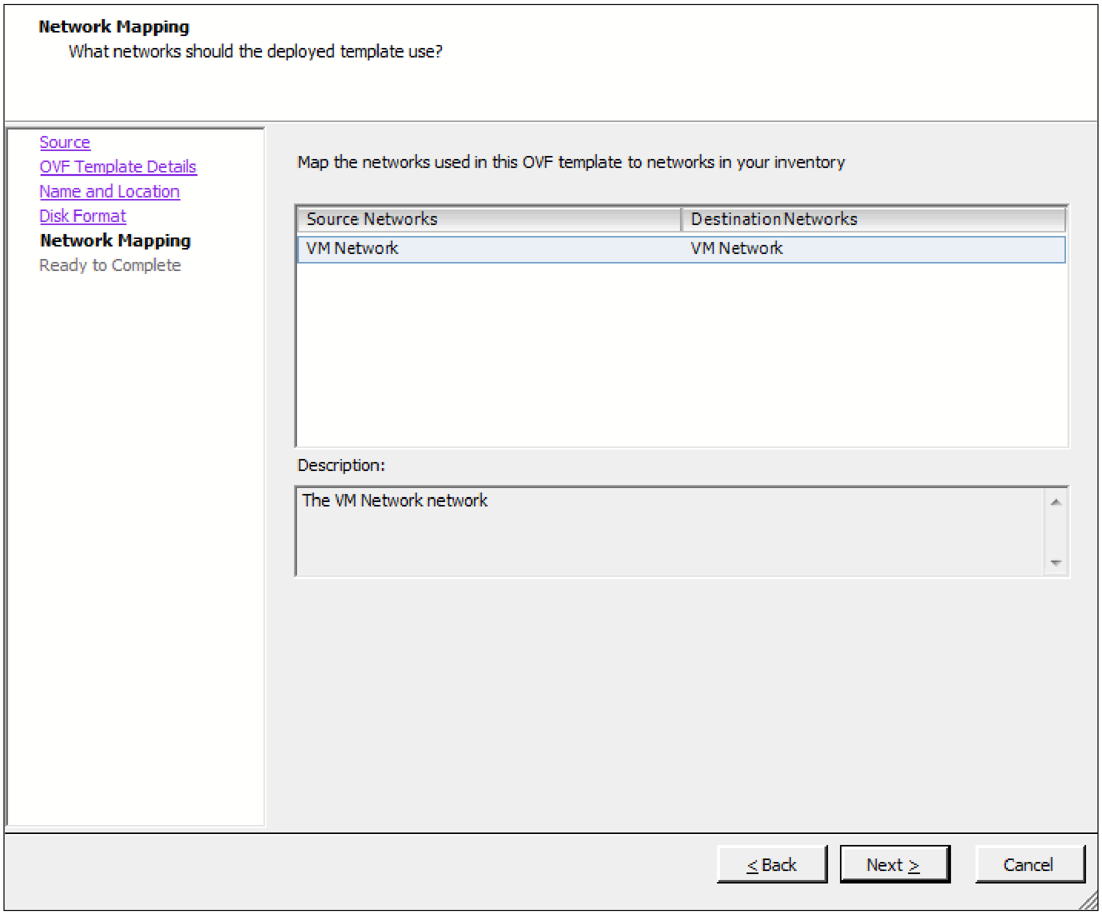
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

Figure 3-36 Disk Format panel

7. In the Network Mapping panel (Figure 3-37), click **Next**.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

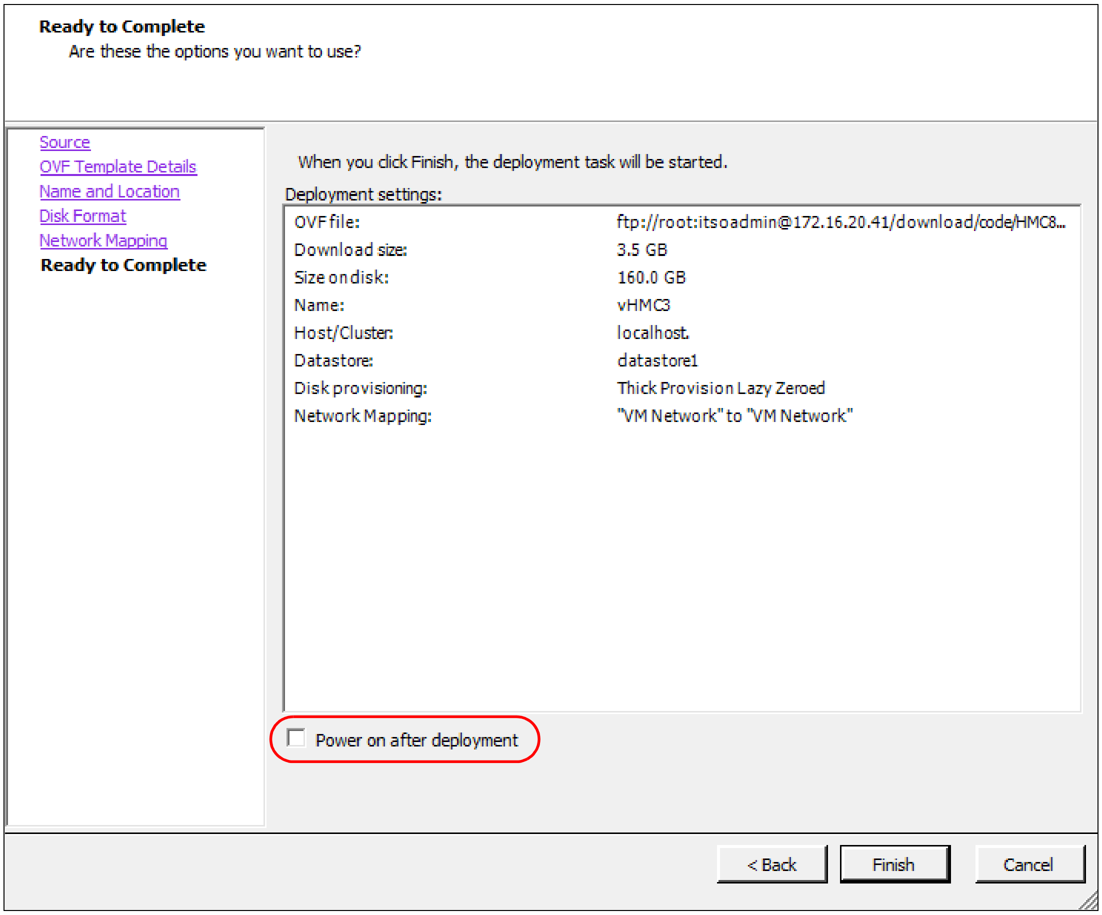
Source Networks	Destination Networks
VM Network	VM Network

Description:

The VM Network network

Figure 3-37 Network Mapping panel

8. In the Ready to Complete panel (Figure 3-38), to allow further configuration, *do not select* the Power on after deployment option. Click **Finish** to start downloading the OVA file onto the VMware to deploy the vHMC.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

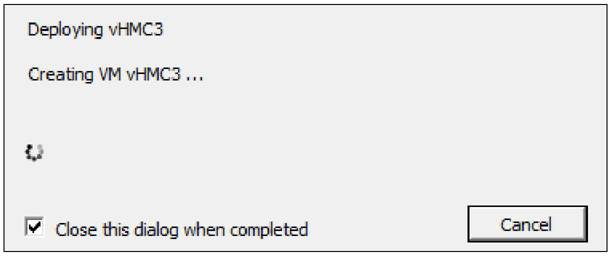
Deployment settings:

OVF file:	ftp://root:itsoadmin@172.16.20.41/download/code/HMC8...
Download size:	3.5 GB
Size on disk:	160.0 GB
Name:	vHMC3
Host/Cluster:	localhost.
Datastore:	datastore1
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"VM Network" to "VM Network"

☐ Power on after deployment

Figure 3-38 Ready to Complete panel

The deployment creates the VM (Figure 3-39).



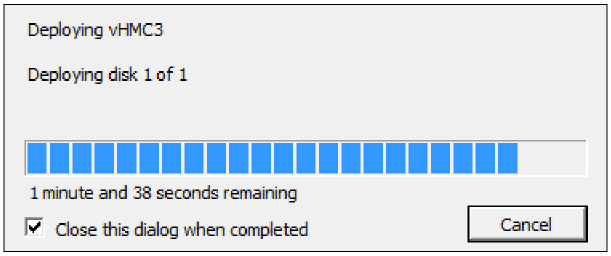
Deploying vHMC3

Creating VM vHMC3 ...

☑ Close this dialog when completed

Figure 3-39 Creating VM

The deployment continues and the OVA file is being uploaded (Figure 3-40).



Deploying vHMC3

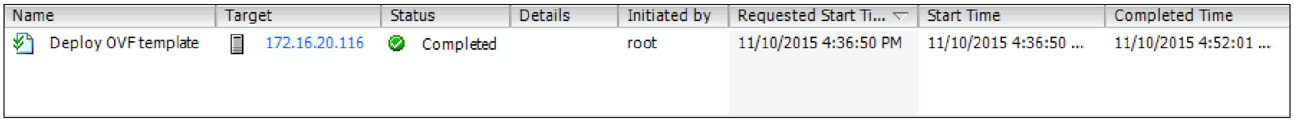
Deploying disk 1 of 1

1 minute and 38 seconds remaining

☑ Close this dialog when completed

Figure 3-40 Deploying VM

After the deployment finishes, you see the status in the vSphere Tasks pane (Figure 3-41).



Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Deploy OVF template	172.16.20.116	✓ Completed		root	11/10/2015 4:36:50 PM	11/10/2015 4:36:50 ...	11/10/2015 4:52:01 ...

Figure 3-41 Deployment completed

9. From the main vSphere panel, right-click the freshly deployed vHMC, and select **Edit Settings** (Figure 3-42).

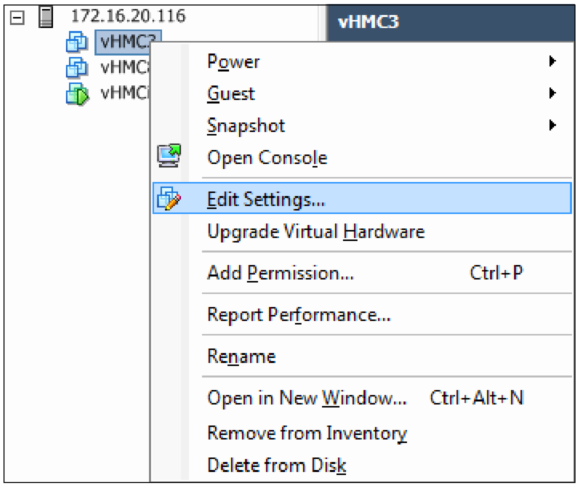
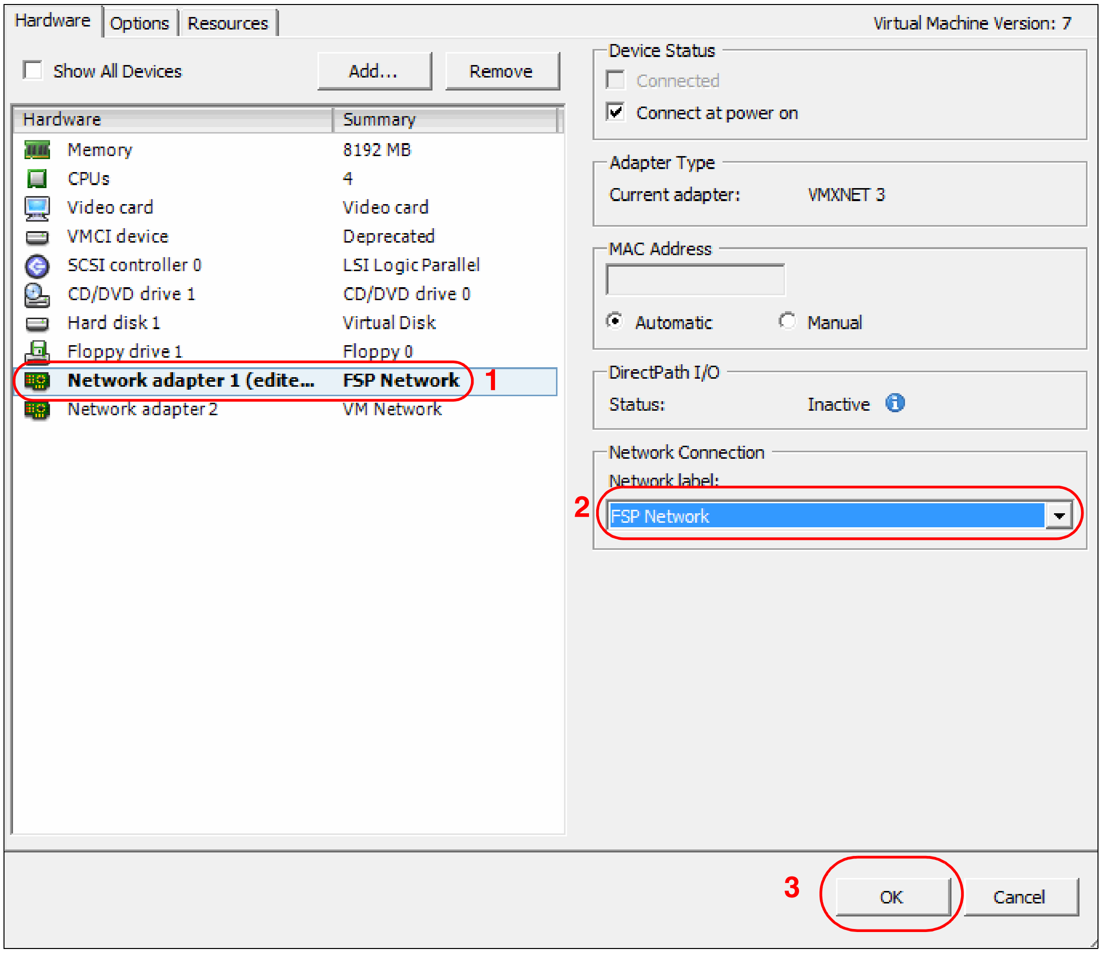


Figure 3-42 Edit VM settings

10. In the Virtual Machine properties panel (Figure 3-43), select the first virtual NIC, choose the appropriate network bridge, and then click **OK**.



Hardware | Options | Resources

Virtual Machine Version: 7

□ Show All Devices

Add... | Remove

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	CD/DVD drive 0
Hard disk 1	Virtual Disk
Floppy drive 1	Floppy 0
Network adapter 1 (edite...	**FSP Network**
Network adapter 2	VM Network

Device Status

□ Connected

☑ Connect at power on

Adapter Type

Current adapter: VMXNET 3

MAC Address

● Automatic ○ Manual

DirectPath I/O

Status: Inactive

Network Connection

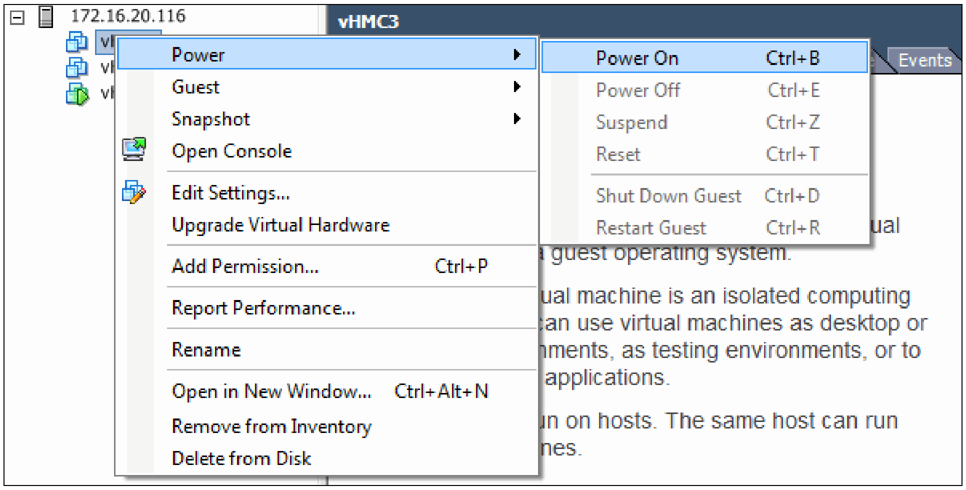
Network label:

FSP Network

OK | Cancel

Figure 3-43 VM Properties

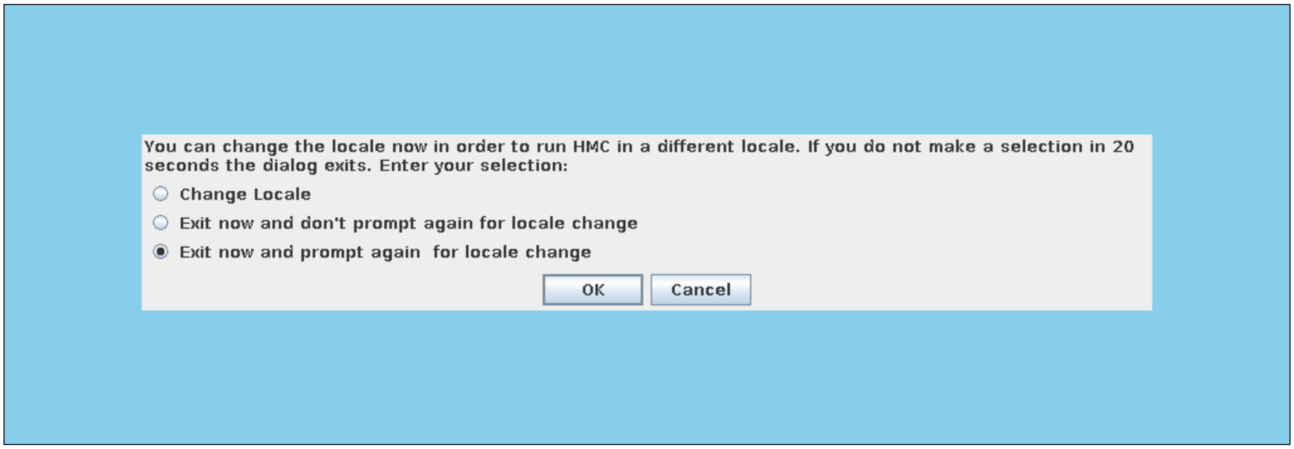
11. In the main vSphere pane, right-click the new VM and select **Power** → **Power On**, (Figure 3-44).



ual
a guest operating system.
ual machine is an isolated computing
an use virtual machines as desktop or
nments, as testing environments, or to
applications.
un on hosts. The same host can run
nes.

Figure 3-44 Power On the new VM

After the console opens, the locale change panel is displayed (Figure 3-45). You can now proceed with the Installation Wizard for the initial HMC configuration, and then follow step 5 on page 225.



You can change the locale now in order to run HMC in a different locale. If you do not make a selection in 20 seconds the dialog exits. Enter your selection:

○ Change Locale

○ Exit now and don't prompt again for locale change

● Exit now and prompt again for locale change

Figure 3-45   HMC locale selection

3.2.2 KVM virtual appliance deployment

This section describes the installation of an HMC, using the KVM image file. This method actually bypasses the whole installation phase, and brings you directly to the *HMC Installation Wizard*.

As an example of a KVM HMC deployment without the Activation Engine, you can use the *virt-manager* graphical interface to create the VM. This is necessary if you want to activate the DHCP server.

1. Verify that virtualization packages are installed on systems with Red Hat Enterprise Linux (RHEL) version 6.4 or later.
2. From the KVM server prompt, create a storage pool directory to host you virtual machine. This example uses `/var/lib/libvirt/images/vHMC2` directory:

   ```
   mkdir -p /var/lib/libvirt/images/vHMC2
   ```

3. Upload the image `.tar` file of the KVM `KVM_image.tar.gz` file to the host system, and move it to the appropriate location. This example moves it to `/var/lib/libvirt/images/vHMC2`.
4. Change to the appropriate directory:

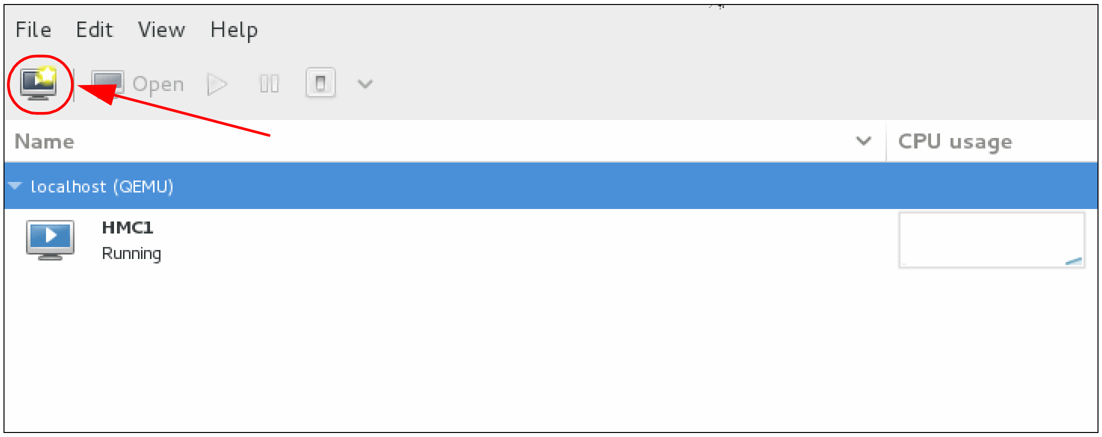
   ```
   cd /var/lib/libvirt/images/vHMC2
   ```

   Extract the virtual disk images:

   ```
   tar -zxvf KVM_image.tar.gz
   ```

5. For an installation engine without the Activation Engine, invoke the *KVM virtual machine manager* graphical interface to create the VM by using the **`virt-manager`** command.

6. You can now start creating your new virtual HMC by clicking the **New Virtual Machine** icon (Figure 3-46).

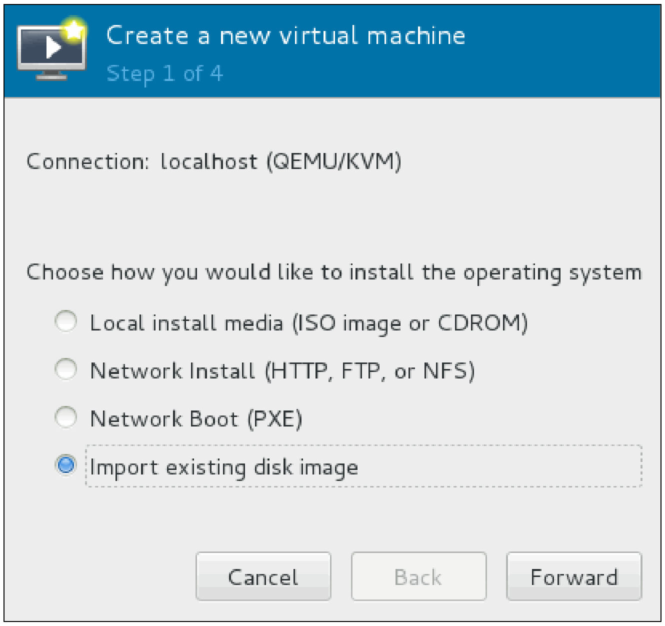


localhost (QEMU)

HMC1
Running

Figure 3-46 Create a new VM for deployment

7. Select **Import existing disk image** (Figure 3-47), and click **Forward**.



Connection: localhost (QEMU/KVM)

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)

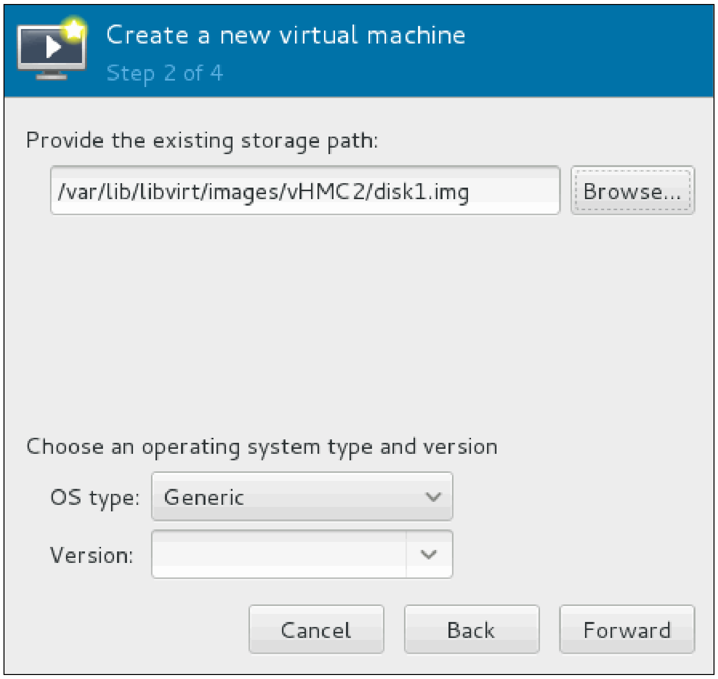
○ Network Install (HTTP, FTP, or NFS)

○ Network Boot (PXE)

● Import existing disk image

Figure 3-47 Choice of disk image

8. Click **Browse** to navigate in the KVM storage pools, select the appropriate image file that was previously uploaded, and click **Forward** (Figure 3-48).



Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

/var/lib/libvirt/images/vHMC2/disk1.img

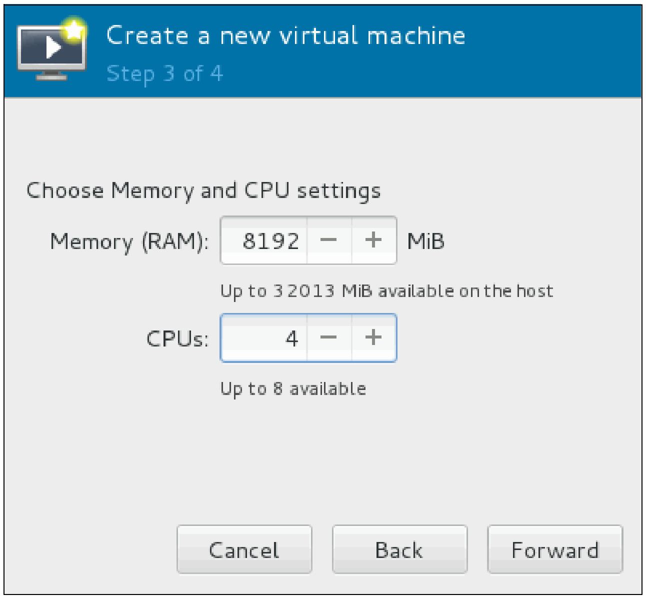
Choose an operating system type and version

OS type: Generic

Version:

Figure 3-48 Choose the disk image

9. Specify the memory size and number of CPUs (Figure 3-49).



Create a new virtual machine

Step 3 of 4

Choose Memory and CPU settings

Memory (RAM): 8192 MiB

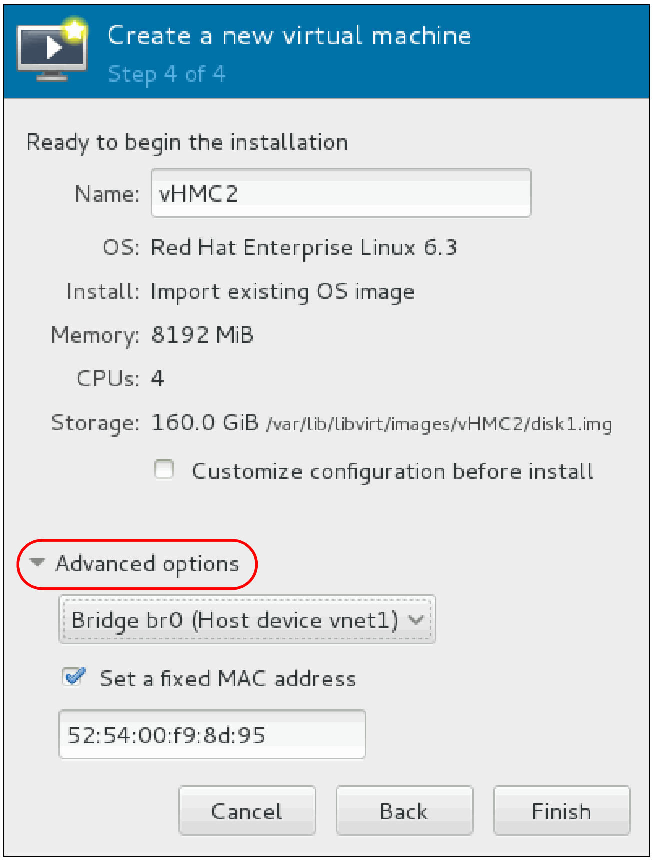
Up to 32013 MiB available on the host

CPUs: 4

Up to 8 available

Figure 3-49 Memory and CPUs selection

10. In the next panel (Figure 3-50), you can either select Customize configuration, in order to add another NIC, or change other parameters. In this example, select **Advanced options**, and then chose the appropriate network bridge. Click **Finish** to create the VM.



Create a new virtual machine
Step 4 of 4

Ready to begin the installation

Name: vHMC2

OS: Red Hat Enterprise Linux 6.3

Install: Import existing OS image

Memory: 8192 MiB

CPUs: 4

Storage: 160.0 GiB /var/lib/libvirt/images/vHMC2/disk1.img

□ Customize configuration before install

Advanced options

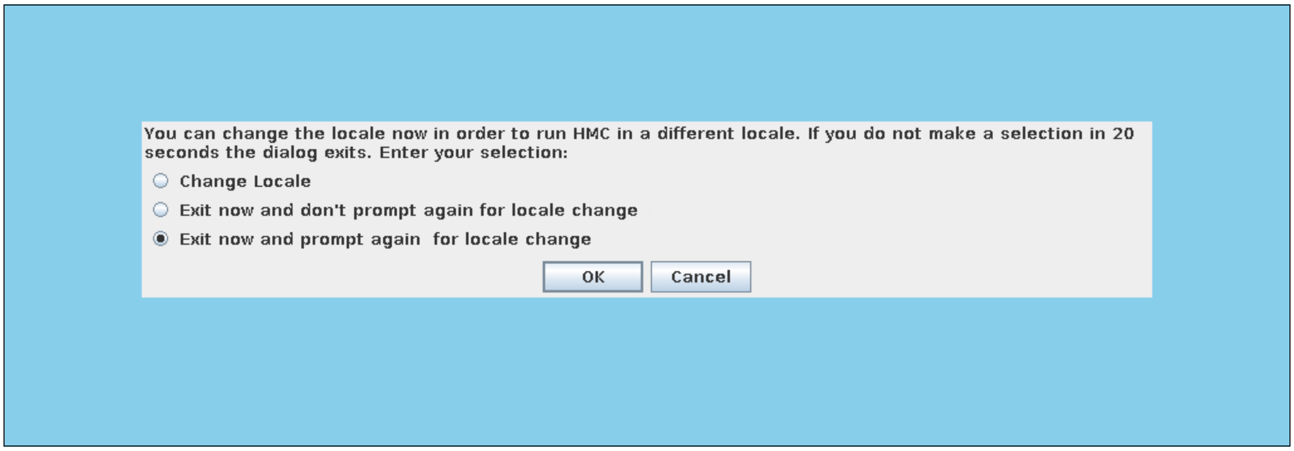
Bridge br0 (Host device vnet1)

☑ Set a fixed MAC address

52:54:00:f9:8d:95

Figure 3-50 Advanced options

11. The HMC reboots and displays the locale selection graphical dialog box (Figure 3-51). You can now proceed with the Installation Wizard for the initial HMC configuration, and follow the process described in step 5 on page 225.



You can change the locale now in order to run HMC in a different locale. If you do not make a selection in 20 seconds the dialog exits. Enter your selection:

○ Change Locale
○ Exit now and don't prompt again for locale change
● Exit now and prompt again for locale change

Figure 3-51 HMC locale selection

3.2.3 VMware appliance deployment with Activation Engine

This section describes the deployment of an HMC with the AE, using the VMware image file.

The Activation Engine is a framework that allows various components within a virtual machine to be configured during system startup. The Activation Engine can be used only with pre-captured disk images. For example, if a vHMC is created by using the HMC Recovery ISO file, then the Activation Engine is not enabled. To use the Activation Engine, set up an XML configuration profile to allow the vHMC to be in a ready-to-manage state on the first start. For detailed information regarding the XML configuration file, see the IBM Knowledge Center for HMC.

The `VMware_image.tar.gz` image provides the OVA image deployment file, and also a sample XML (`vHMC-Conf.xml`) configuration file for the Activation Engine.

> **Important:** The VMware server might not have all the UNIX commands required to create the files used to deploy the vHMC. For this reason, in the next example, the files are extracted on a Linux server providing an FTP server.

You can extract the OVA file on your local workstation or on a UNIX server providing FTP services.

This example uses a Linux server providing an FTP server. The files are extracted in a user directory owned by the `ftpuser` user ID, with the commands shown in Example 3-11. The `ftpuser` user ID is enabled for FTP services.

Example 3-11 Extract the files from VMWare tar file

```
#su - ftpuser
cd /home/ftpuser/vHMCvmware:
# tar -zxvf VMwareimage.tar.gz
# ls -al
total 7088220
drwxrwxr-x. 2 ftpuser ftpuser         84 Nov 11 09:05 .
drwx------. 7 ftpuser ftpuser       4096 Nov 10 19:27 ..
-rwxr-xr-x. 1 ftpuser ftpuser      11212 Nov 10 18:59 README.txt
-rwxr-xr-x. 1 ftpuser ftpuser      57153 Nov 10 18:59 vHMC-Conf.xml
-rwxr-xr-x. 1 ftpuser ftpuser 3744356352 Nov 10 19:02 vHMC.ova
-rw-r--r--. 1 ftpuser ftpuser 3513904650 Nov 11 09:06 VMware_image.tar.gz
```

After the files are extracted, use the following steps to deploy a vHMC VMware image with AE from the FTP server. All of these commands are issued with the `root` user ID:

1. Create a floppy disk image for VMware, with the commands shown in Example 3-12.

   Example 3-12 Create a floppy disk image

   ```
   # mkdir -p /tmp/VMwareFloppy
   # dd if=/dev/zero of=/tmp/VMwareFloppy/VMwareFloppy.flp count=1440 bs=1k
   1440+0 records in
   1440+0 records out
   1474560 bytes (1.5 MB) copied, 0.00317229 s, 465 MB/s
   # echo y|/sbin/mkfs.ext2 /tmp/VMwareFloppy/VMwareFloppy.flp
   ```

2. Loop-mount the floppy disk image as shown in Example 3-13.

Example 3-13 Loop mount virtual floppy image

```
# mount -o loop,rw /tmp/VMwareFloppy/VMwareFloppy.flp /mnt/Floppy
# df -h /mnt/Floppy
Filesystem      Size  Used Avail Use% Mounted on
/dev/loop0      1.4M   19K  1.3M   2% /mnt/Floppy
# df -h /mnt/Floppy
Filesystem      Size  Used Avail Use% Mounted on
/dev/loop0      1.4M   19K  1.3M   2% /mnt/Floppy
# ls -al /mnt/Floppy
total 13
drwxr-xr-x. 3 root root  1024 Nov 11 09:22 .
drwxr-xr-x. 5 root root    45 Nov  9 15:01 ..
drwx------. 2 root root 12288 Nov 11 09:22 lost+found
```

3. Edit the `vHMC-Conf.xml` file to change the values to match your environment. In this example, the file uses the parameters shown in Example 3-14. Non-default values are highlighted in bold.

Example 3-14 vHMC-Conf.xml for VMWare AE deployment

```
<vHMC-Configuration>
        <LicenseAgreement>
        </LicenseAgreement>
        <AcceptLicense>Yes</AcceptLicense>
        <Locale>en_US.UTF-8</Locale>
        <SetupWizard>No</SetupWizard>
        <SetupCallHomeWizard>No</SetupCallHomeWizard>
        <SetupKeyboard>No</SetupKeyboard>
        <Ethernet>
                <Enable>yes</Enable>
                <IPVersion>IPV4</IPVersion>
                <IPv4NetworkType>static</IPv4NetworkType>
                <IPv4Address>172.16.20.131</IPv4Address>
                <IPv4Netmask>255.255.252.0</IPv4Netmask>
                <IPv4Gateway>172.16.20.1</IPv4Gateway>
                <IPv6NetworkType></IPv6NetworkType>
                <IPv6Address></IPv6Address>
                <IPv6Gateway></IPv6Gateway>
                <Hostname>vHMCae</Hostname>
                <Domain>itso.ibm.com</Domain>
                <DNSServers></DNSServers>
                <Firewall>
                        <PEGASUS>Enabled</PEGASUS>
                        <RPD>Enabled</RPD>
                        <FCS>Enabled</FCS>
                        <I5250>Enabled</I5250>
                        <PING>Enabled</PING>
                        <L2TP>Disabled</L2TP>
                        <SLP>Enabled</SLP>
                        <RSCT>Enabled</RSCT>
                        <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
                        <SSH>Enabled</SSH>
                        <VTTY>Enabled</VTTY>
                        <NTP>Disabled</NTP>
                        <SNMPTraps>Disabled</SNMPTraps>
                        <SNMPAgents>Disabled</SNMPAgents>
                </Firewall>
        </Ethernet>
        <Ethernet>
                <Enable>yes</Enable>
                <IPVersion>IPV4</IPVersion>
                <IPv4NetworkType>static</IPv4NetworkType>
                <IPv4Address>10.1.0.131</IPv4Address>
                <IPv4Netmask>255.255.240.0</IPv4Netmask>
                <IPv4Gateway></IPv4Gateway>
                <IPv6NetworkType></IPv6NetworkType>
                <IPv6Address></IPv6Address>
                <IPv6Gateway></IPv6Gateway>
                <Hostname></Hostname>
                <Domain></Domain>
                <DNSServers></DNSServers>
                <Firewall>
                        <PEGASUS>Enabled</PEGASUS>
                        <RPD>Enabled</RPD>
                        <FCS>Enabled</FCS>
                        <I5250>Enabled</I5250>
                        <PING>Enabled</PING>
                        <L2TP>Disabled</L2TP>
                        <SLP>Enabled</SLP>
                        <RSCT>Enabled</RSCT>
                        <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
                        <SSH>Enabled</SSH>
                        <VTTY>Enabled</VTTY>
                        <NTP>Disabled</NTP>
                        <SNMPTraps>Disabled</SNMPTraps>
                        <SNMPAgents>Disabled</SNMPAgents>
                </Firewall>
        </Ethernet>
</vHMC-Configuration>
```

4. Copy the file on the virtual floppy image, then unmount it as shown in Example 3-15.

Example 3-15 Copy XML config file on virtual floppy

```
# chmod 777 vHMC-Conf.xml
# cp vHMC-Conf.xml /mnt/Floppy/
# ls -al /mnt/Floppy/
total 16
drwxr-xr-x. 3 root root  1024 Nov 11 10:01 .
drwxr-xr-x. 5 root root    45 Nov  9 15:01 ..
drwx------. 2 root root 12288 Nov 11 09:22 lost+found
-rwxr-xr-x. 1 root root  2046 Nov 11 10:01 vHMC-Conf.xml
# umount /mnt/Floppy
```

5. Create the `/vmfs/volumes/datastore1/Floppies` directory on the *VMWare* server with this command:

```
mkdir -p /vmfs/volumes/datastore1/Floppies
```

Upload the floppy image file to the VMware server, as shown in Example 3-16.

Example 3-16 Transfer the virtual floppy image on VMware server

```
# scp /tmp/VMwareFloppy/VMwareFloppy.flp
root@172.16.20.116:/vmfs/volumes/datastore1/Floppies
Password:
VMwareFloppy.flp
100% 1440KB   1.4MB/s   00:00
```

6. From the vSphere client user interface, deploy an OVF template, as shown in Figure 3-52.

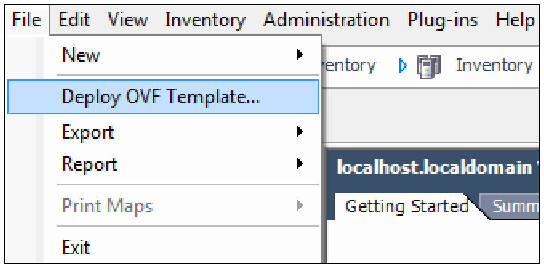
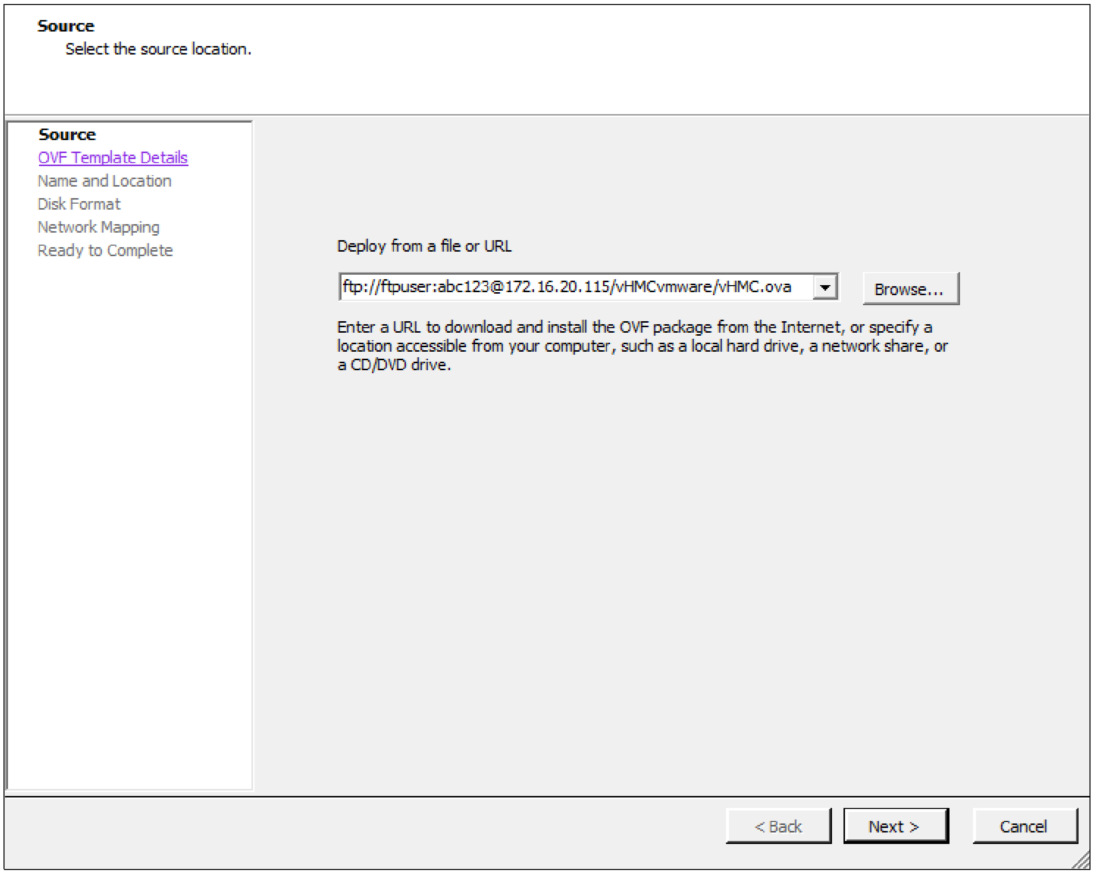


Figure 3-52 Deploy a new VM

7. You are prompted to browse to the OVA file location as shown in Figure 3-53. The default is to browse for an OVA file located on the workstation running the vSphere client. In this example the deployment location uses a URL with the user and password specified:

`ftp://ftpuser:abc123@172.16.20.115/vHMCvmware/vHMC.ova`


Source

Select the source location.

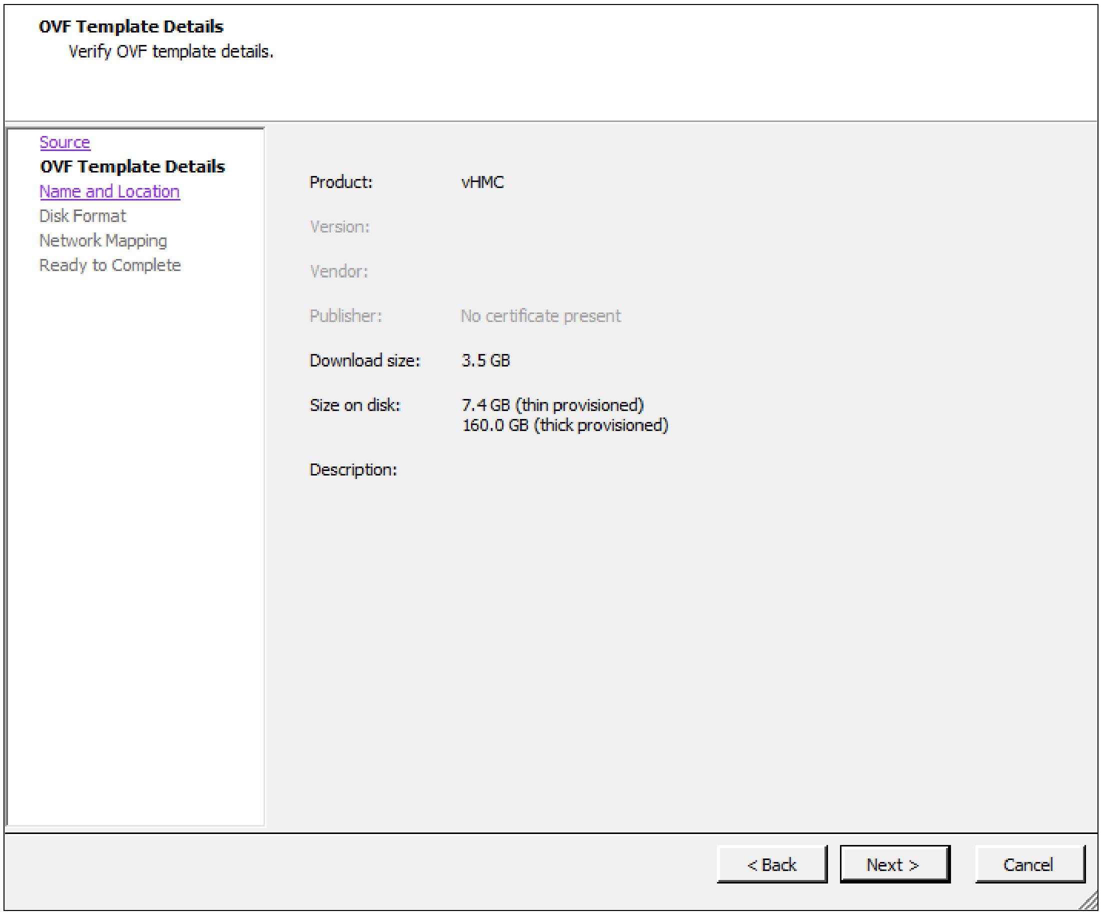
Deploy from a file or URL

ftp://ftpuser:abc123@172.16.20.115/vHMCvmware/vHMC.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Figure 3-53 Choose an OVA file to deploy

8. In the OVF Template Details panel (Figure 3-54), click **Next** to continue.



OVF Template Details

Verify OVF template details.

Product: vHMC

Version:

Vendor:

Publisher: No certificate present

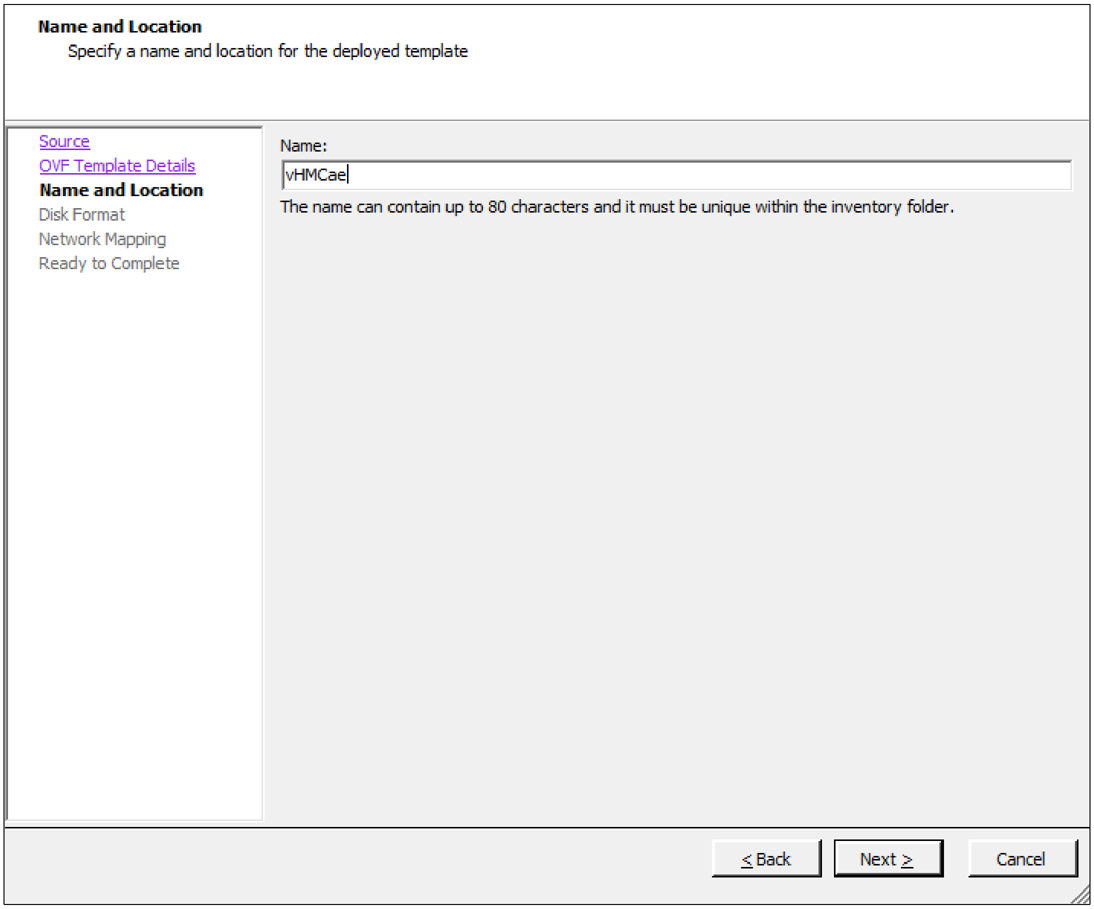
Download size: 3.5 GB

Size on disk: 7.4 GB (thin provisioned)
160.0 GB (thick provisioned)

Description:

Figure 3-54 OVF template details

9. In the OVF Name and Location panel, enter a VM name, as shown in Figure 3-55, and click **Next**.



Name and Location

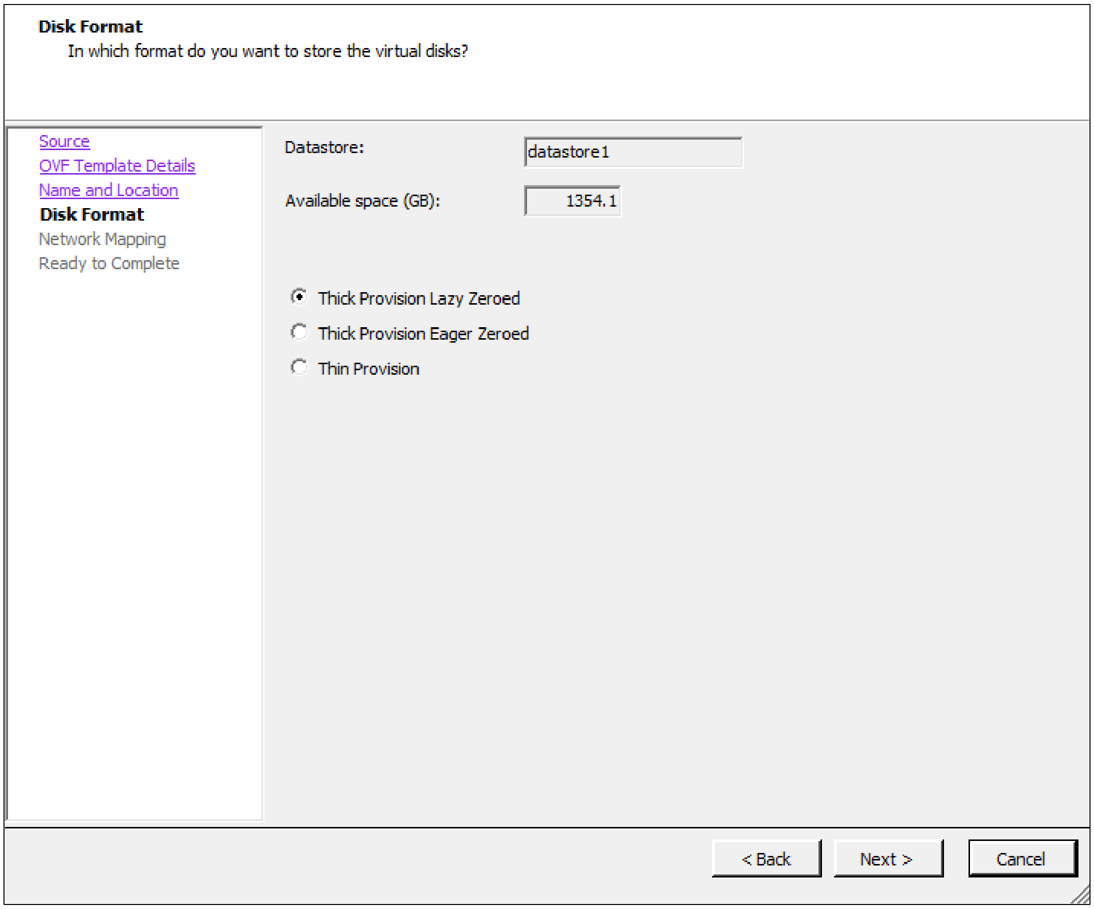
Specify a name and location for the deployed template

Name: vHMCae

The name can contain up to 80 characters and it must be unique within the inventory folder.

Figure 3-55 Choose a VM name

10. In the Disk Format panel (Figure 3-56), click **Next**.



Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1

Available space (GB): 1354.1

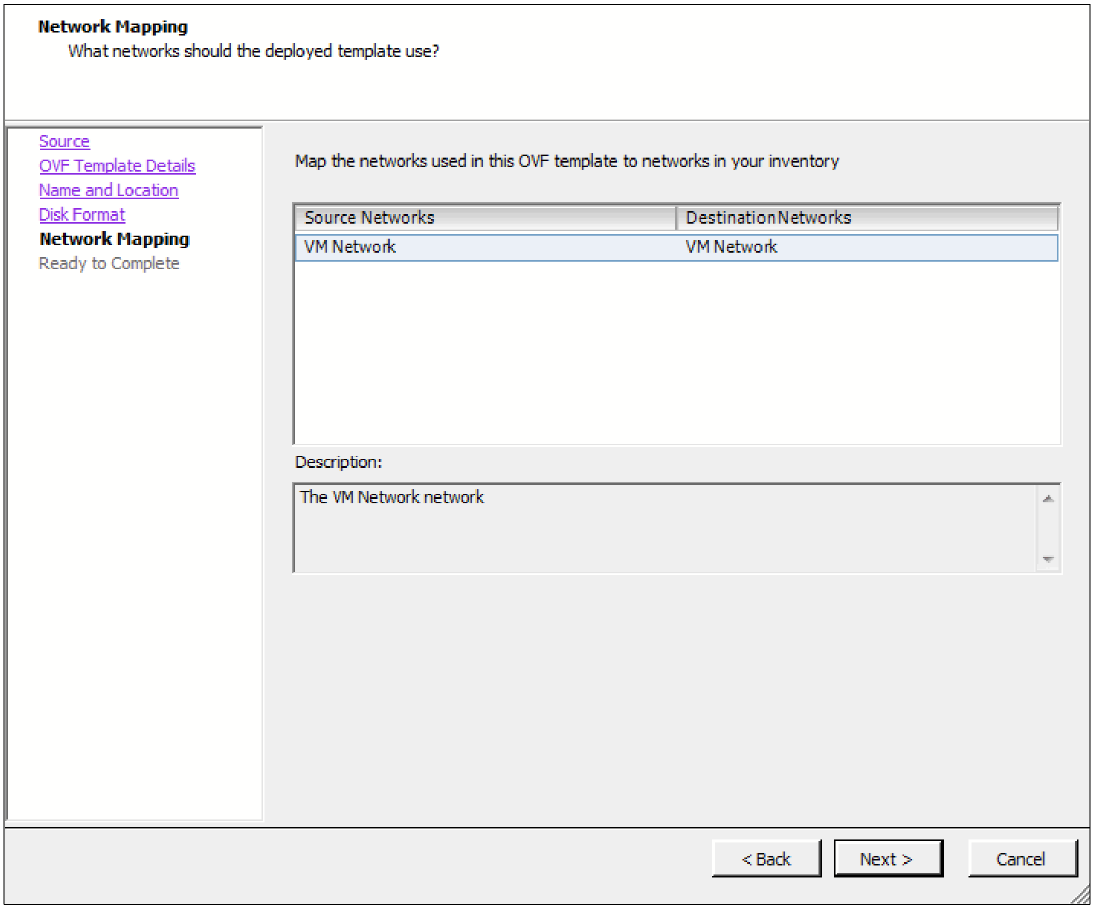
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

Figure 3-56 Disk Format

11.In the Network Mapping panel (Figure 3-57), click **Next**.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

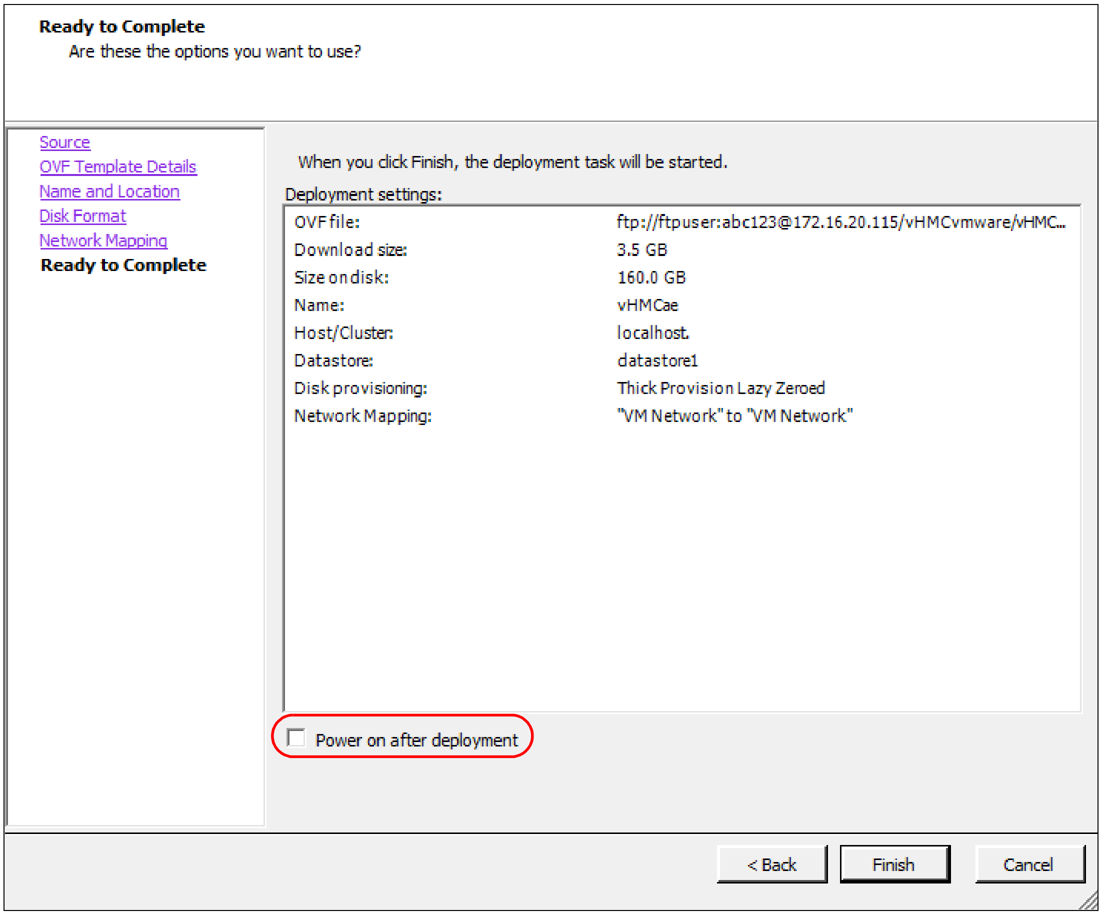
Source Networks	DestinationNetworks
VM Network	VM Network

Description:

The VM Network network

Figure 3-57 Network Mapping

12. In the Ready to Complete panel (Figure 3-58), *do not select* Power on after deployment, because you will be changing several settings later. Click **Finish** to create the VM.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

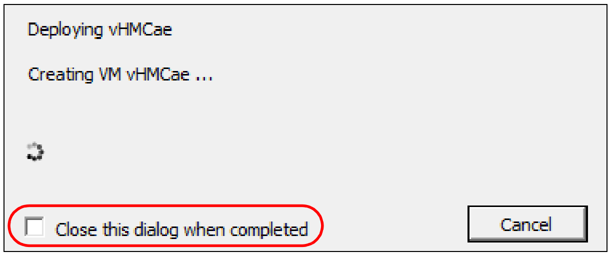
Deployment settings:

OVF file:	ftp://ftpuser:abc123@172.16.20.115/vHMCvmware/vHMC...
Download size:	3.5 GB
Size on disk:	160.0 GB
Name:	vHMCae
Host/Cluster:	localhost.
Datastore:	datastore1
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"VM Network" to "VM Network"

□ Power on after deployment

Figure 3-58 Ready to Complete

13. The VM creation now starts (Figure 3-59). If you do not select **Close this dialog box**, a completion panel will be displayed.



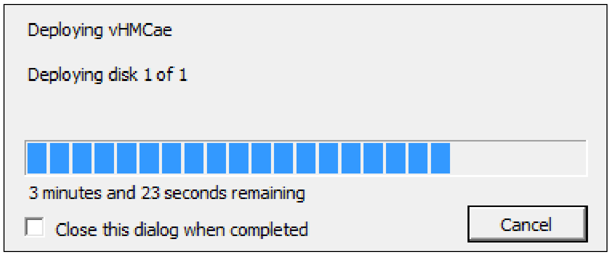
Deploying vHMCae

Creating VM vHMCae ...

□ Close this dialog when completed

Figure 3-59 Deployment starts

VMware downloads the file from the FTP server; the progress is displayed (Figure 3-60).



Deploying vHMCae

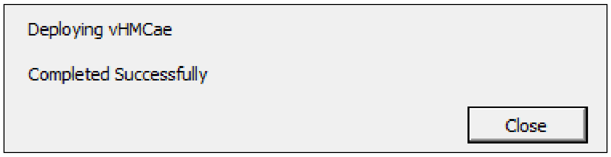
Deploying disk 1 of 1

3 minutes and 23 seconds remaining

□ Close this dialog when completed

Figure 3-60 OVA download

14. In the Deployment success panel (Figure 3-61), click **Close**.



Deploying vHMCae

Completed Successfully

Figure 3-61 Deployment is successful

15. Right-click the fresh VM and then select **Edit Settings** (Figure 3-62).

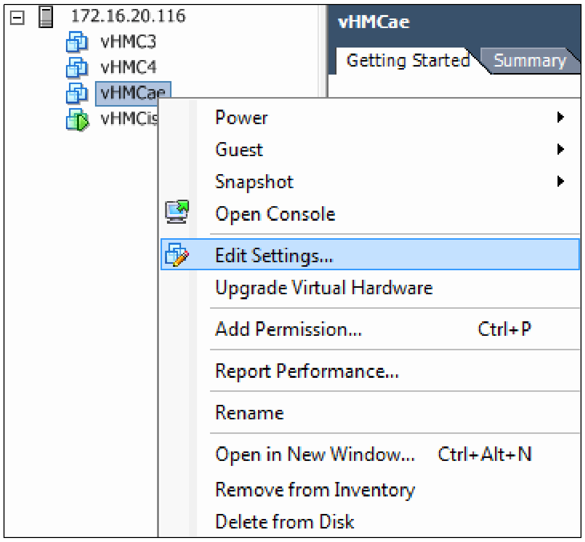
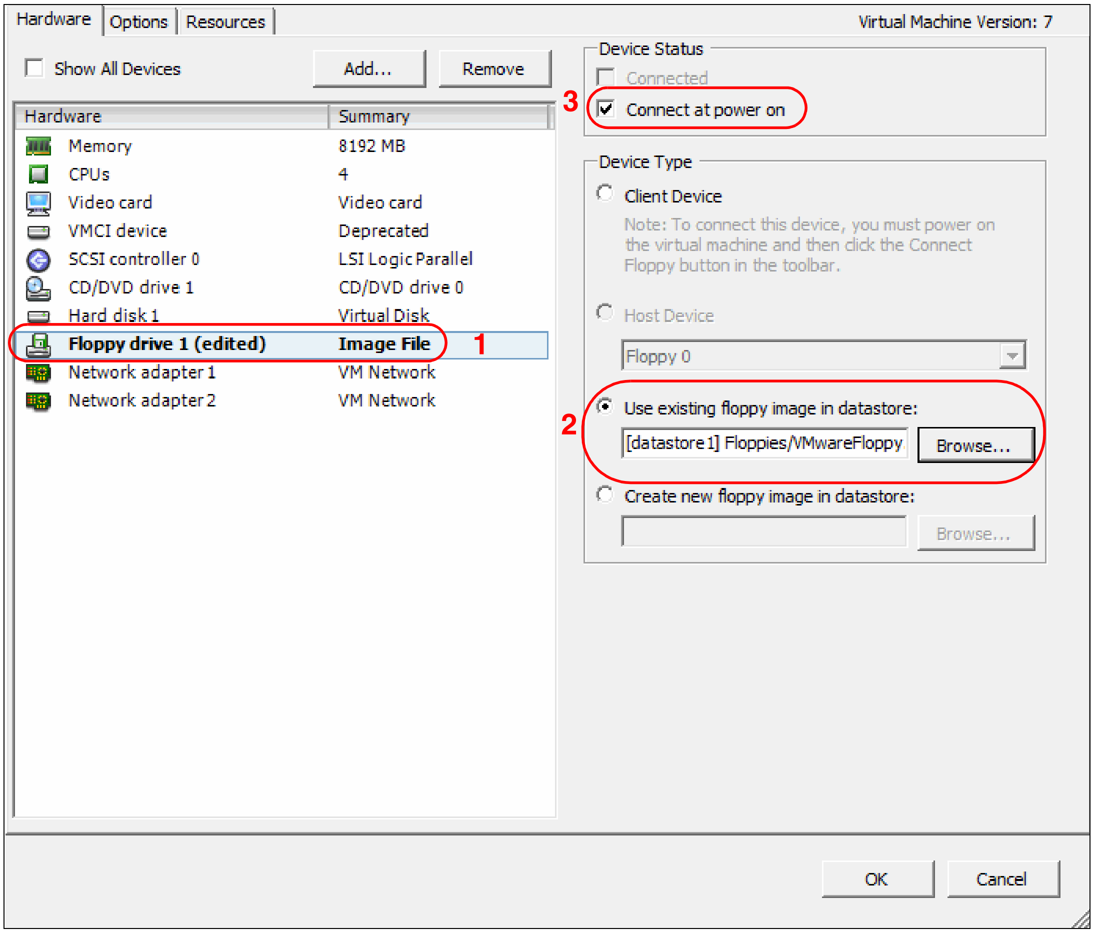


Figure 3-62 Edit Settings

16. Select **Floppy drive** (Figure 3-63), and navigate to connect the virtual floppy image uploaded previously. Select **Connect at power**. *Do not click* OK yet.



Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	CD/DVD drive 0
Hard disk 1	Virtual Disk
Floppy drive 1 (edited)	**Image File**
Network adapter 1	VM Network
Network adapter 2	VM Network

Device Status

□ Connected

☑ Connect at power on

Device Type

○ Client Device

Note: To connect this device, you must power on the virtual machine and then click the Connect Floppy button in the toolbar.

○ Host Device

Floppy 0

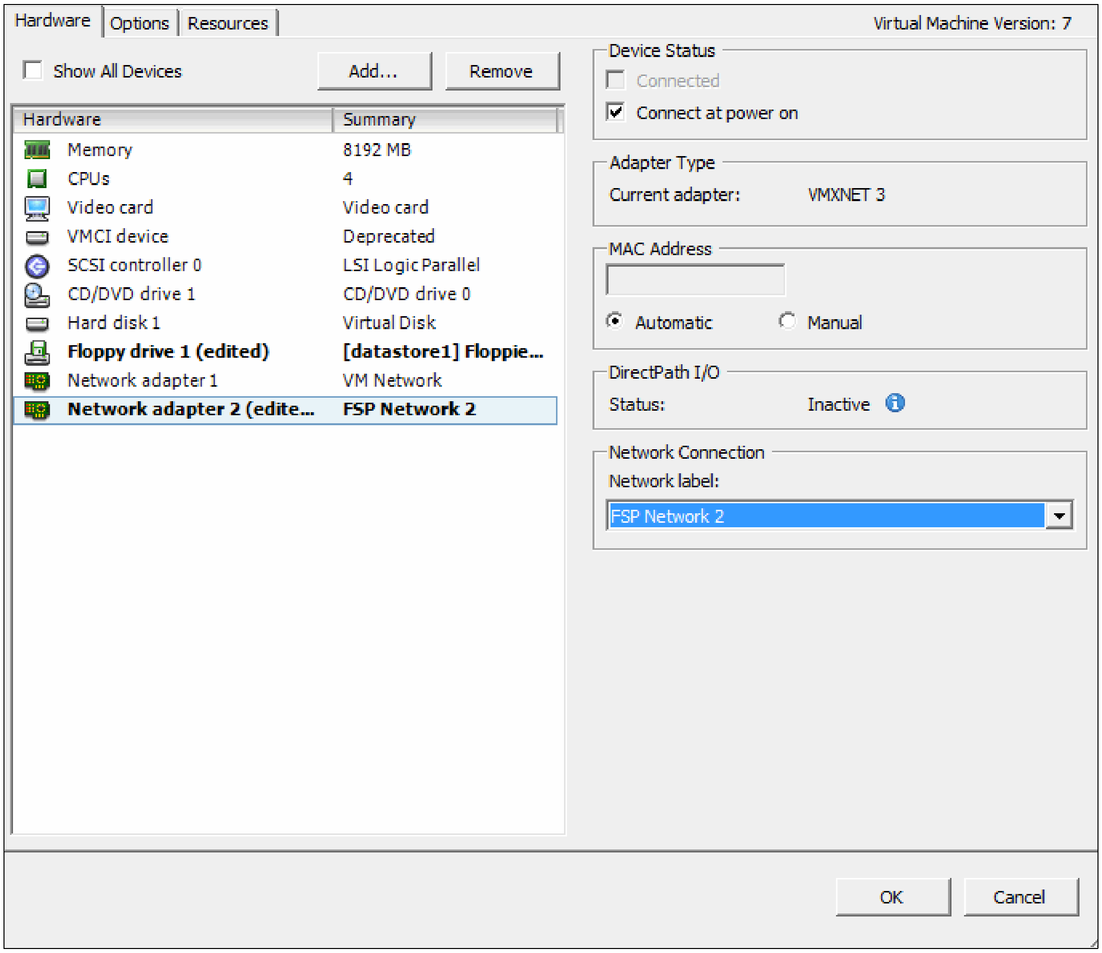
● Use existing floppy image in datastore:

[datastore1] Floppies/VMwareFloppy

○ Create new floppy image in datastore:

Figure 3-63 Choose floppy image

17. Select **Network adapter** (Figure 3-64) and the appropriate network bridges for the virtual NICs. Click **OK** to complete the configuration.



Virtual Machine Version: 7

☐ Show All Devices

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	CD/DVD drive 0
Hard disk 1	Virtual Disk
Floppy drive 1 (edited)	**[datastore1] Floppie...**
Network adapter 1	VM Network
Network adapter 2 (edite...	**FSP Network 2**

Device Status

☐ Connected

☑ Connect at power on

Adapter Type

Current adapter: VMXNET 3

MAC Address

● Automatic ○ Manual

DirectPath I/O

Status: Inactive

Network Connection

Network label:

FSP Network 2

Figure 3-64 Network bridge selection

18. From the main vSphere panel, right-click the new VM and select **Open Console** (Figure 3-65).

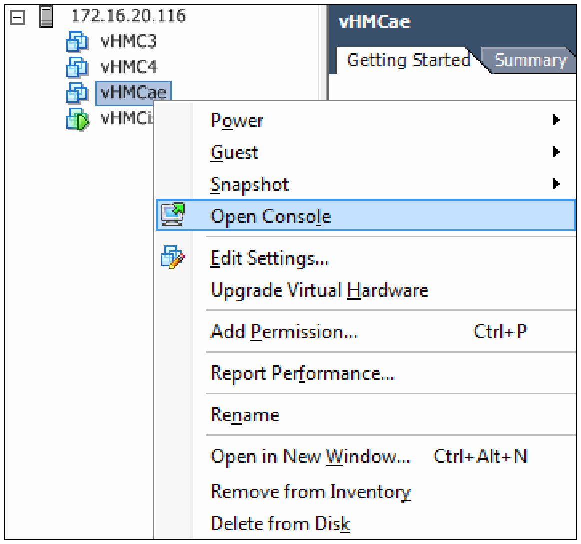


Figure 3-65 Open the console

19. Click the **Power On** button (Figure 3-66) to boot the VM.

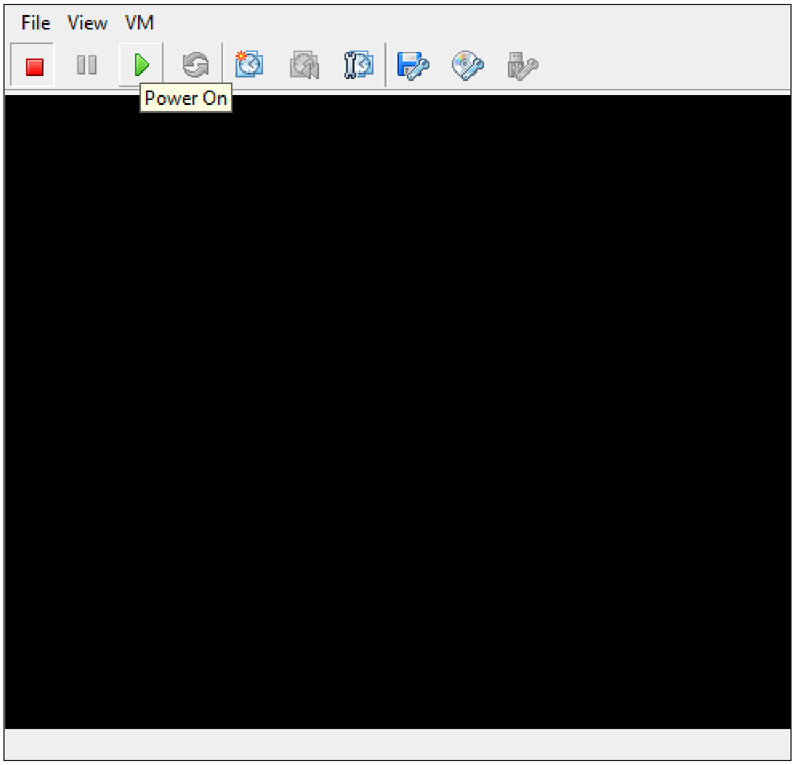
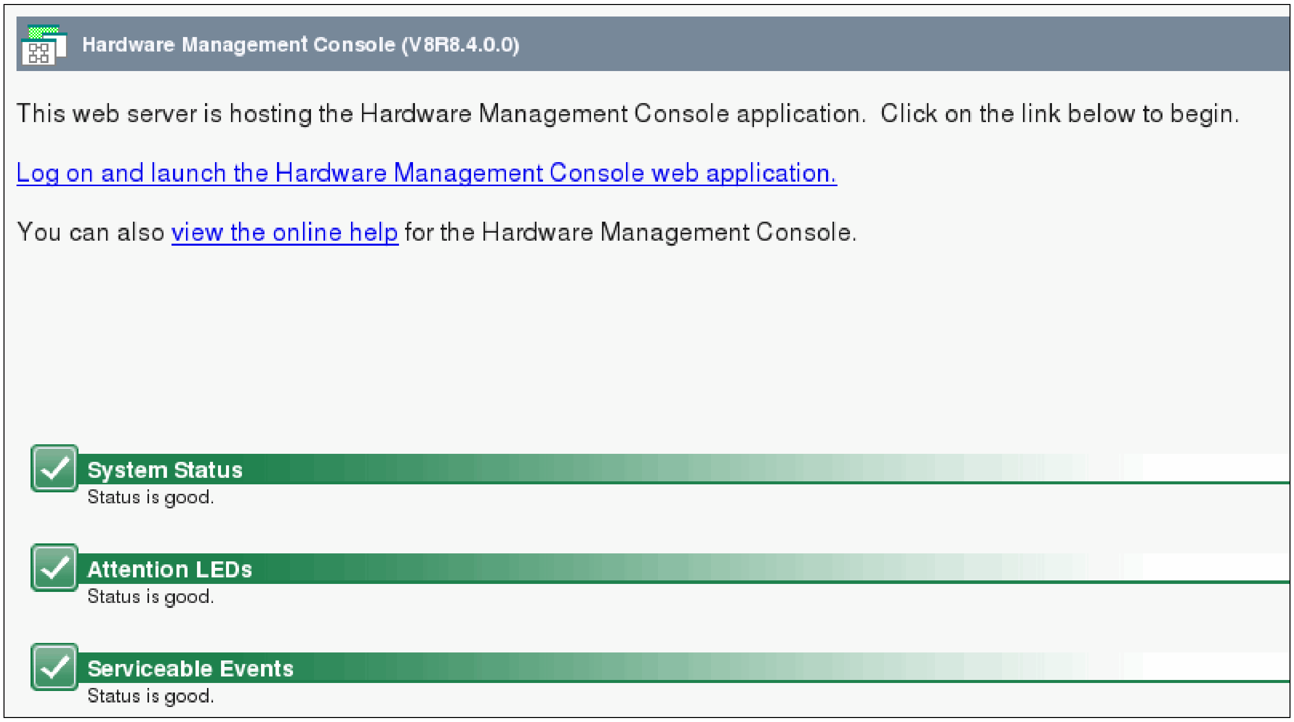


Figure 3-66 Boot the VM

20. After the vHMC is booted, and AE completed its work, you can now log in from the console, as shown in Figure 3-67.



Hardware Management Console (V8R8.4.0.0)

This web server is hosting the Hardware Management Console application. Click on the link below to begin.

Log on and launch the Hardware Management Console web application.

You can also view the online help for the Hardware Management Console.

✓ System Status
Status is good.

✓ Attention LEDs
Status is good.

✓ Serviceable Events
Status is good.

Figure 3-67   HMC welcome panel

Because the SSH connection is also available, you can use **ssh** to get to the freshly customized vHMC, as shown in Example 3-17.

Example 3-17   An ssh connection to the HMC

```
# ssh hscroot@172.16.20.131
The authenticity of host '172.16.20.131 (172.16.20.131)' can't be established.
ECDSA key fingerprint is d4:b4:a3:b4:7a:32:11:37:c1:9d:48:75:72:80:66:e2.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.20.131' (ECDSA) to the list of known hosts.
hscroot@172.16.20.131's password:
hscroot@vHMCae:~> lshmc -n
hostname=vHMCae,domain=itso.ibm.com,"ipaddr=172.16.20.131,10.1.0.131","networkmask
=255.255.252.0,255.255.240.0",gateway=172.16.20.1,nameserver=,domainsuffix=itso.ib
m.com,slipipaddr=10.253.0.1,slipnetmask=255.255.0.0,"ipaddrlpar=172.16.20.131,10.1
.0.131","networkmasklpar=255.255.252.0,255.255.240.0",clients=,ipv6addrlpar=,"slpi
paddrs=172.16.20.131,10.1.0.131,fe80::20c:29ff:fe43:a22/64,fe80::20c:29ff:fe43:a2c
/64",ipv4addr_eth0=172.16.20.131,ipv4netmask_eth0=255.255.252.0,ipv4dhcp_eth0=off,
ipv6addr_eth0=,ipv6auto_eth0=off,ipv6privacy_eth0=off,ipv6dhcp_eth0=off,lparcomm_e
th0=off,jumboframe_eth0=off,speed_eth0=auto,duplex_eth0=auto,tso_eth0=,ipv4addr_et
h1=10.1.0.131,ipv4netmask_eth1=255.255.240.0,ipv4dhcp_eth1=off,ipv6addr_eth1=,ipv6
auto_eth1=off,ipv6privacy_eth1=off,ipv6dhcp_eth1=off,lparcomm_eth1=off,jumboframe_
eth1=off,speed_eth1=auto,duplex_eth1=auto,tso_eth1=
```

The vHMC is now properly customized, and you can proceed with further tasks.

3.2.4 KVM virtual appliance deployment with AE

This section describes the deployment of an HMC with the Activation Engine (AE), using the KVM image file.

The AE is a framework that allows various components within a virtual machine to be configured during system startup. The AE can be used only with pre-capture disk images. For example, if a vHMC is created by using the HMC Recovery ISO file, then the AE is not enabled. To use the AE, you must set up an XML configuration profile to allow the vHMC to be in a ready-to-manage state on first start. For detailed information regarding the XML configuration file, see the IBM Knowledge Center for HMC.

The `KVM_image.tar.gz` image provides two XML sample configuration files:

- The `domain.xml` file describes the VM (domain). It is given as an input to the **`virsh`** command to create the VM. It is a KVM configuration file. For further details, see the KVM documentation. This file can be renamed to match your naming requirements. It can be named after the VM.
- The `vHMC-Conf.xml` file is provided with the HMC configuration customization. It is used by the HMC installer to configure the HMC in the first place. It uses HMC related XML tags that are described in the IBM Knowledge Center for the HMC.

The following examples provides two sets of these XML configuration files. One shows a simple AE deployment, and the other an advanced deployment with chosen MAC addresses.

Simple AE deployment

To deploy an HMC with a simple configuration, with two NICs, use the following steps:

1. Verify that virtualization packages are installed on systems with Red Hat Enterprise Linux (RHEL) version 6.4 or later.
2. Create a storage pool directory to host you virtual machine, for example `/var/lib/libvirt/images/vHMC2`:

   ```
   mkdir -p /var/lib/libvirt/images/vHMC2
   ```

3. Upload the image `.tar` file of the KVM `KVM_image.tar.gz` file to the host system, and move it to the appropriate location. This example copies it to `/var/lib/libvirt/images/vHMC2`.
4. Change to the appropriate directory:

   ```
   cd /var/lib/libvirt/images/vHMC2
   ```

   Extract the virtual disk image file:

   ```
   tar -zxvf KVM_image.tar.gz
   ```

   When complete, the extracted files are listed, as shown in Example 3-18.

   Example 3-18 KVM image files

   ```
   [root@kvm1 vHMC2]# ls -als
   total 9985924
         0 drwxr-xr-x. 2 root root           91 Nov 10 09:36 .
         0 drwxr-xr-x. 7 root root           66 Nov 10 09:32 ..
         4 -rw-r--r--. 1 root root          214 Oct 23 15:05 checksum
   9985848 -rw-r--r--. 1 root root 171798691840 Oct 23 14:41 disk1.img
         4 -rw-r--r--. 1 root root         1654 Oct 12 19:40 domain.xml
        12 -rw-r--r--. 1 root root        11212 Oct 21 12:52 README.txt
        56 -rw-r--r--. 1 root root        57153 Oct 19 16:09 vHMC-Conf.xml
   ```

You can now make a copy of the domain file with the **cp domain.xml vHMC2.xml** command and customize the VM. Example 3-19 shows the vHMC2.xml domain configuration file with a second NIC. The non-default configuration tags are bold.

Example 3-19 vHMC2.xml configuration file

```
<domain type='kvm'>
  <name>vHMC2</name>
  <uuid></uuid>
  <memory unit='KiB'>4194304</memory>
  <currentMemory unit='KiB'>4194304</currentMemory>
  <vcpu placement='static'>2</vcpu>
  <os>
    <type arch='x86_64' machine='rhel6.3.0'>hvm</type>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='cdrom'>
      <target dev='hdc' bus='ide'/>
      <readonly/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='raw' cache='none'/>
      <source file='/var/lib/libvirt/images/vHMC2/disk1.img'/>
      <target dev='vda' bus='virtio'/>
    </disk>
    <disk type='file' device='floppy'>
      <driver name='qemu' type='raw' cache='default'/>
      <source file='/var/lib/libvirt/images/vHMC2/Floppy.img'/>
      <target dev='fda' bus='fdc'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <interface type='bridge'>
      <source bridge='br0'/>
      <target dev='vnet0'/>
      <model type='virtio'/>
    </interface>
    <interface type='bridge'>
      <source bridge='br1'/>
      <target dev='vnet1'/>
      <model type='virtio'/>
    </interface>
    <serial type='pty'>
      <target port='0'/>
    </serial>
    <console type='pty'>
```

```
      <target type='serial' port='0'/>
    </console>
    <input type='mouse' bus='ps2'/>
    <graphics type='vnc' port='-1' autoport='yes'/>
    <video>
      <model type='vga'/>
    </video>
    <memballoon model='virtio'>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
function='0x0'/>
    </memballoon>
  </devices>
</domain>
```

5. Create the floppy disk image, using the **dd** command, to host the `vHMC-Conf.xml` file, as shown in Example 3-20. The floppy disk image file name must be the same as the one specified in the `domain.xml` configuration file used to define the VM (**`vHMC2.xml`** in this example).

Example 3-20 Create a floppy disk image file

```
[root@kvm1 vHMC2]# dd if=/dev/zero of=/var/lib/libvirt/images/vHMC2/Floppy.img
count=1440 bs=1k
1440+0 records in
1440+0 records out
1474560 bytes (1.5 MB) copied, 0.00322682 s, 457 MB/s
```

6. The **mkfs.ext2** command is used to create a file system on the floppy disk image, as shown in Example 3-21.

Example 3-21 Create a file system on floppy image file

```
[root@kvm1 vHMC2]# echo y|/sbin/mkfs.ext2
/var/lib/libvirt/images/vHMC2/Floppy.img
mke2fs 1.42.9 (28-Dec-2013)
/var/lib/libvirt/images/vHMC2/Floppy.img is not a block special device.
Proceed anyway? (y,n) Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
Stride=0 blocks, Stripe width=0 blocks
184 inodes, 1440 blocks
72 blocks (5.00%) reserved for the super user
First data block=1
Maximum filesystem blocks=1572864
1 block group
8192 blocks per group, 8192 fragments per group
184 inodes per group

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

7. The default `vHMC-Conf.xml` configuration file is modified (Example 3-22) to match the new VM configuration. It has a configured second NIC and changed firewall tags.

> **Note:** The file name cannot be changed. You can add allowed configuration tags, but none of the default tags from the default configuration file should be removed.

Example 3-22 vHMC-Conf.xml files

```
<vHMC-Configuration>
        <LicenseAgreement>
        </LicenseAgreement>
        <AcceptLicense>Yes</AcceptLicense>
        <Locale>en_US.UTF-8</Locale>
        <SetupWizard>No</SetupWizard>
        <SetupCallHomeWizard>No</SetupCallHomeWizard>
        <SetupKeyboard>No</SetupKeyboard>
        <Ethernet>
                <Enable>yes</Enable>
                <IPVersion>IPV4</IPVersion>
                <IPv4NetworkType>static</IPv4NetworkType>
                <IPv4Address>172.16.20.130</IPv4Address>
                <IPv4Netmask>255.255.252.0</IPv4Netmask>
                <IPv4Gateway>172.16.20.1</IPv4Gateway>
                <IPv6NetworkType></IPv6NetworkType>
                <IPv6Address></IPv6Address>
                <IPv6Gateway></IPv6Gateway>
                <Hostname>vHMC2</Hostname>
                <Domain>itso.ibm.com</Domain>
                <DNSServers></DNSServers>
                <Firewall>
                        <PEGASUS>Enabled</PEGASUS>
                        <RPD>Enabled</RPD>
                        <FCS>Enabled</FCS>
                        <I5250>Enabled</I5250>
                        <PING>Enabled</PING>
                        <L2TP>Disabled</L2TP>
                        <SLP>Enabled</SLP>
                        <RSCT>Enabled</RSCT>
                        <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
                        <SSH>Enabled</SSH>
                        <VTTY>Enabled</VTTY>
                        <NTP>Disabled</NTP>
                        <SNMPTraps>Disabled</SNMPTraps>
                        <SNMPAgents>Disabled</SNMPAgents>
                </Firewall>
        </Ethernet>
        <Ethernet>
                <Enable>yes</Enable>
                <IPVersion>IPV4</IPVersion>
                <IPv4NetworkType>static</IPv4NetworkType>
                <IPv4Address>10.1.0.130</IPv4Address>
                <IPv4Netmask>255.255.240.0</IPv4Netmask>
                <IPv4Gateway></IPv4Gateway>
                <IPv6NetworkType></IPv6NetworkType>
                <IPv6Address></IPv6Address>
                <IPv6Gateway></IPv6Gateway>
                <Hostname>vHMC2</Hostname>
                <Domain>itso.ibm.com</Domain>
                <DNSServers></DNSServers>
                <Firewall>
                        <PEGASUS>Enabled</PEGASUS>
                        <RPD>Enabled</RPD>
                        <FCS>Enabled</FCS>
                        <I5250>Enabled</I5250>
                        <PING>Enabled</PING>
                        <L2TP>Disabled</L2TP>
                        <SLP>Enabled</SLP>
                        <RSCT>Enabled</RSCT>
                        <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
                        <SSH>Enabled</SSH>
                        <VTTY>Enabled</VTTY>
                        <NTP>Disabled</NTP>
                        <SNMPTraps>Disabled</SNMPTraps>
                        <SNMPAgents>Disabled</SNMPAgents>
                </Firewall>
        </Ethernet>
</vHMC-Configuration>
```

8. You can now mount the floppy image file as a file system with the mount command (Example 3-23).

Example 3-23 Loop mount the floppy image file

```
[root@kvm1 vHMC2]# mount -o loop,rw /var/lib/libvirt/images/vHMC2/Floppy.img
/mnt/Floppy
[root@kvm1 vHMC2]# df -h /mnt/Floppy/
Filesystem      Size  Used Avail Use% Mounted on
/dev/loop0      1.4M   19K  1.3M   2% /mnt/Floppy
```

9. Copy the customized `vHMC-Conf.xml` file onto the floppy image file system (Example 3-24).

Example 3-24 Copy the configuration file on the floppy file system

```
[root@kvm1 vHMC2]# cp /var/lib/libvirt/images/vHMC2/vHMC-Conf.xml /mnt/Floppy
[root@kvm1 vHMC2]# ls -altr /mnt/Floppy/
total 16
drwxr-xr-x. 5 root root    45 Nov  9 15:01 ..
drwx------. 2 root root 12288 Nov  9 18:06 lost+found
-rwxr-xr-x. 1 root root  1170 Nov  9 18:15 vHMC-Conf.xml
```

10. Unmount the floppy image file system, with the **`umount /mnt/Floppy/`** command.

11. Use the **`virsh define`** command (Example 3-25) to create the VM. You can also list the existing VMs with the **`virsh list`** command.

Example 3-25 Define the VM

```
[root@kvm1 vHMC2]# virsh define /var/lib/libvirt/images/vHMC2/vHMC2.xml
Domain vHMC2 defined from /var/lib/libvirt/images/vHMC2/vHMC2.xml

[root@kvm1 vHMC2]# virsh list --all
 Id    Name                           State
----------------------------------------------------
 19    HMC1                           running
 -     vHMC2                          shut off
```

Note: If you need to start the deployment of a vHMC, you must use the fresh image file extracted from `KVM_image.tar.gz`.

Do not use an image file that was used for a previous HMC deployment, because it might contain previous customization.

12. Start the VM with the **`virsh start`** command (Example 3-26) and check its status with the **`virsh list`** command.

Example 3-26 Start the VM

```
[root@kvm1 vHMC2]# virsh start vHMC2
Domain vHMC2 started

[root@kvm1 vHMC2]# virsh list --all
 Id    Name                           State
----------------------------------------------------
 19    HMC1                           running
 44    vHMC2                          running
```

13. You can now open the console, see the deployment progress from the virtual machine manager, and open the VM console, as shown in Figure 3-68.

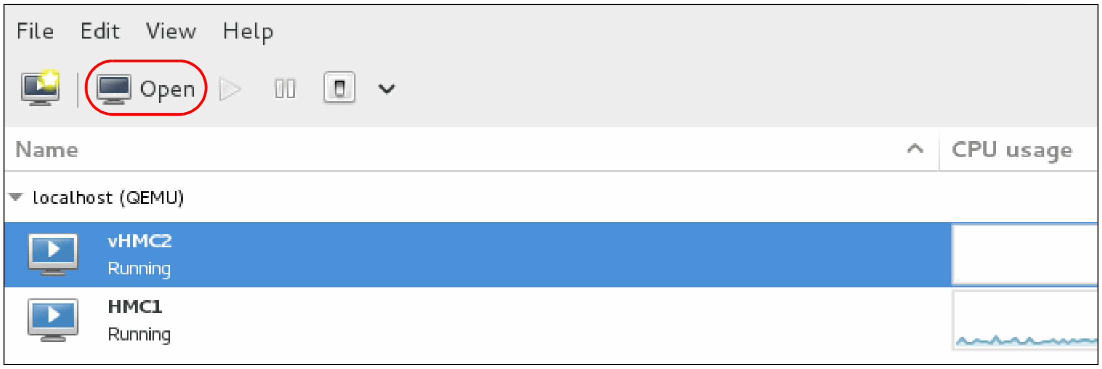
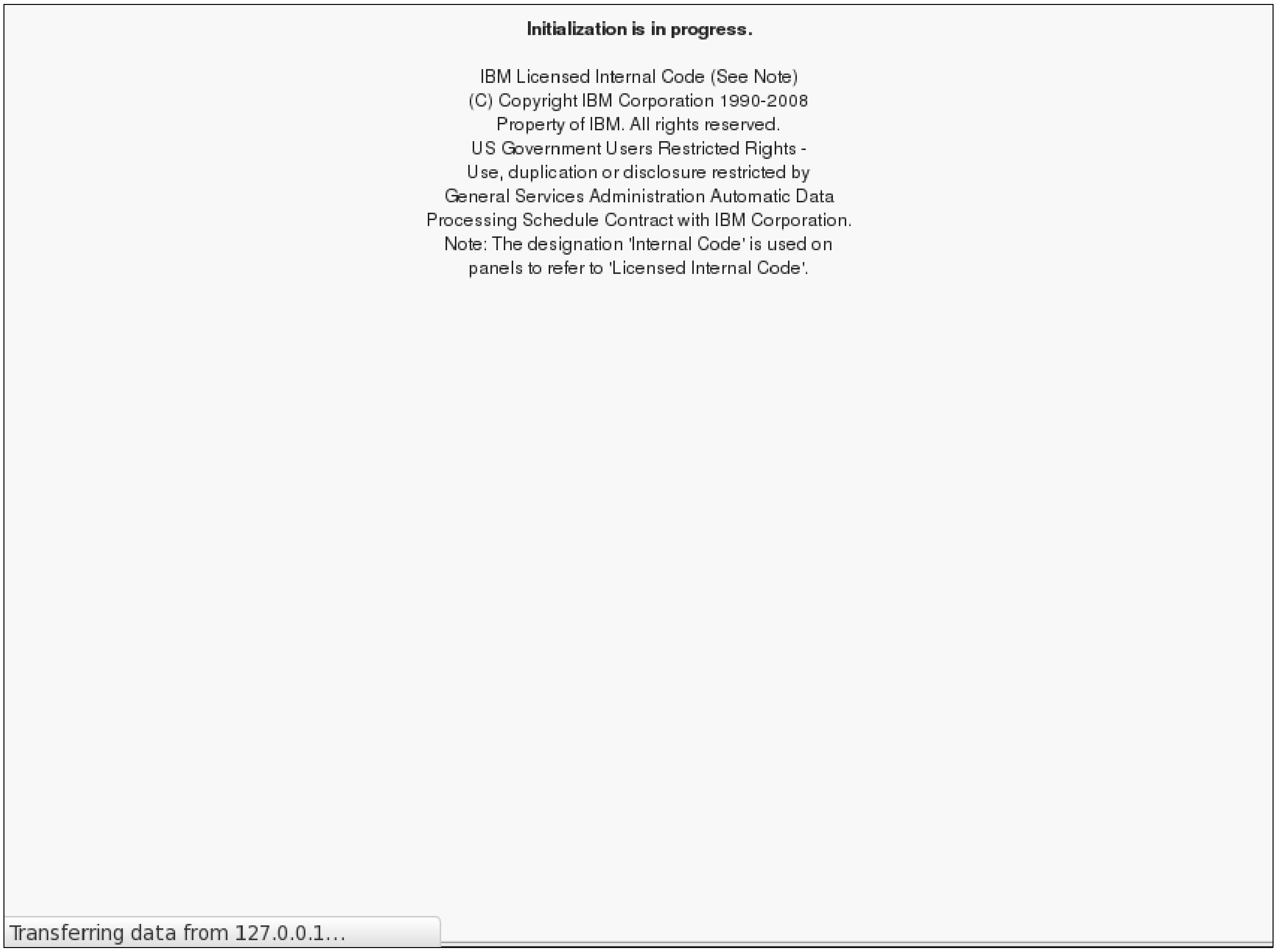


Figure 3-68 Virtual Machine Manager

The initialization starts and the HMC customization takes place, showing that it is in progress (Figure 3-69).



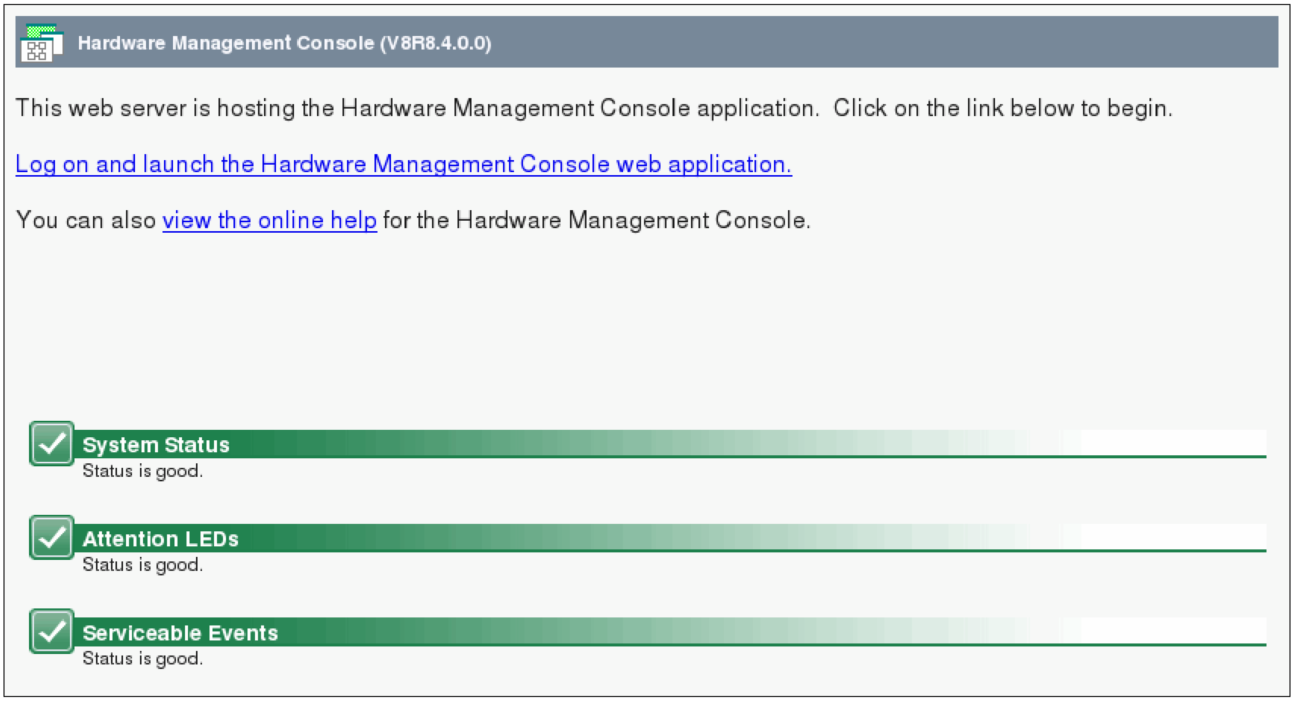
Initialization is in progress.

IBM Licensed Internal Code (See Note)
(C) Copyright IBM Corporation 1990-2008
Property of IBM. All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by
General Services Administration Automatic Data
Processing Schedule Contract with IBM Corporation.
Note: The designation 'Internal Code' is used on
panels to refer to 'Licensed Internal Code'.

Transferring data from 127.0.0.1...

Figure 3-69 KVM HMC deployment progress

14. After the deployment finishes, you can log in from the HMC console (Figure 3-70).



Hardware Management Console (V8R8.4.0.0)

This web server is hosting the Hardware Management Console application. Click on the link below to begin.

Log on and launch the Hardware Management Console web application.

You can also view the online help for the Hardware Management Console.

✓ System Status
Status is good.

✓ Attention LEDs
Status is good.

✓ Serviceable Events
Status is good.

Figure 3-70 HMC Welcome panel

The remote execution is also enabled, from the configuration deployment file, and ssh login is also available as shown in Example 3-27.

Example 3-27 ssh to the AE deployed HMC

```
[root@kvm1 vHMC2]# ssh hscroot@172.16.20.130
The authenticity of host '172.16.20.130 (172.16.20.130)' can't be established.
ECDSA key fingerprint is 36:1b:a3:5c:b7:ea:4b:e2:8d:11:ea:36:f9:27:22:ab.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.20.130' (ECDSA) to the list of known hosts.
hscroot@172.16.20.130's password:
Last login: Tue Nov 10 16:21:06 2015 from 172.16.20.115
hscroot@vHMC2:~>
```

15. After the vHMC is started, you might need to adjust the date, time, and time zone. To do this, use the **chhmc** command (Example 3-28) and reboot the HMC as requested.

Example 3-28 Change date and time from the command line

```
hscroot@vHMC2:~> chhmc -c date -s modify --datetime 110920262015 --clock local
--timezone 'America/New_York'
The Customize Date/Time request completed successfully. Please reboot the HMC.

hscroot@vHMC2:~> hmcshutdown -r -t now
```

After the rebooting, you can proceed with further tasks.

Note: For *Activation Engine* problem determination, look at the /var/hsc/log/AE.log file after the vHMC is booted by using a *Restricted Shell Terminal* from the HMC Management panel.

Advanced AE deployment

This section provides an example of `domain.xml` (`vHMC2.xml`) and `vHMC-Conf.xml` files, with two NICs, with specific MAC addresses. The steps and commands to deploy the vHMC are the same as in “Simple AE deployment” on page 212.

Example 3-29 shows a domain file with two NICs with customized MAC addresses.

Example 3-29 Domain XML file with MAC addresses

```
<domain type='kvm'>
  <name>vHMC2</name>
  <uuid></uuid>
  <memory unit='KiB'>4194304</memory>
  <currentMemory unit='KiB'>4194304</currentMemory>
  <vcpu placement='static'>2</vcpu>
  <os>
    <type arch='x86_64' machine='rhel6.3.0'>hvm</type>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='cdrom'>
      <target dev='hdc' bus='ide'/>
      <readonly/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='raw' cache='none'/>
      <source file='/var/lib/libvirt/images/vHMC2/disk1.img'/>
      <target dev='vda' bus='virtio'/>
    </disk>
    <disk type='file' device='floppy'>
      <driver name='qemu' type='raw' cache='default'/>
      <source file='/var/lib/libvirt/images/vHMC2/Floppy.img'/>
      <target dev='fda' bus='fdc'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <interface type='bridge'>
      <mac address='52:54:00:f7:57:17'/>
      <source bridge='br0'/>
      <target dev='vnet0'/>
      <model type='virtio'/>
    </interface>
    <interface type='bridge'>
      <mac address='52:54:00:f7:57:18'/>
      <source bridge='br1'/>
      <target dev='vnet1'/>
      <model type='virtio'/>
    </interface>
    <serial type='pty'>
      <target port='0'/>
    </serial>
    <console type='pty'>
      <target type='serial' port='0'/>
    </console>
    <input type='mouse' bus='ps2'/>
    <graphics type='vnc' port='-1' autoport='yes'/>
    <video>
      <model type='vga'/>
    </video>
    <memballoon model='virtio'>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
    </memballoon>
  </devices>
</domain>
```

Example 3-30 shows the matching `vHMC-Conf.xml` file to customize the vHMC with the AE.

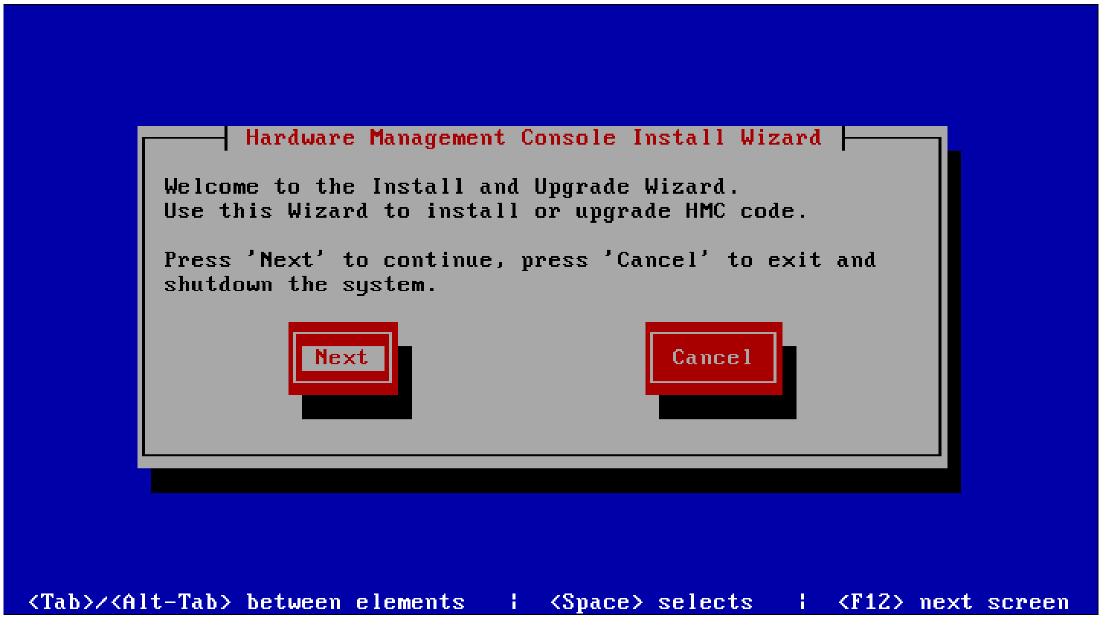
Example 3-30 vHMC-Conf.xml file with MAC addresses

```
<vHMC-Configuration>
        <LicenseAgreement>
        </LicenseAgreement>
        <AcceptLicense>Yes</AcceptLicense>
        <Locale>en_US.UTF-8</Locale>
        <SetupWizard>No</SetupWizard>
        <SetupCallHomeWizard>No</SetupCallHomeWizard>
        <SetupKeyboard>No</SetupKeyboard>
        <Ethernet>
                <Enable>yes</Enable>
                <MACAddr>52:54:00:f7:57:17</MACAddr>
                <IPVersion>IPV4</IPVersion>
                <IPv4NetworkType>static</IPv4NetworkType>
                <IPv4Address>172.16.20.130</IPv4Address>
                <IPv4Netmask>255.255.252.0</IPv4Netmask>
                <IPv4Gateway>172.16.20.1</IPv4Gateway>
                <IPv6NetworkType></IPv6NetworkType>
                <IPv6Address></IPv6Address>
                <IPv6Gateway></IPv6Gateway>
                <Hostname>vHMC2</Hostname>
                <Domain>itso.ibm.com</Domain>
                <DNSServers></DNSServers>
                <Firewall>
                        <PEGASUS>Enabled</PEGASUS>
                        <RPD>Enabled</RPD>
                        <FCS>Enabled</FCS>
                        <I5250>Enabled</I5250>
                        <PING>Enabled</PING>
                        <L2TP>Disabled</L2TP>
                        <SLP>Enabled</SLP>
                        <RSCT>Enabled</RSCT>
                        <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
                        <SSH>Enabled</SSH>
                        <VTTY>Enabled</VTTY>
                        <NTP>Disabled</NTP>
                        <SNMPTraps>Disabled</SNMPTraps>
                        <SNMPAgents>Disabled</SNMPAgents>
                </Firewall>
        </Ethernet>
        <Ethernet>
                <Enable>yes</Enable>
                <MACAddr>52:54:00:f7:57:18</MACAddr>
                <IPVersion>IPV4</IPVersion>
                <IPv4NetworkType>static</IPv4NetworkType>
                <IPv4Address>10.1.0.130</IPv4Address>
                <IPv4Netmask>255.255.240.0</IPv4Netmask>
                <IPv4Gateway></IPv4Gateway>
                <IPv6NetworkType></IPv6NetworkType>
                <IPv6Address></IPv6Address>
                <IPv6Gateway></IPv6Gateway>
                <Hostname></Hostname>
                <Domain></Domain>
                <DNSServers></DNSServers>
                <Firewall>
                        <PEGASUS>Enabled</PEGASUS>
                        <RPD>Enabled</RPD>
                        <FCS>Enabled</FCS>
                        <I5250>Enabled</I5250>
                        <PING>Enabled</PING>
                        <L2TP>Disabled</L2TP>
                        <SLP>Enabled</SLP>
                        <RSCT>Enabled</RSCT>
                        <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
                        <SSH>Enabled</SSH>
                        <VTTY>Enabled</VTTY>
                        <NTP>Disabled</NTP>
                        <SNMPTraps>Disabled</SNMPTraps>
                        <SNMPAgents>Disabled</SNMPAgents>
                </Firewall>
        </Ethernet>
</vHMC-Configuration>
```

3.3 HMC Install Wizard

First see 3.1.1, “Physical HMC installation” on page 156, then complete the following steps:

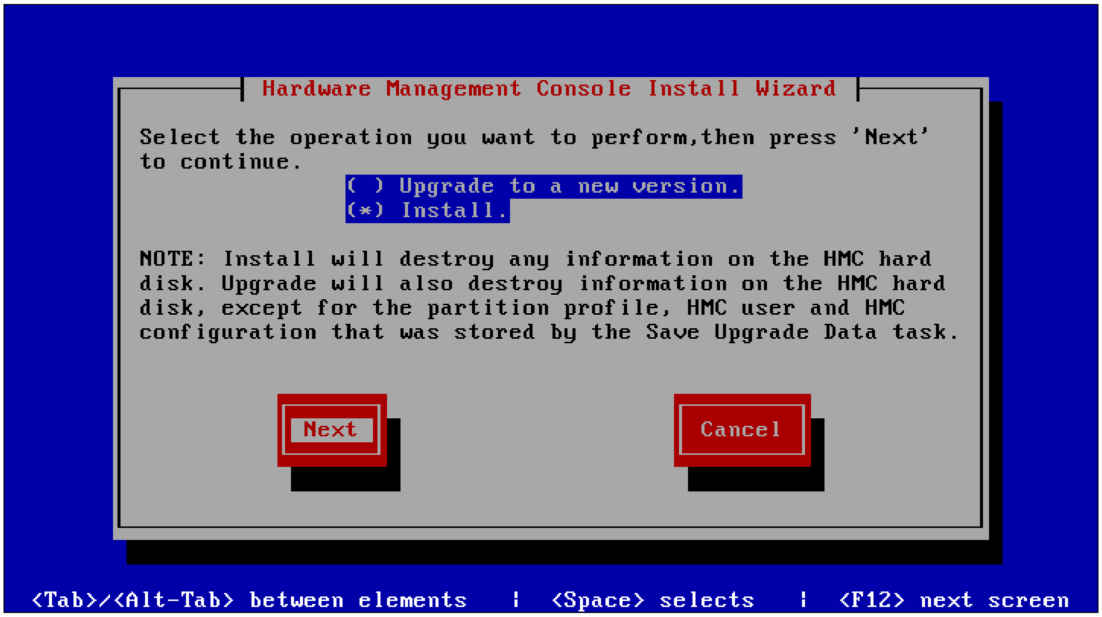
1. Select **Next** (Figure 3-71).



```
Hardware Management Console Install Wizard

Welcome to the Install and Upgrade Wizard.
Use this Wizard to install or upgrade HMC code.

Press 'Next' to continue, press 'Cancel' to exit and
shutdown the system.

        Next                        Cancel

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Figure 3-71 HMC Install Wizard

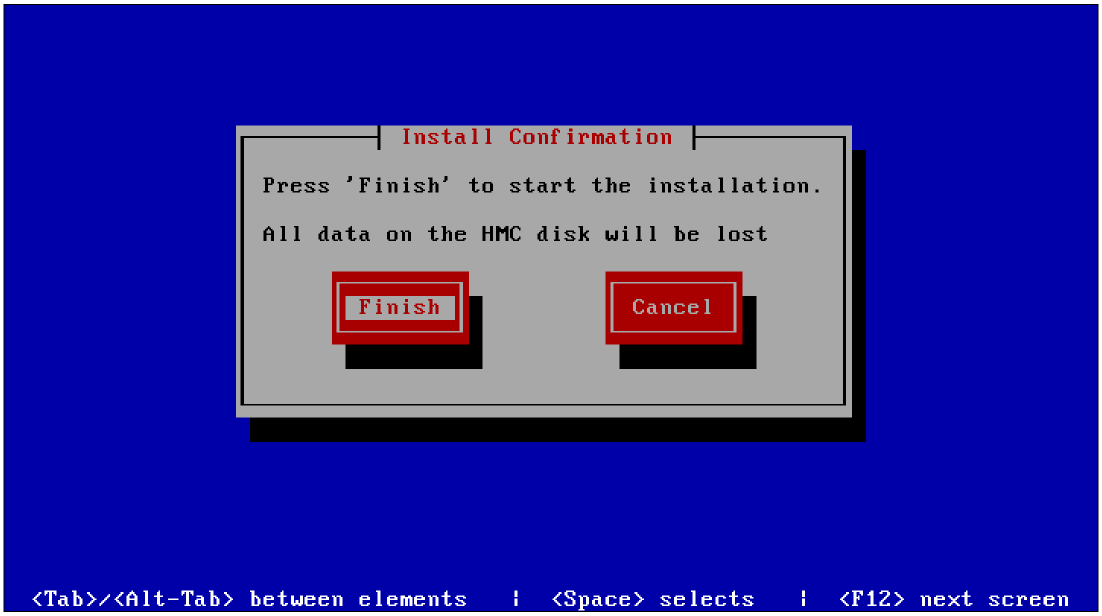
2. Select **Install**, and use the tab key to select **Next** (Figure 3-72).



```
Hardware Management Console Install Wizard

Select the operation you want to perform,then press 'Next'
to continue.
                ( ) Upgrade to a new version.
                (*) Install.

NOTE: Install will destroy any information on the HMC hard
disk. Upgrade will also destroy information on the HMC hard
disk, except for the partition profile, HMC user and HMC
configuration that was stored by the Save Upgrade Data task.

        Next                           Cancel

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Figure 3-72 HMC Install Wizard selection

3. Select **Finish** to confirm the installation (Figure 3-73).

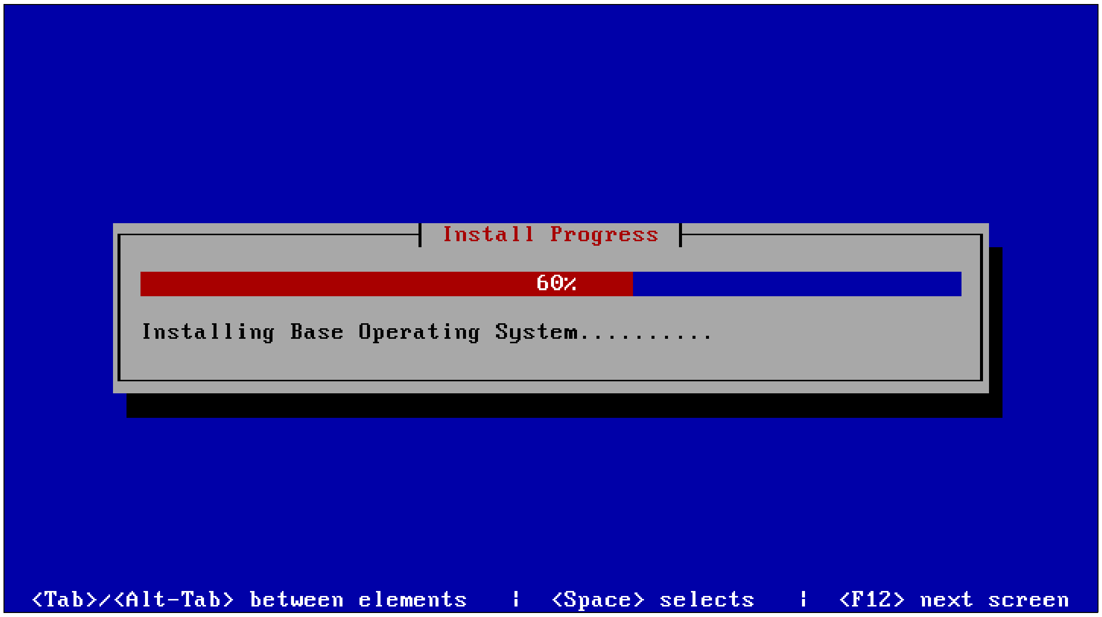


```
Install Confirmation

Press 'Finish' to start the installation.

All data on the HMC disk will be lost
```

Finish
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 3-73 Confirm installation

The installation progress is shown on the console (Figure 3-74).

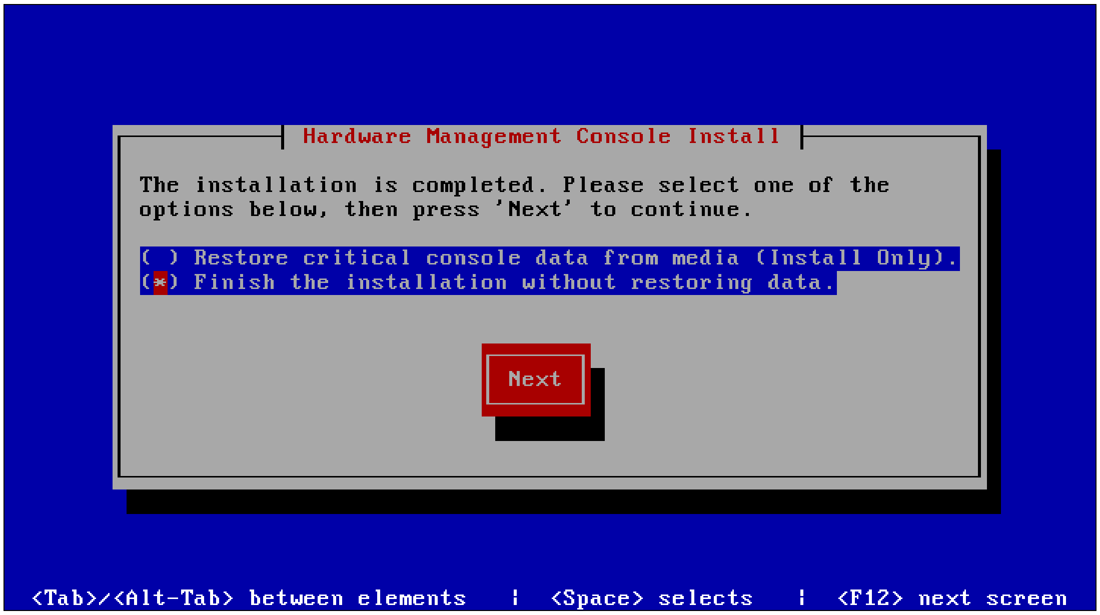


```
Install Progress

60%

Installing Base Operating System..........
```

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 3-74 HMC Wizard Installs Base Operating System

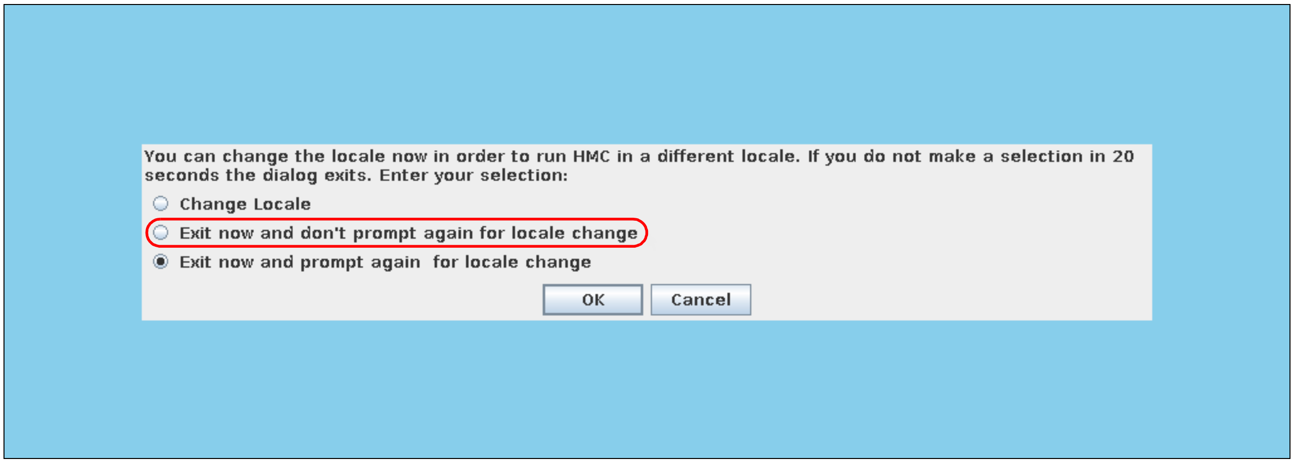
4. When the HMC Wizard finishes the installation (Figure 3-75), use the cursor to move to **Finish**, and then use Space or Tab to select **Next** and press Enter.



```
Hardware Management Console Install

The installation is completed. Please select one of the
options below, then press 'Next' to continue.

( ) Restore critical console data from media (Install Only).
(*) Finish the installation without restoring data.

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Figure 3-75 Finish Installation

5. The HMC now reboots, removing upgrade data, if any, and displays the locale selection dialog box. The default action is to display at every reboot and time out after 20 seconds. To change this action, select the appropriate entry from the three options (Figure 3-76). If you do not want to show this panel on subsequent boots, select the second option (**Exit now and don't prompt again for locale change**). Click **OK**.

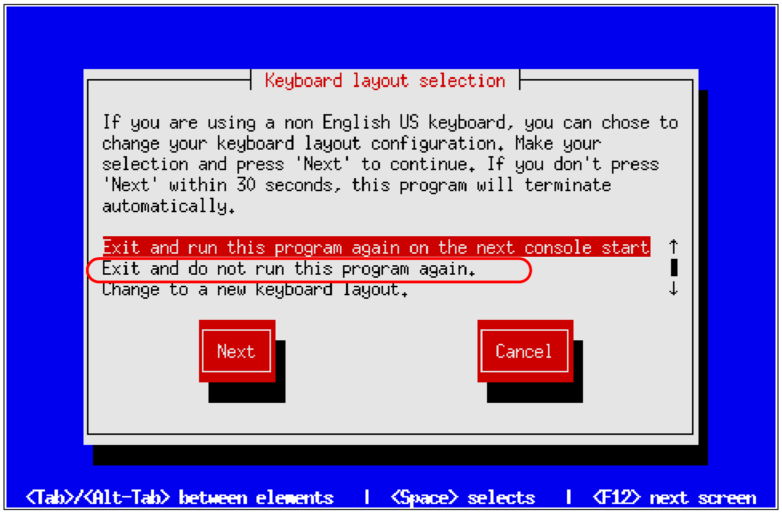


You can change the locale now in order to run HMC in a different locale. If you do not make a selection in 20 seconds the dialog exits. Enter your selection:

○ Change Locale
○ Exit now and don't prompt again for locale change
● Exit now and prompt again for locale change

Figure 3-76 Change the HMC locale

6. The Keyboard layout selection panel (Figure 3-77) allows for a non English US keyboard to be selected. The panel times out after 30 seconds if no selection is made. If you do not want to get this panel to be shown on subsequent boots, select the second option. Then, select **Next**.



Keyboard layout selection

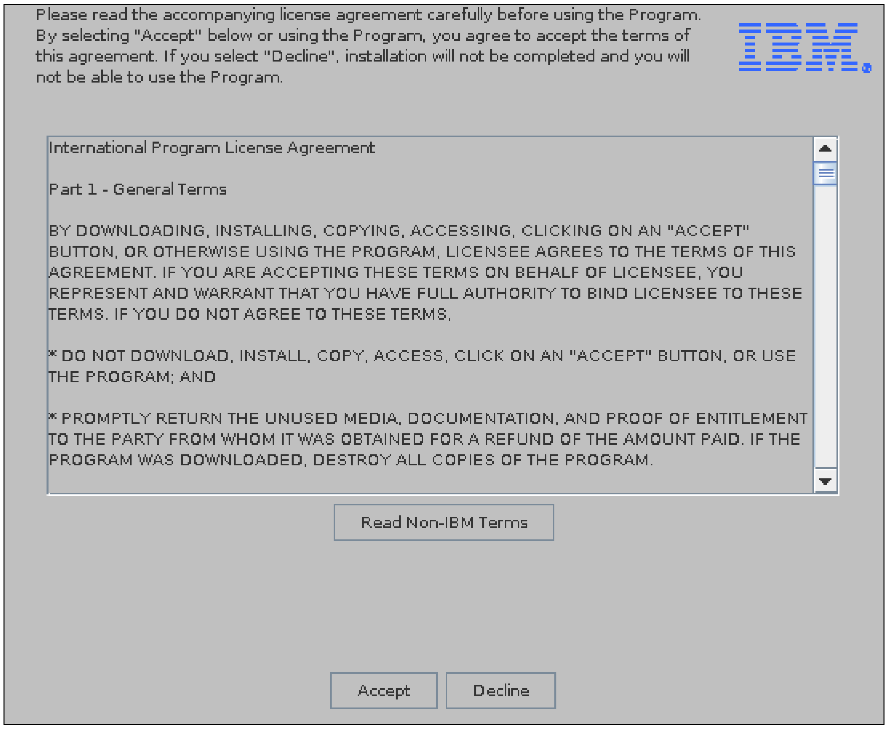
If you are using a non English US keyboard, you can chose to change your keyboard layout configuration. Make your selection and press 'Next' to continue. If you don't press 'Next' within 30 seconds, this program will terminate automatically.

Exit and run this program again on the next console start
[✓ Exit and do not run this program again.]
Change to a new keyboard layout.

Next
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 3-77 Keyboard layout selection

7. Read the license agreement, and click **Accept** (Figure 3-78).



Please read the accompanying license agreement carefully before using the Program. By selecting "Accept" below or using the Program, you agree to accept the terms of this agreement. If you select "Decline", installation will not be completed and you will not be able to use the Program.

International Program License Agreement

Part 1 - General Terms

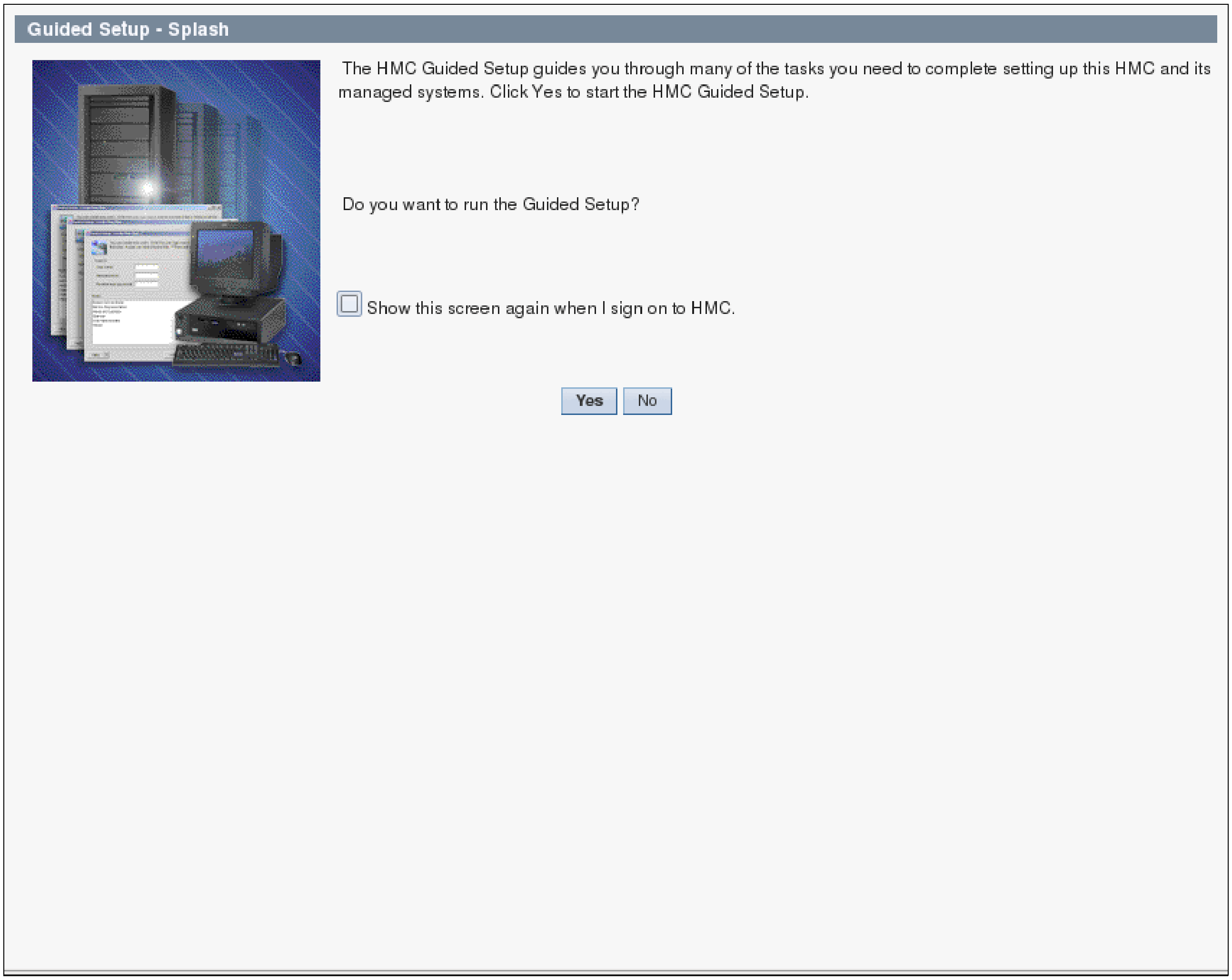
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND

* PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

Figure 3-78 Accept License window

8. In the Guided Setup window (Figure 3-79), *deselect* **Show this screen again** and click **Yes**.



Guided Setup - Splash

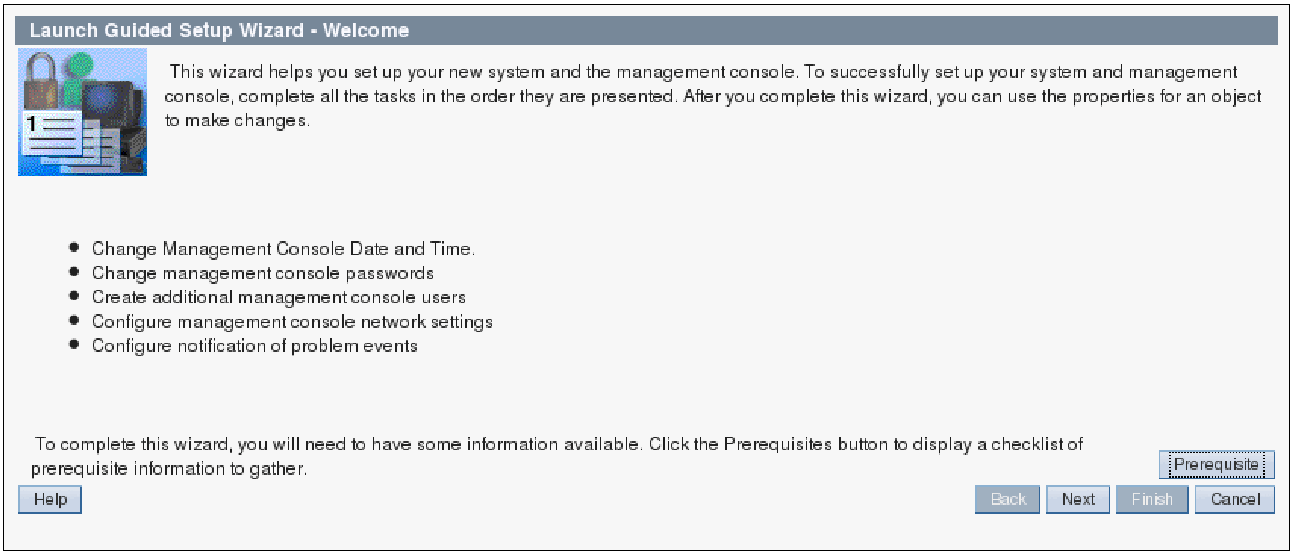
The HMC Guided Setup guides you through many of the tasks you need to complete setting up this HMC and its managed systems. Click Yes to start the HMC Guided Setup.

Do you want to run the Guided Setup?

☐ Show this screen again when I sign on to HMC.

Figure 3-79 Guided Setup - Splash window

9. In the Guided Setup Wizard (Figure 3-80), click **Next**.



Launch Guided Setup Wizard - Welcome

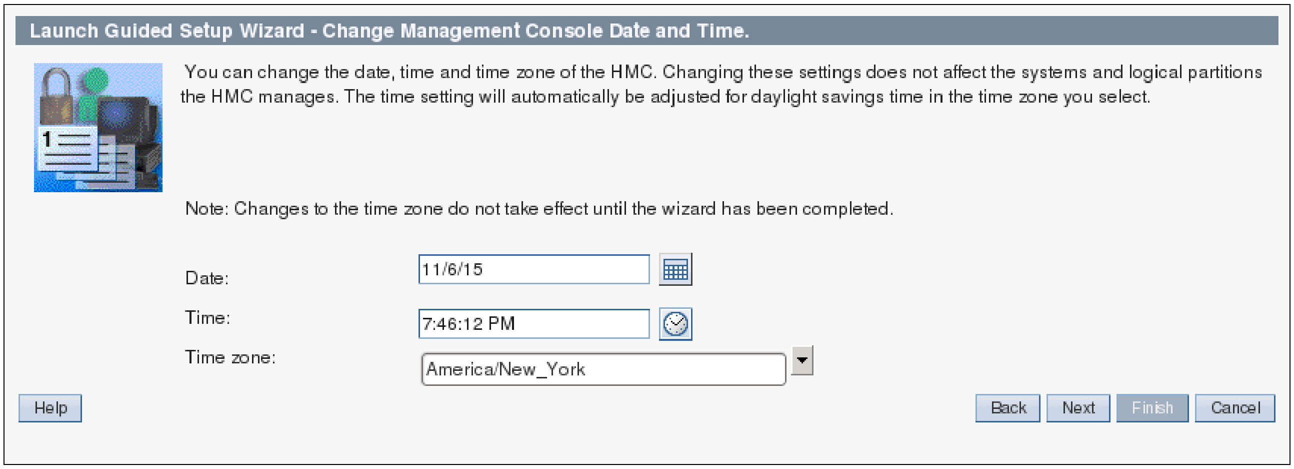
This wizard helps you set up your new system and the management console. To successfully set up your system and management console, complete all the tasks in the order they are presented. After you complete this wizard, you can use the properties for an object to make changes.

- Change Management Console Date and Time.
- Change management console passwords
- Create additional management console users
- Configure management console network settings
- Configure notification of problem events

To complete this wizard, you will need to have some information available. Click the Prerequisites button to display a checklist of prerequisite information to gather.

Figure 3-80 Setup wizard welcome

10. Change the date, time, and time zone, if necessary, and click **Finish** (Figure 3-81).



Launch Guided Setup Wizard - Change Management Console Date and Time.

You can change the date, time and time zone of the HMC. Changing these settings does not affect the systems and logical partitions the HMC manages. The time setting will automatically be adjusted for daylight savings time in the time zone you select.

Note: Changes to the time zone do not take effect until the wizard has been completed.

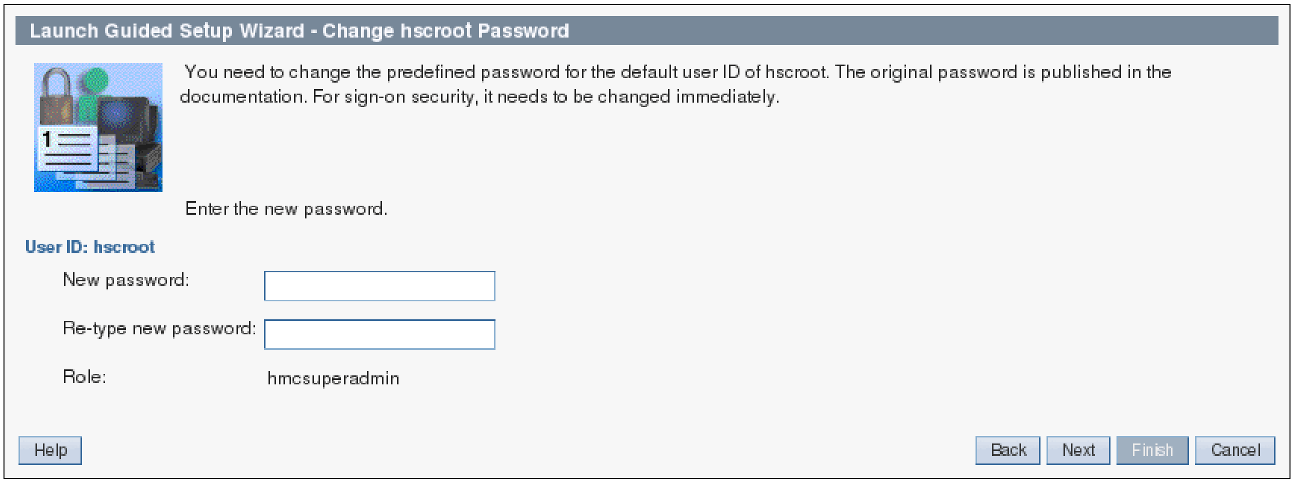
Date: 11/6/15

Time: 7:46:12 PM

Time zone: America/New_York

Figure 3-81 Change the date and time

11.Although you can change the `hscroot` password in the next panel (Figure 3-82), do not change it now for this example. You can change the `hscroot` password later. Click **Next**.



Launch Guided Setup Wizard - Change hscroot Password

You need to change the predefined password for the default user ID of hscroot. The original password is published in the documentation. For sign-on security, it needs to be changed immediately.

Enter the new password.

User ID: hscroot

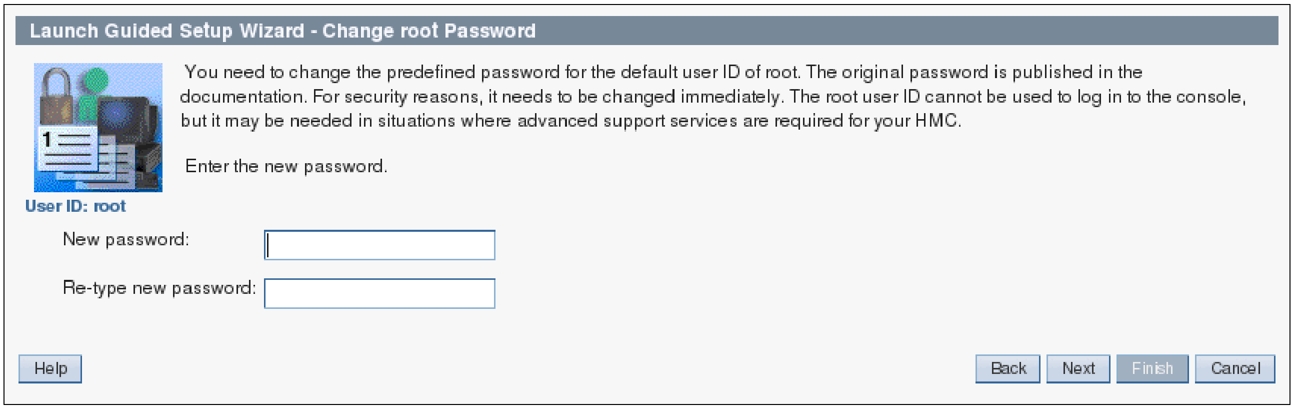
New password:

Re-type new password:

Role: hmcsuperadmin

Figure 3-82 The hscroot password change panel

12.Although you can change the `root` password in the next panel (Figure 3-83), do not change it now for this example. You can change the *`root`* password later. Click **Next**.



Launch Guided Setup Wizard - Change root Password

You need to change the predefined password for the default user ID of root. The original password is published in the documentation. For security reasons, it needs to be changed immediately. The root user ID cannot be used to log in to the console, but it may be needed in situations where advanced support services are required for your HMC.

Enter the new password.

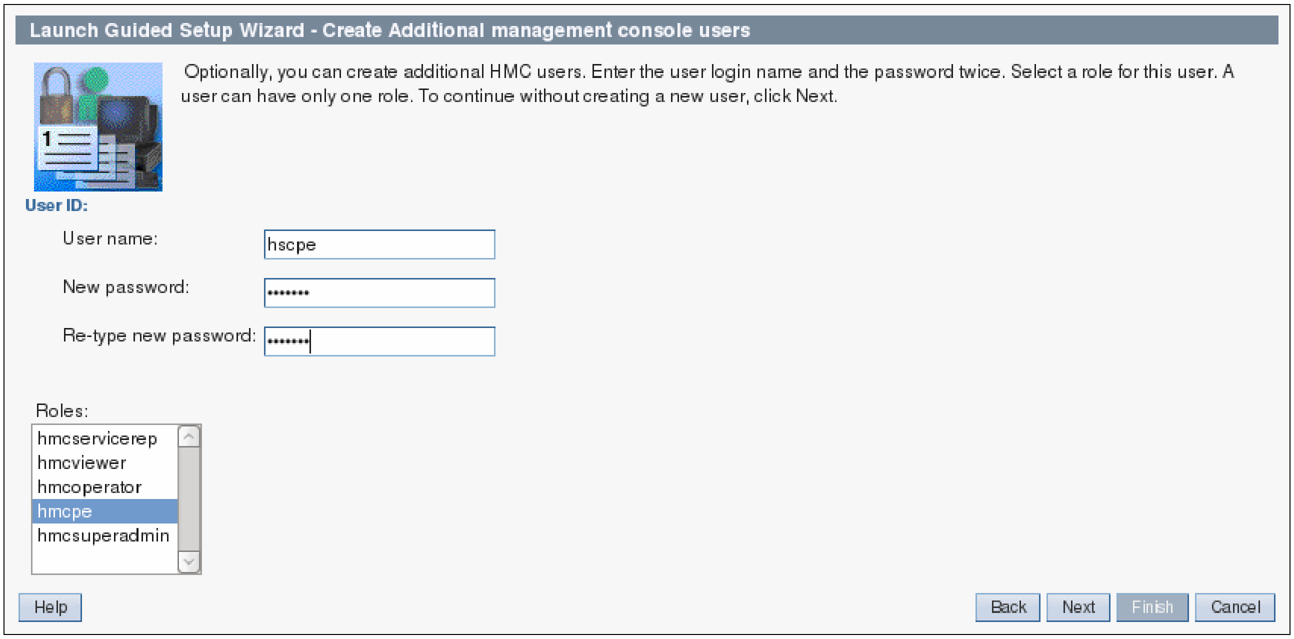
User ID: root

New password:

Re-type new password:

Figure 3-83 The root password change panel

13. You can create the `hscpe` user and `hmcpe` role with a password, as shown in Figure 3-84, and click **Next**.



Launch Guided Setup Wizard - Create Additional management console users

Optionally, you can create additional HMC users. Enter the user login name and the password twice. Select a role for this user. A user can have only one role. To continue without creating a new user, click Next.

User ID:

User name: hscpe

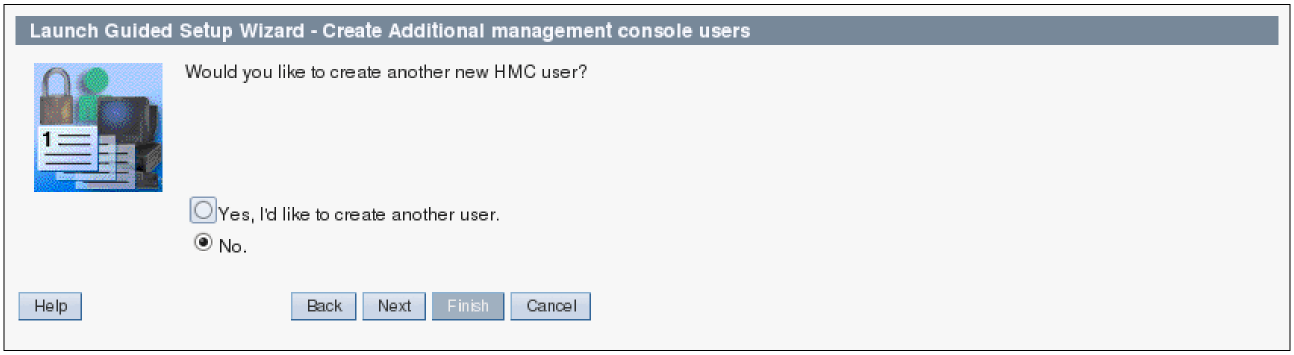
New password: •••••••

Re-type new password: •••••••

Roles: hmcservicerep, hmcviewer, hmcoperator, hmcpe (selected), hmcsuperadmin

Figure 3-84 Create an hscpe user

14. Although you can create additional HMC users in the next panel (Figure 3-85), do not create them now. Creating additional users can be done later. Click **Finish**.



Launch Guided Setup Wizard - Create Additional management console users

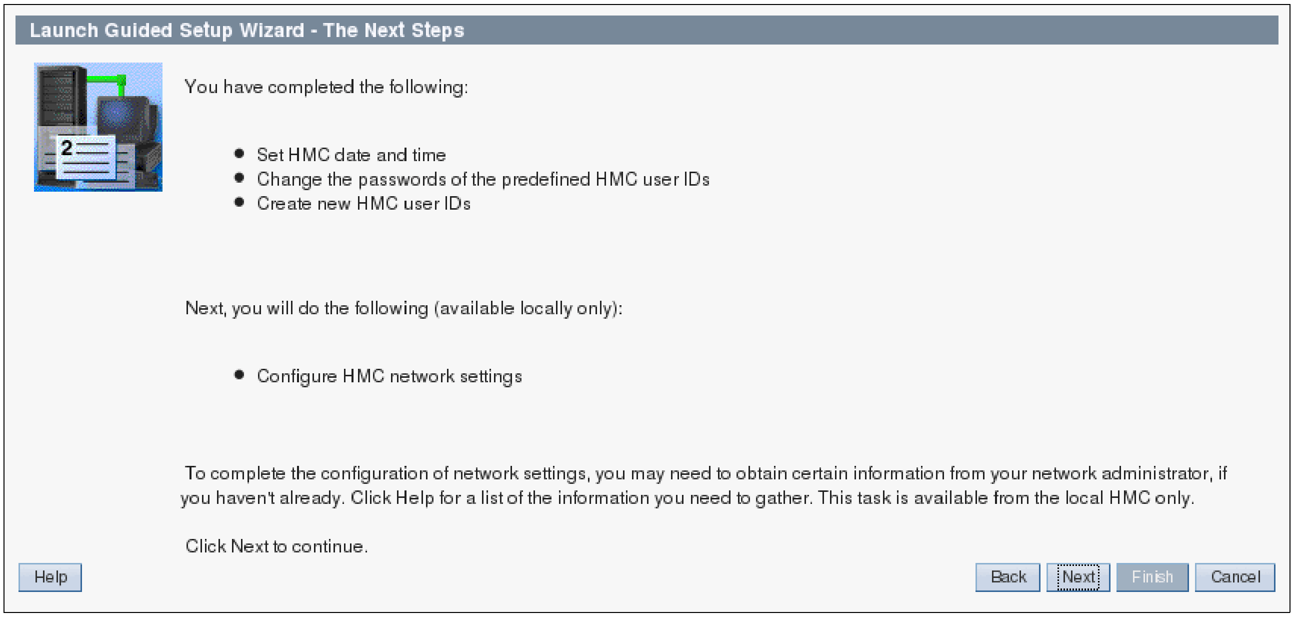
Would you like to create another new HMC user?

○ Yes, I'd like to create another user.

● No.

Figure 3-85 Create an extra user

15. In the next panel (Figure 3-86), click **Next**.



Launch Guided Setup Wizard - The Next Steps

You have completed the following:

- Set HMC date and time
- Change the passwords of the predefined HMC user IDs
- Create new HMC user IDs

Next, you will do the following (available locally only):

- Configure HMC network settings

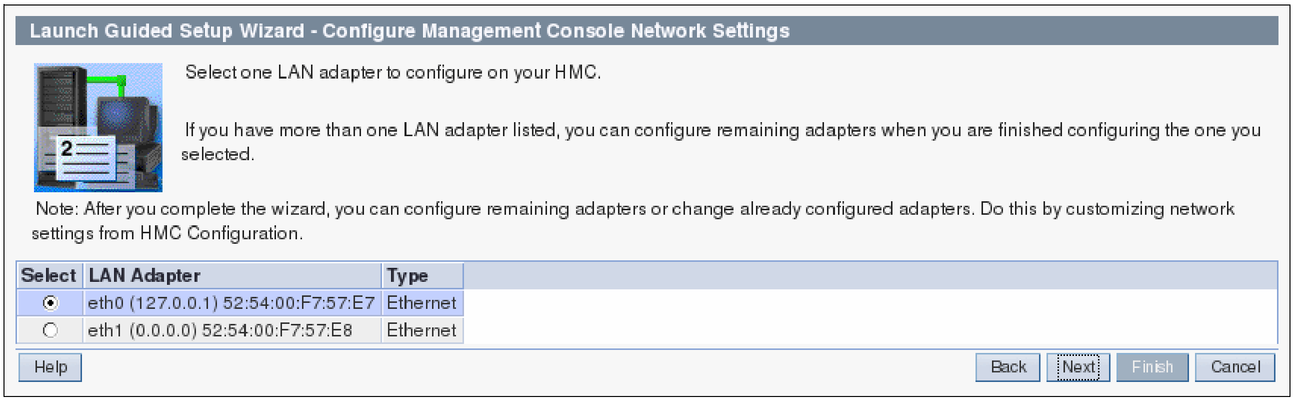
To complete the configuration of network settings, you may need to obtain certain information from your network administrator, if you haven't already. Click Help for a list of the information you need to gather. This task is available from the local HMC only.

Click Next to continue.

Figure 3-86 Date, time and user are set

16. You are now ready to configure the network (Figure 3-87). Click **Next** to configure eth0.

Notice which MAC addresses are listed. Be sure they match the proper networks. In case of a virtual HMC, you validate which NIC belongs to its appropriate Ethernet bridge.



Launch Guided Setup Wizard - Configure Management Console Network Settings

Select one LAN adapter to configure on your HMC.

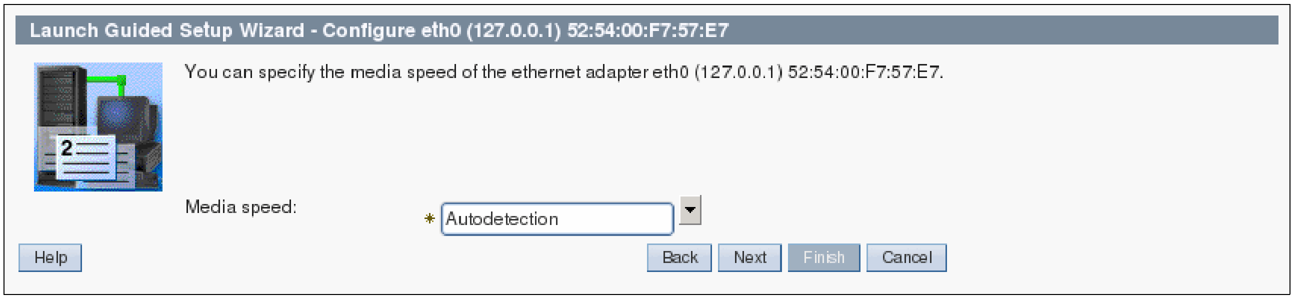
If you have more than one LAN adapter listed, you can configure remaining adapters when you are finished configuring the one you selected.

Note: After you complete the wizard, you can configure remaining adapters or change already configured adapters. Do this by customizing network settings from HMC Configuration.

Select	LAN Adapter	Type
●	eth0 (127.0.0.1) 52:54:00:F7:57:E7	Ethernet
○	eth1 (0.0.0.0) 52:54:00:F7:57:E8	Ethernet

Figure 3-87 Setup Wizard Network settings

17. For eth0, keep the **Autodetection** setting (Figure 3-88), and then click **Next**.



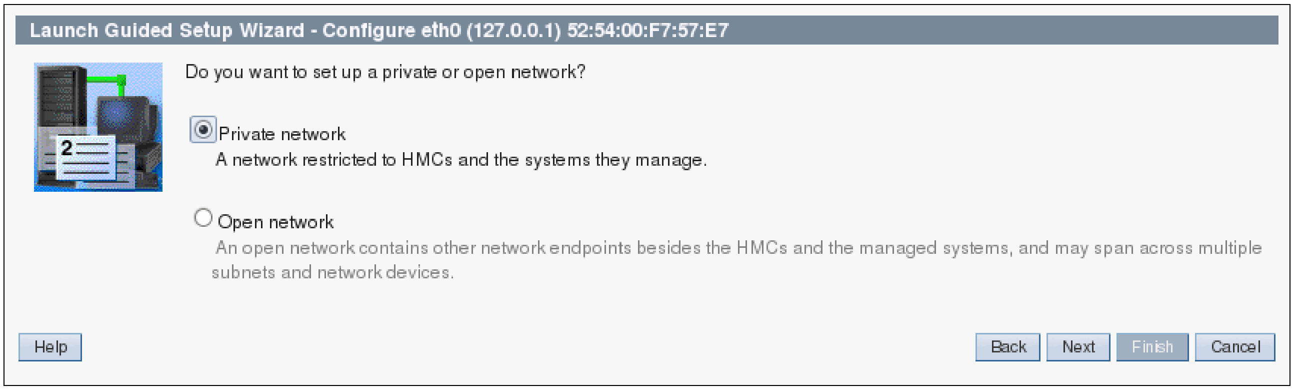
Launch Guided Setup Wizard - Configure eth0 (127.0.0.1) 52:54:00:F7:57:E7

You can specify the media speed of the ethernet adapter eth0 (127.0.0.1) 52:54:00:F7:57:E7.

Media speed: * Autodetection

Figure 3-88 eth0 speed selection

18. Select **Private network** for eth0 (Figure 3-89), and then click **Next**.



Launch Guided Setup Wizard - Configure eth0 (127.0.0.1) 52:54:00:F7:57:E7

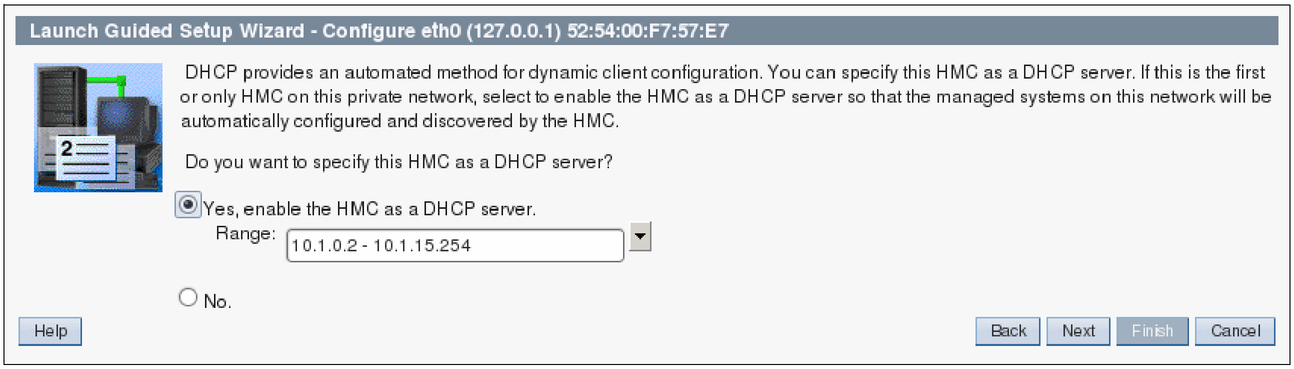
Do you want to set up a private or open network?

● Private network
A network restricted to HMCs and the systems they manage.

○ Open network
An open network contains other network endpoints besides the HMCs and the managed systems, and may span across multiple subnets and network devices.

Figure 3-89 Set network to private for eth0

19. Select a private IP range in the drop-down list (Figure 3-90), and then click **Next**.



Launch Guided Setup Wizard - Configure eth0 (127.0.0.1) 52:54:00:F7:57:E7

DHCP provides an automated method for dynamic client configuration. You can specify this HMC as a DHCP server. If this is the first or only HMC on this private network, select to enable the HMC as a DHCP server so that the managed systems on this network will be automatically configured and discovered by the HMC.

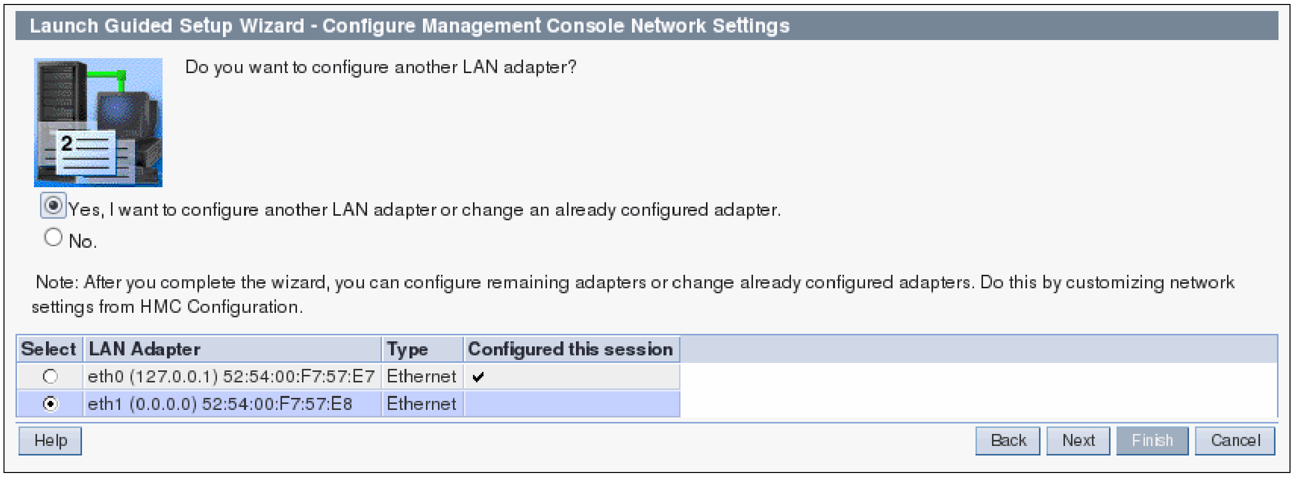
Do you want to specify this HMC as a DHCP server?

● Yes, enable the HMC as a DHCP server.
Range: 10.1.0.2 - 10.1.15.254

○ No.

Figure 3-90 Select the range for eth0

20. Select **Yes**, be sure **eth1** is selected, and then click **Next** (Figure 3-91).



Launch Guided Setup Wizard - Configure Management Console Network Settings

Do you want to configure another LAN adapter?

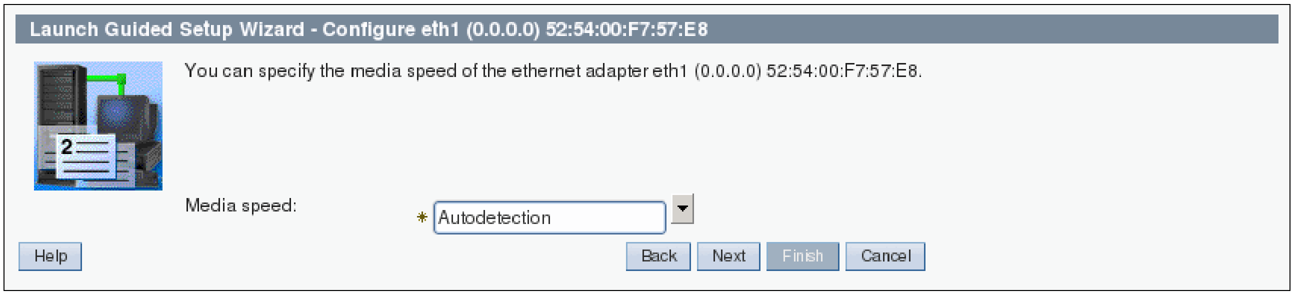
● Yes, I want to configure another LAN adapter or change an already configured adapter.
○ No.

Note: After you complete the wizard, you can configure remaining adapters or change already configured adapters. Do this by customizing network settings from HMC Configuration.

Select	LAN Adapter	Type	Configured this session
○	eth0 (127.0.0.1) 52:54:00:F7:57:E7	Ethernet	✓
●	eth1 (0.0.0.0) 52:54:00:F7:57:E8	Ethernet	

Figure 3-91 Select eth1 for configuration

21. Select **Autodetection** for eth1 (Figure 3-92) and click **Next**.



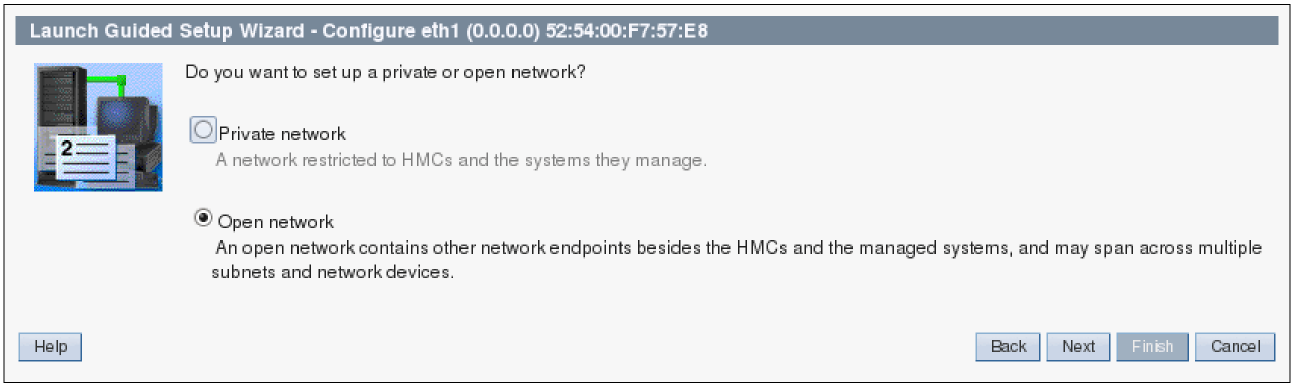
Launch Guided Setup Wizard - Configure eth1 (0.0.0.0) 52:54:00:F7:57:E8

You can specify the media speed of the ethernet adapter eth1 (0.0.0.0) 52:54:00:F7:57:E8.

Media speed: * Autodetection

Figure 3-92 Select Auto detection for eth1

22. Select eth1 to be an open network (Figure 3-93) and click **Next**.



Launch Guided Setup Wizard - Configure eth1 (0.0.0.0) 52:54:00:F7:57:E8

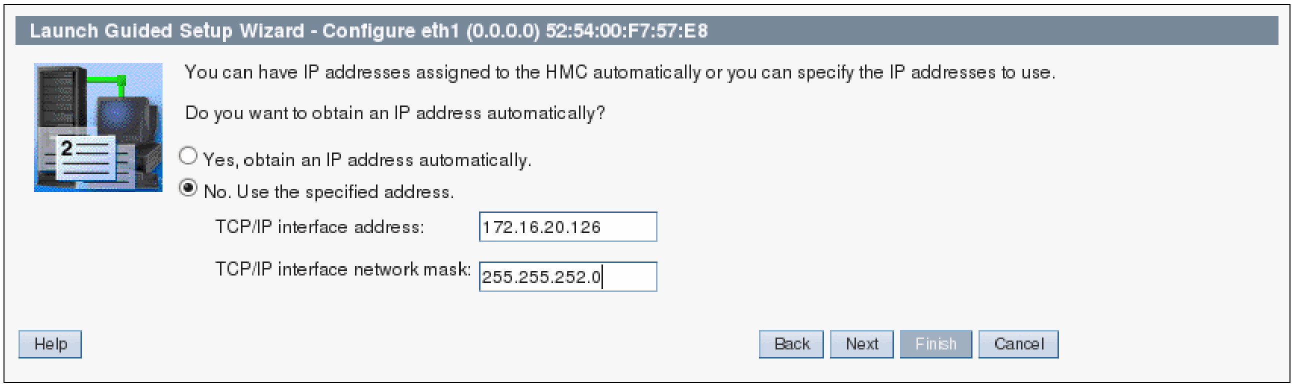
Do you want to set up a private or open network?

○ Private network
A network restricted to HMCs and the systems they manage.

● Open network
An open network contains other network endpoints besides the HMCs and the managed systems, and may span across multiple subnets and network devices.

Figure 3-93 eth1 is an open network

23. Select an IP address and subnet mask (Figure 3-94) and click **Next**.



Launch Guided Setup Wizard - Configure eth1 (0.0.0.0) 52:54:00:F7:57:E8

You can have IP addresses assigned to the HMC automatically or you can specify the IP addresses to use.

Do you want to obtain an IP address automatically?

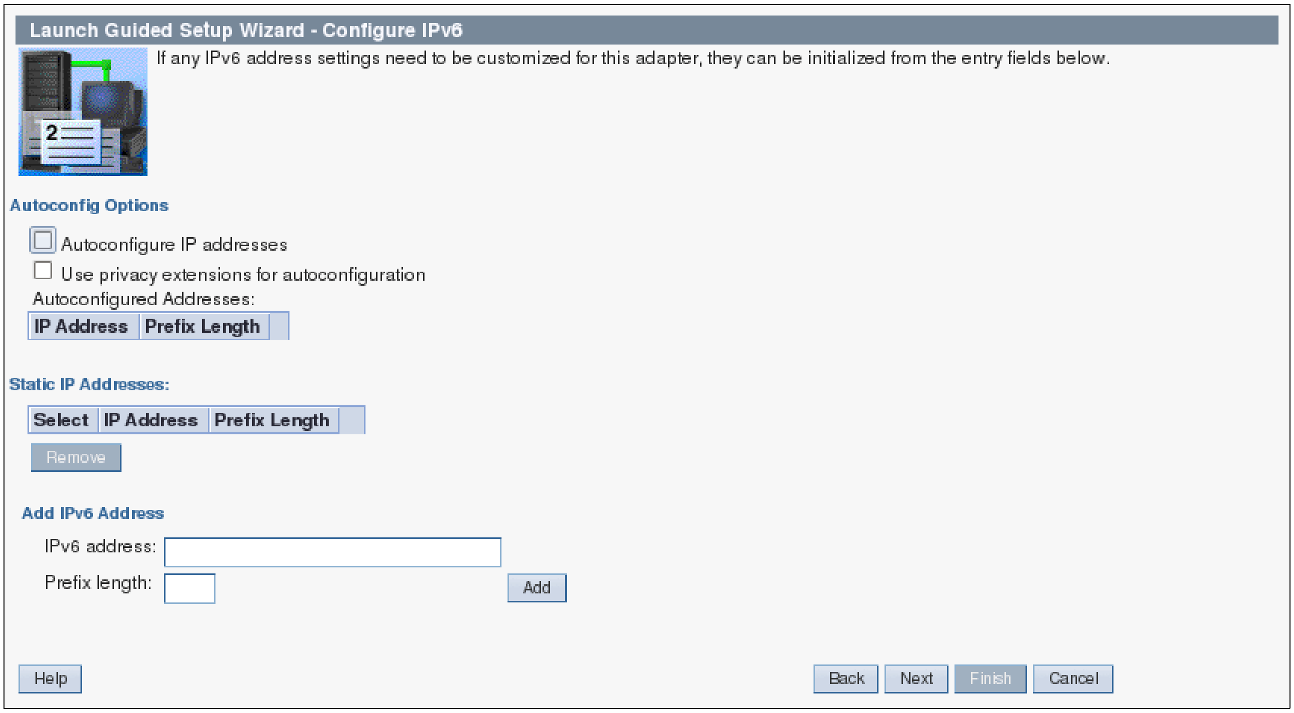
○ Yes, obtain an IP address automatically.
● No. Use the specified address.

TCP/IP interface address: 172.16.20.126

TCP/IP interface network mask: 255.255.252.0

Figure 3-94 Set an IP address for eth1

24. If no IPv6 configuration is required, click **Next** (Figure 3-95).



Launch Guided Setup Wizard - Configure IPv6

If any IPv6 address settings need to be customized for this adapter, they can be initialized from the entry fields below.

Autoconfig Options

☐ Autoconfigure IP addresses
☐ Use privacy extensions for autoconfiguration

Autoconfigured Addresses:

IP Address	Prefix Length

Static IP Addresses:

Select	IP Address	Prefix Length

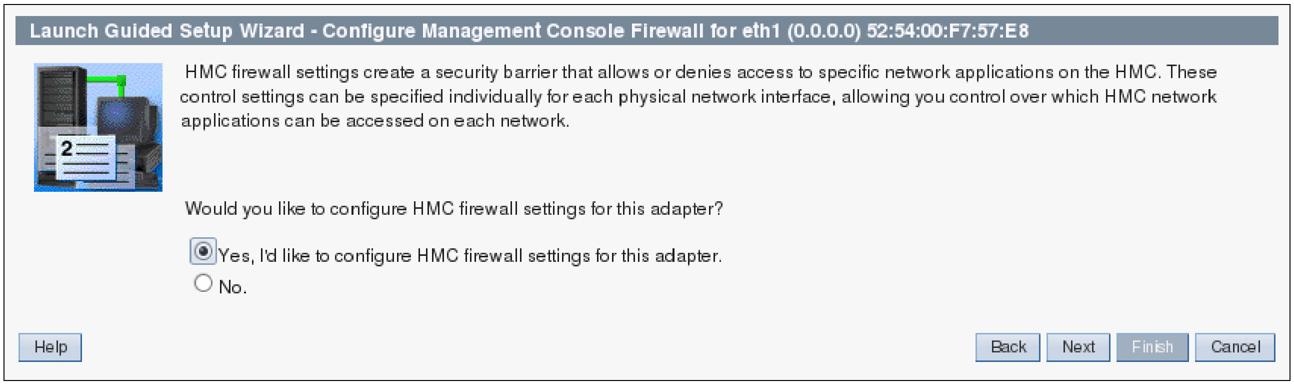
Add IPv6 Address

IPv6 address:

Prefix length:

Figure 3-95 IPv6 configuration

25. To configure the HMC firewall rules, select **Yes** (Figure 3-96) and click **Next**.



Launch Guided Setup Wizard - Configure Management Console Firewall for eth1 (0.0.0.0) 52:54:00:F7:57:E8

HMC firewall settings create a security barrier that allows or denies access to specific network applications on the HMC. These control settings can be specified individually for each physical network interface, allowing you control over which HMC network applications can be accessed on each network.

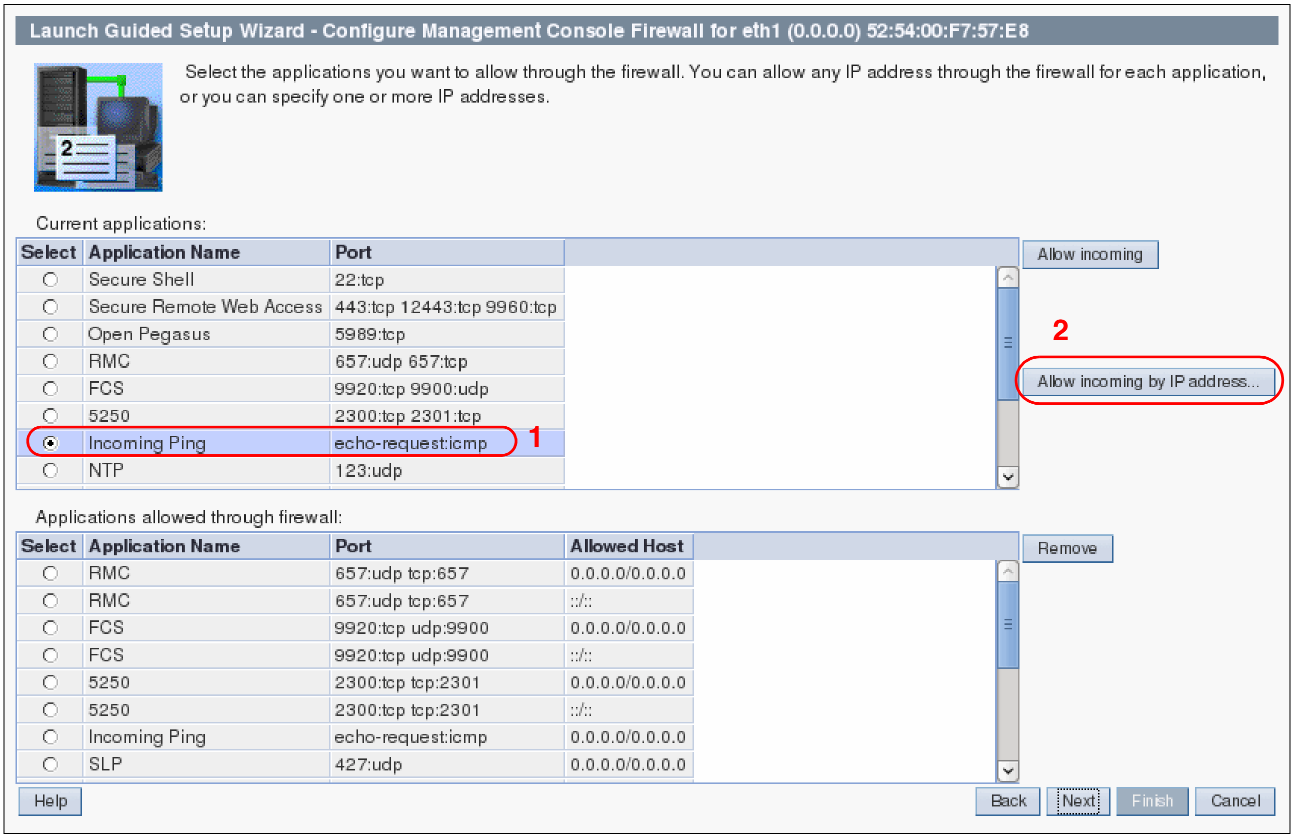
Would you like to configure HMC firewall settings for this adapter?

● Yes, I'd like to configure HMC firewall settings for this adapter.
○ No.

Figure 3-96 Firewall configuration on eth1

26. Add the appropriate applications to be allowed by the HMC's firewall on eth1 (Figure 3-97). The top box lists the application to be enabled. The bottom box lists the application that are already enabled. In the *Current applications* list, select an application, and then click **Allow incoming by IP address** to add it to the *Applications allowed through firewall* list. Repeat this process for each application you need.

> **Note:** To ease the remote administration of the HMC and managed systems later, add the **Secure Shell**, the **Secure Remote Web Access**, and the **Incoming Ping**.



Launch Guided Setup Wizard - Configure Management Console Firewall for eth1 (0.0.0.0) 52:54:00:F7:57:E8

Select the applications you want to allow through the firewall. You can allow any IP address through the firewall for each application, or you can specify one or more IP addresses.

Current applications:

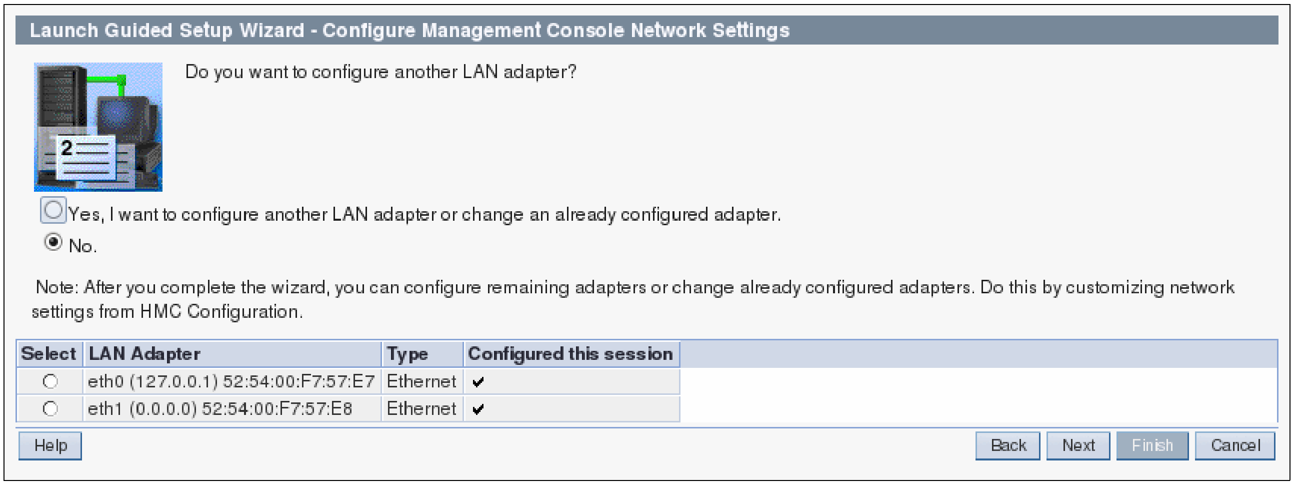
Select	Application Name	Port
○	Secure Shell	22:tcp
○	Secure Remote Web Access	443:tcp 12443:tcp 9960:tcp
○	Open Pegasus	5989:tcp
○	RMC	657:udp 657:tcp
○	FCS	9920:tcp 9900:udp
○	5250	2300:tcp 2301:tcp
●	Incoming Ping	echo-request:icmp
○	NTP	123:udp

Applications allowed through firewall:

Select	Application Name	Port	Allowed Host
○	RMC	657:udp tcp:657	0.0.0.0/0.0.0.0
○	RMC	657:udp tcp:657	::/::
○	FCS	9920:tcp udp:9900	0.0.0.0/0.0.0.0
○	FCS	9920:tcp udp:9900	::/::
○	5250	2300:tcp tcp:2301	0.0.0.0/0.0.0.0
○	5250	2300:tcp tcp:2301	::/::
○	Incoming Ping	echo-request:icmp	0.0.0.0/0.0.0.0
○	SLP	427:udp	0.0.0.0/0.0.0.0

Figure 3-97 Firewall settings for incoming applications

27. You have now completed the network settings. Choose not to configure any other adapter (Figure 3-98), and then click **Next**.



Launch Guided Setup Wizard - Configure Management Console Network Settings

Do you want to configure another LAN adapter?

○ Yes, I want to configure another LAN adapter or change an already configured adapter.

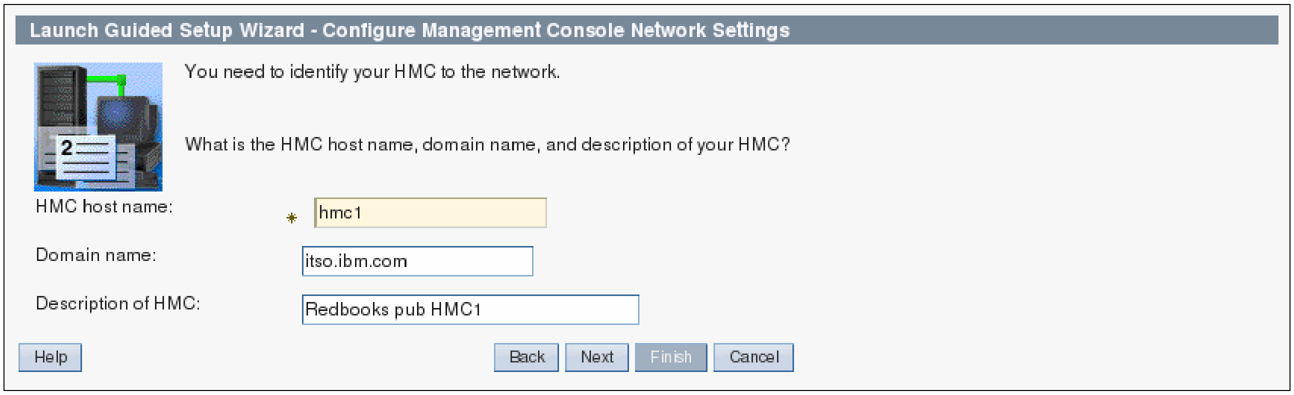
● No.

Note: After you complete the wizard, you can configure remaining adapters or change already configured adapters. Do this by customizing network settings from HMC Configuration.

Select	LAN Adapter	Type	Configured this session
○	eth0 (127.0.0.1) 52:54:00:F7:57:E7	Ethernet	✓
○	eth1 (0.0.0.0) 52:54:00:F7:57:E8	Ethernet	✓

Figure 3-98 HMC Network Settings finished

28. Set the name for this HMC (Figure 3-99). A preferred approach is to specify a domain name and a description, and then click **Next** to proceed.



Launch Guided Setup Wizard - Configure Management Console Network Settings

You need to identify your HMC to the network.

What is the HMC host name, domain name, and description of your HMC?

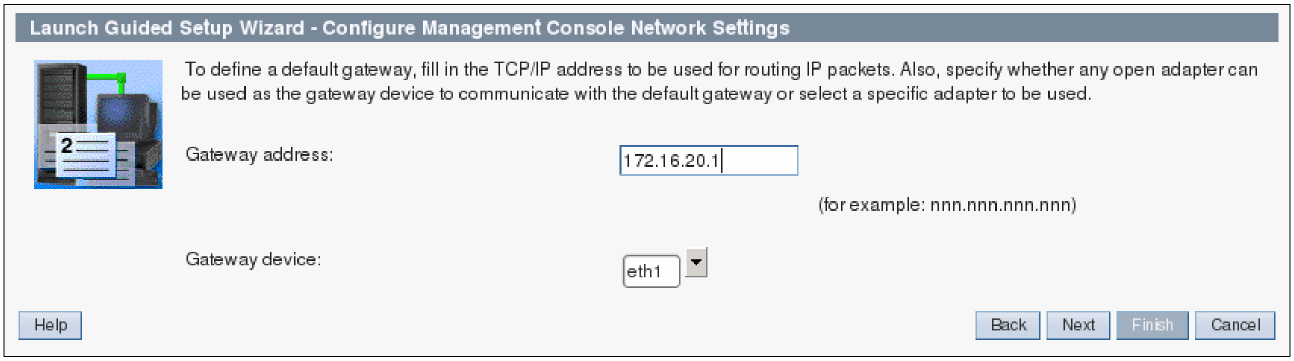
HMC host name: * hmc1

Domain name: itso.ibm.com

Description of HMC: Redbooks pub HMC1

Figure 3-99 Set the HMC host name

29. Choose the default gateway, select the appropriate device, and click **Next** (Figure 3-100).



Launch Guided Setup Wizard - Configure Management Console Network Settings

To define a default gateway, fill in the TCP/IP address to be used for routing IP packets. Also, specify whether any open adapter can be used as the gateway device to communicate with the default gateway or select a specific adapter to be used.

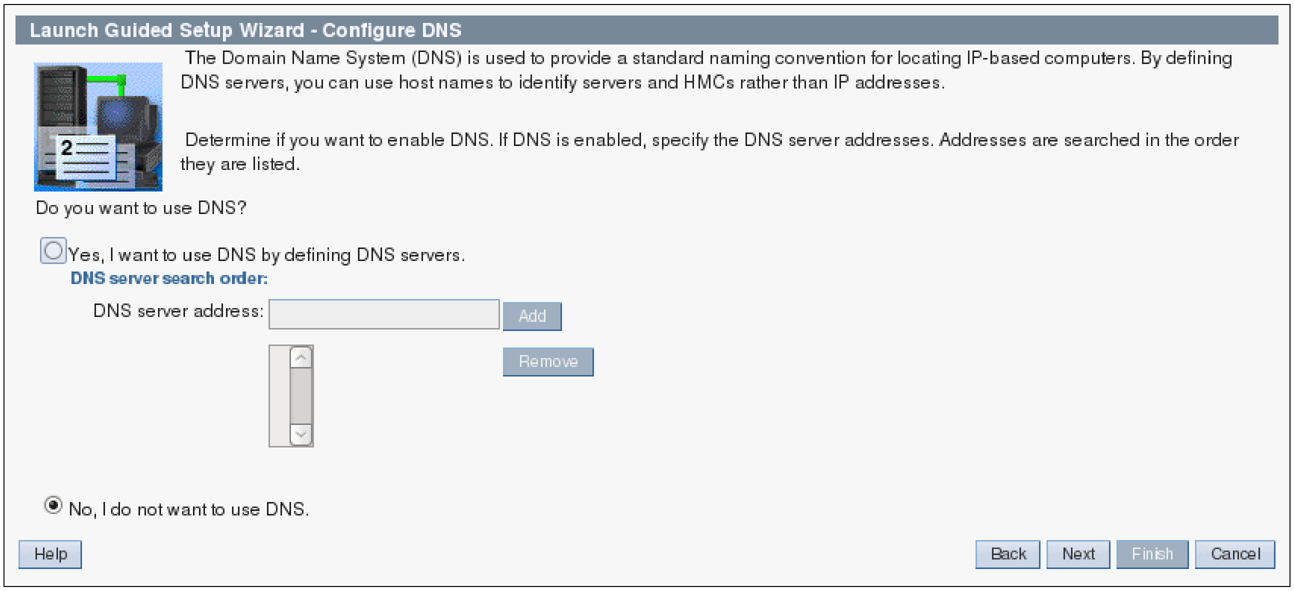
Gateway address: 172.16.20.1

(for example: nnn.nnn.nnn.nnn)

Gateway device: eth1

Figure 3-100 HMC default gateway

30. Although in the Configure DNS panel (Figure 3-101), you may specify the DNS appropriate to your environment, in this example, no DNS is configured so select **No** and click **Next**.



Launch Guided Setup Wizard - Configure DNS

The Domain Name System (DNS) is used to provide a standard naming convention for locating IP-based computers. By defining DNS servers, you can use host names to identify servers and HMCs rather than IP addresses.

Determine if you want to enable DNS. If DNS is enabled, specify the DNS server addresses. Addresses are searched in the order they are listed.

Do you want to use DNS?

○ Yes, I want to use DNS by defining DNS servers.

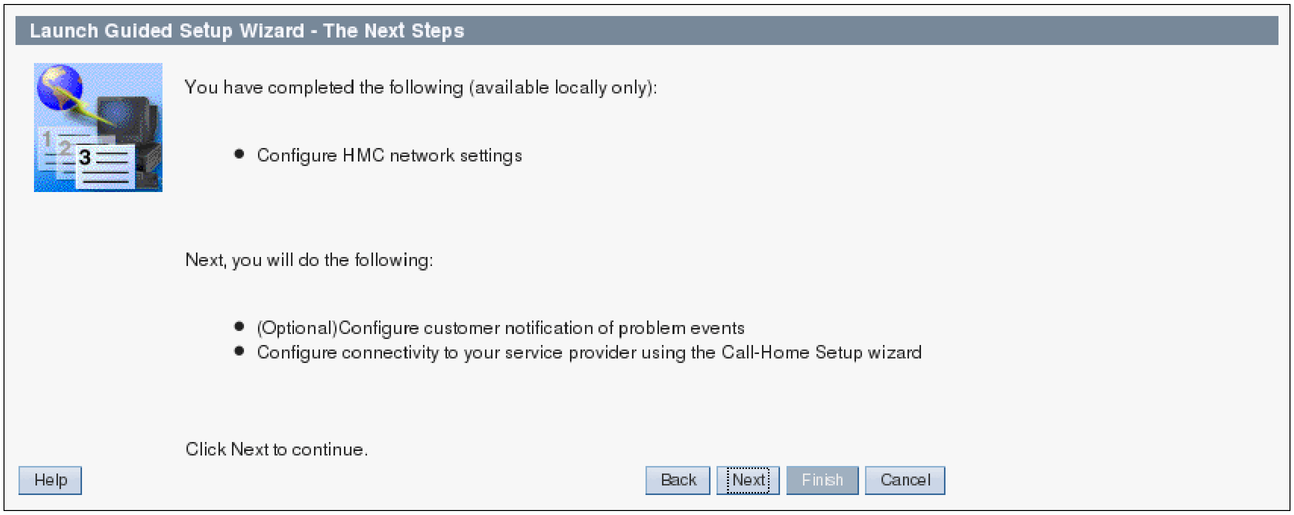
DNS server search order:

DNS server address:

● No, I do not want to use DNS.

Figure 3-101 DNS configuration

31. The Next Steps panel (Figure 3-102) explains that you are finished with the network settings, and will now proceed and configure optional functionalities. Click **Next**.



Launch Guided Setup Wizard - The Next Steps

You have completed the following (available locally only):

- Configure HMC network settings

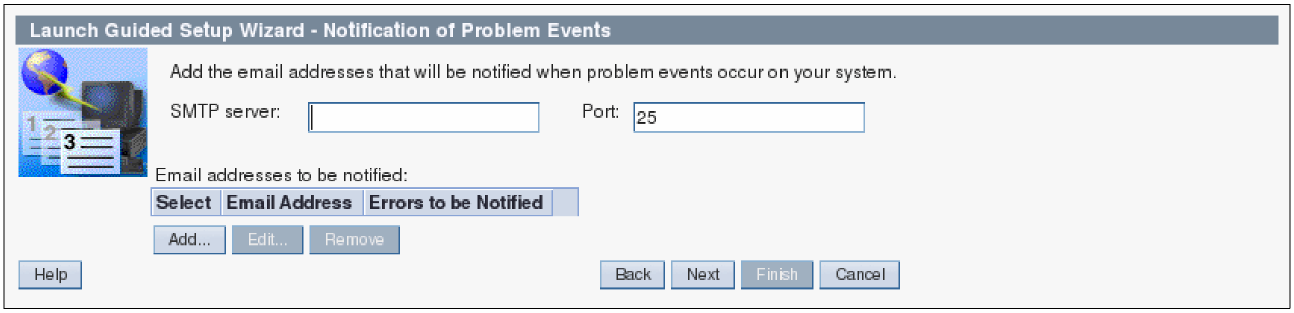
Next, you will do the following:

- (Optional)Configure customer notification of problem events
- Configure connectivity to your service provider using the Call-Home Setup wizard

Click Next to continue.

Figure 3-102 Network settings are completed

32. Although you can set an SMTP server according to your own environment, here in the notification of problem events panel (Figure 3-103), in this example, do not set an SMTP server. Click **Next**.



Launch Guided Setup Wizard - Notification of Problem Events

Add the email addresses that will be notified when problem events occur on your system.

SMTP server:

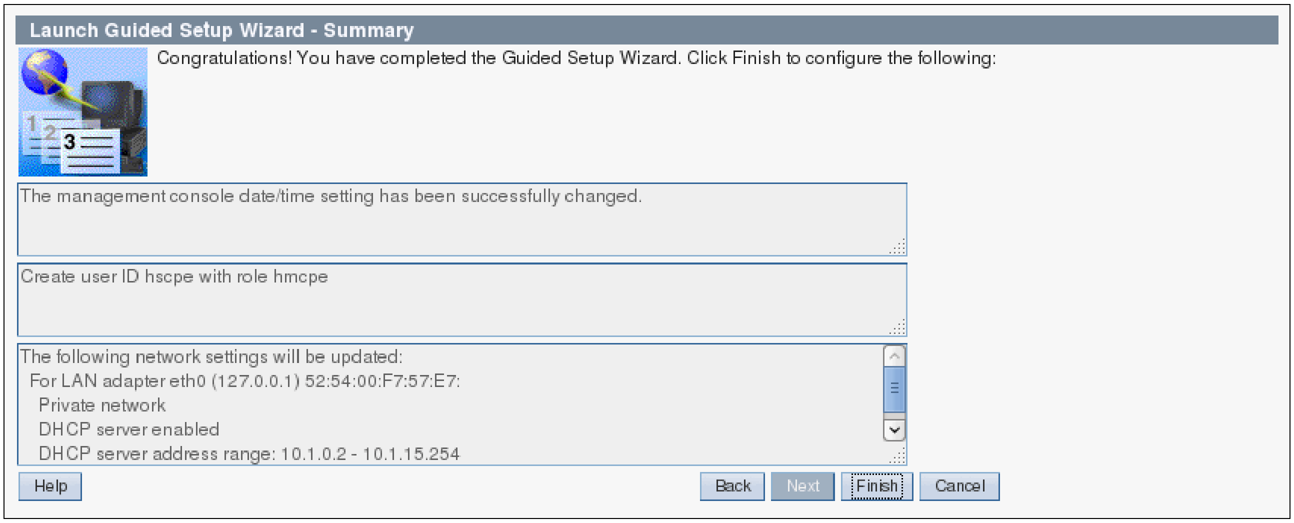
Port: 25

Email addresses to be notified:

Select	Email Address	Errors to be Notified

Figure 3-103 SMTP server setup

33. In the Summary panel (Figure 3-104), check that the configuration is done through the HMC guided setup wizard. Now you can click **Finish**.



Launch Guided Setup Wizard - Summary

Congratulations! You have completed the Guided Setup Wizard. Click Finish to configure the following:

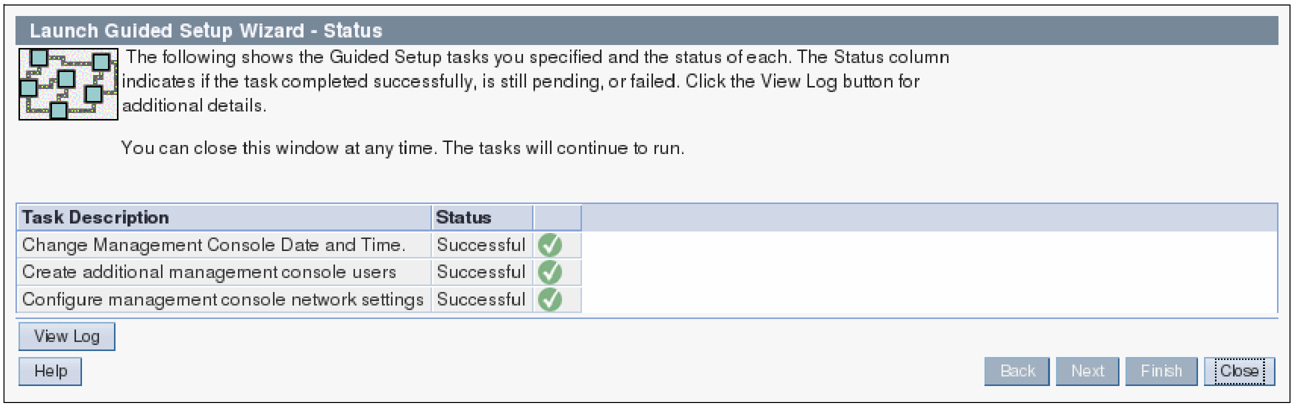
The management console date/time setting has been successfully changed.

Create user ID hscpe with role hmcpe

The following network settings will be updated:
For LAN adapter eth0 (127.0.0.1) 52:54:00:F7:57:E7:
Private network
DHCP server enabled
DHCP server address range: 10.1.0.2 - 10.1.15.254

Figure 3-104 Summary panel

34. The Status panel (Figure 3-105) lists the successful tasks. Click **Close**.



Launch Guided Setup Wizard - Status

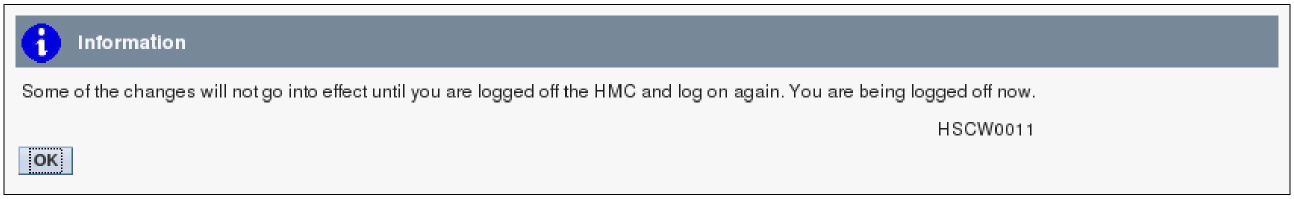
The following shows the Guided Setup tasks you specified and the status of each. The Status column indicates if the task completed successfully, is still pending, or failed. Click the View Log button for additional details.

You can close this window at any time. The tasks will continue to run.

Task Description	Status	
Change Management Console Date and Time.	Successful	✓
Create additional management console users	Successful	✓
Configure management console network settings	Successful	✓

Figure 3-105 Status panel

35. In the information panel (Figure 3-106), click **OK**.



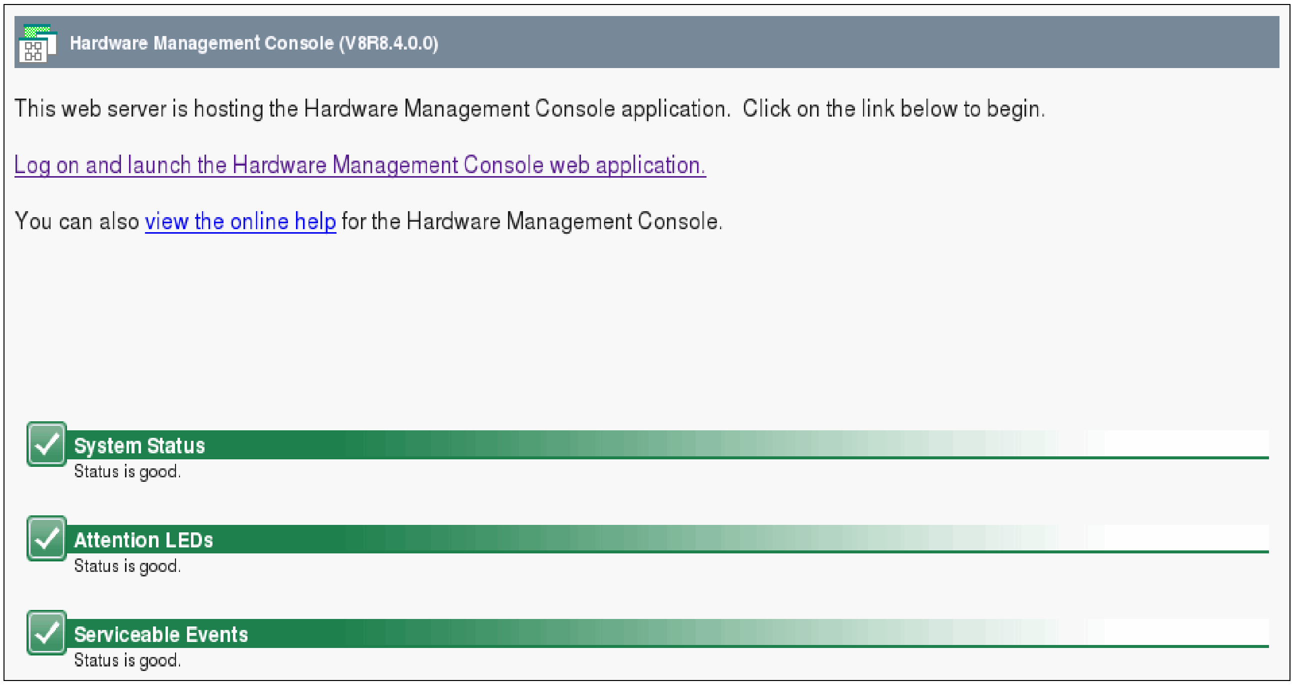
Information

Some of the changes will not go into effect until you are logged off the HMC and log on again. You are being logged off now.

HSCW0011

Figure 3-106 Information panel

36. After a moment, the HMC restarts its processes, and opens the Welcome panel (Figure 3-107). You can now log on.



Hardware Management Console (V8R8.4.0.0)

This web server is hosting the Hardware Management Console application. Click on the link below to begin.

Log on and launch the Hardware Management Console web application.

You can also view the online help for the Hardware Management Console.

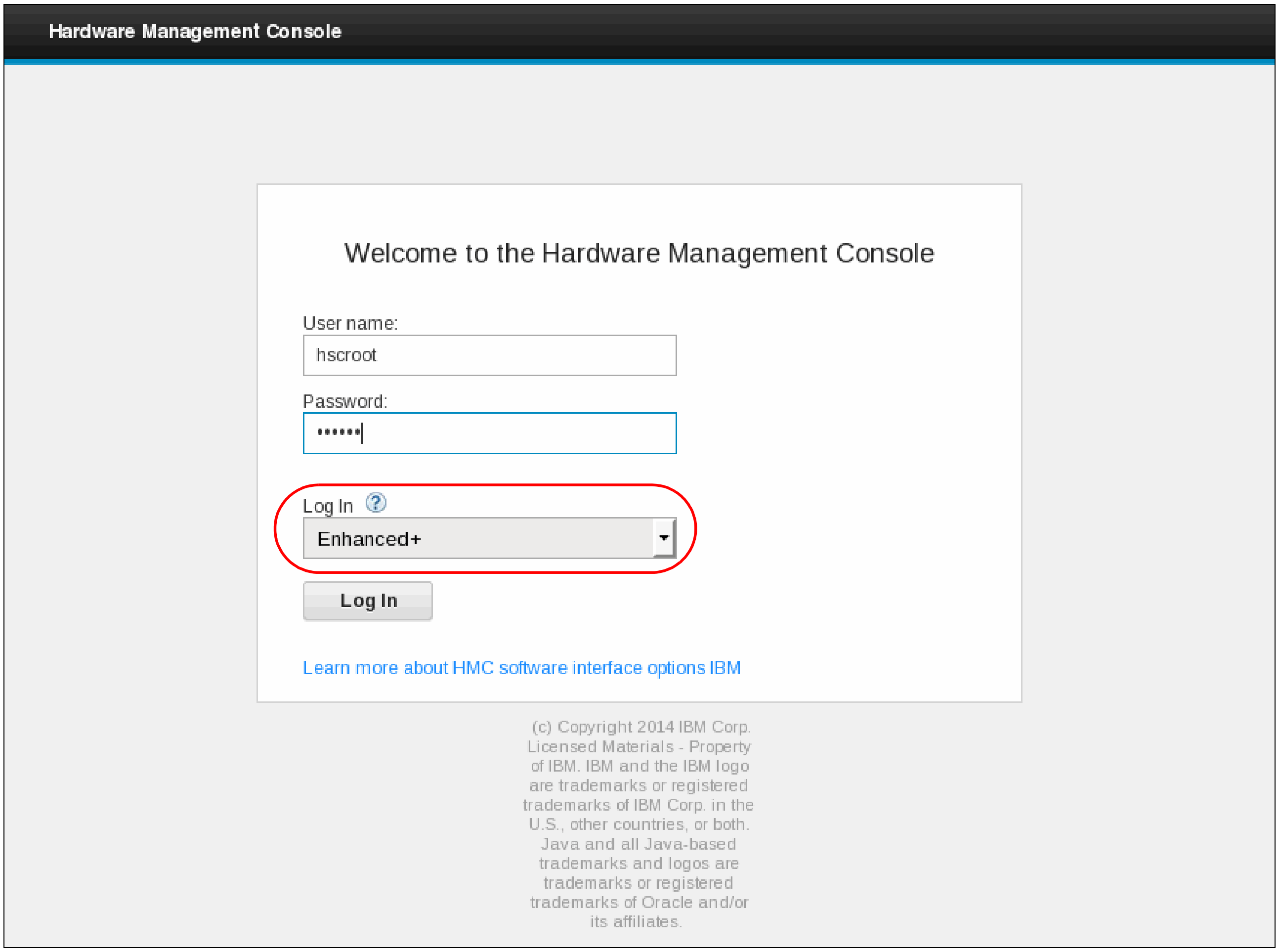
System Status
Status is good.

Attention LEDs
Status is good.

Serviceable Events
Status is good.

Figure 3-107 HMC first logon panel

37.The new HMC Welcome panel proposes to log in (Figure 3-108). Select the new **Enhanced+** login, and log in with the `hscroot` user.



Hardware Management Console

Welcome to the Hardware Management Console

User name: hscroot

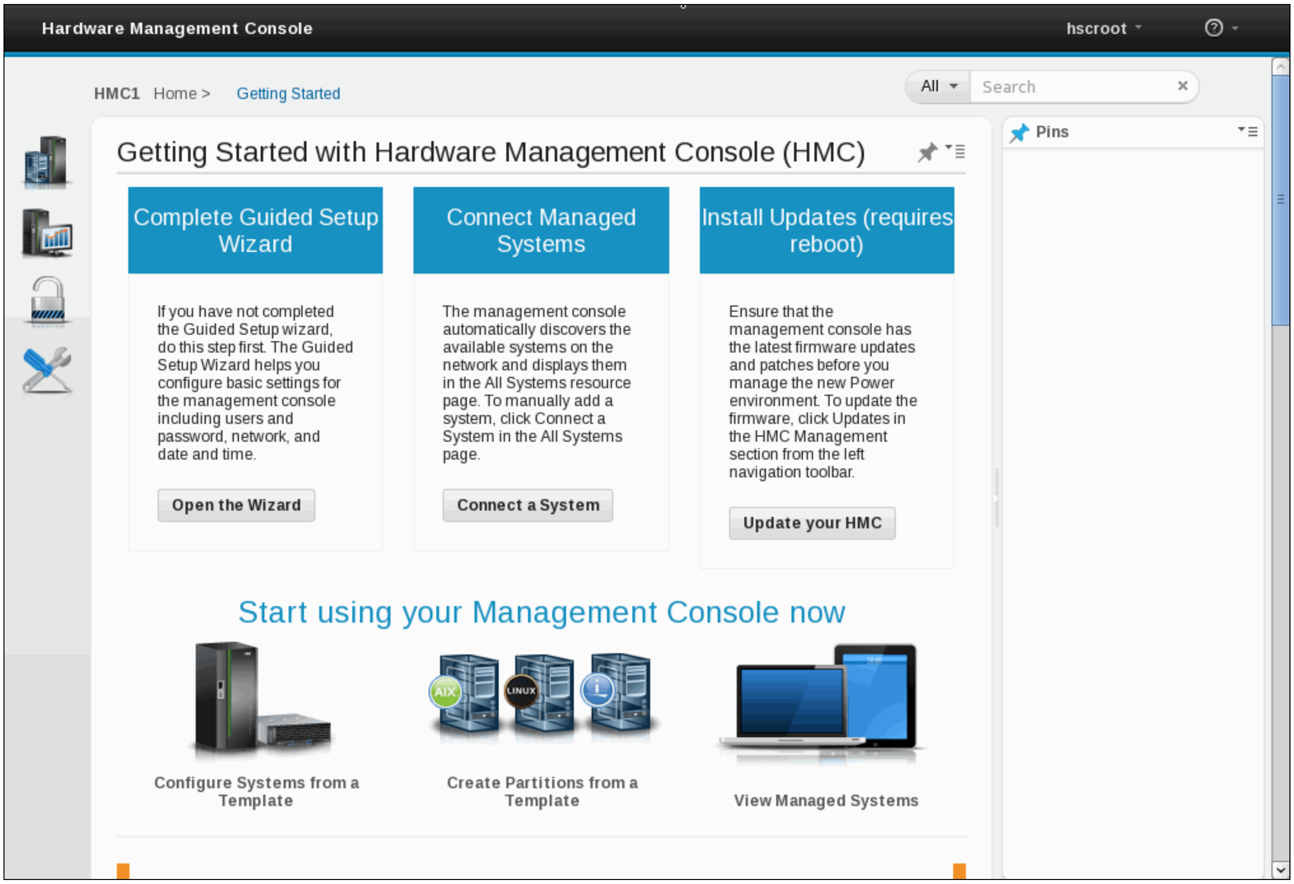
Password: ••••••

Log In: Enhanced+

(c) Copyright 2014 IBM Corp. Licensed Materials - Property of IBM. IBM and the IBM logo are trademarks or registered trademarks of IBM Corp. in the U.S., other countries, or both. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Figure 3-108 HMC Welcome login panel

38. The Getting Started panel opens (Figure 3-109). From here you can start managing with the HMC.



Hardware Management Console

HMC1 Home > Getting Started

Getting Started with Hardware Management Console (HMC)

Complete Guided Setup Wizard

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

Open the Wizard

Connect Managed Systems

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Connect a System

Install Updates (requires reboot)

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

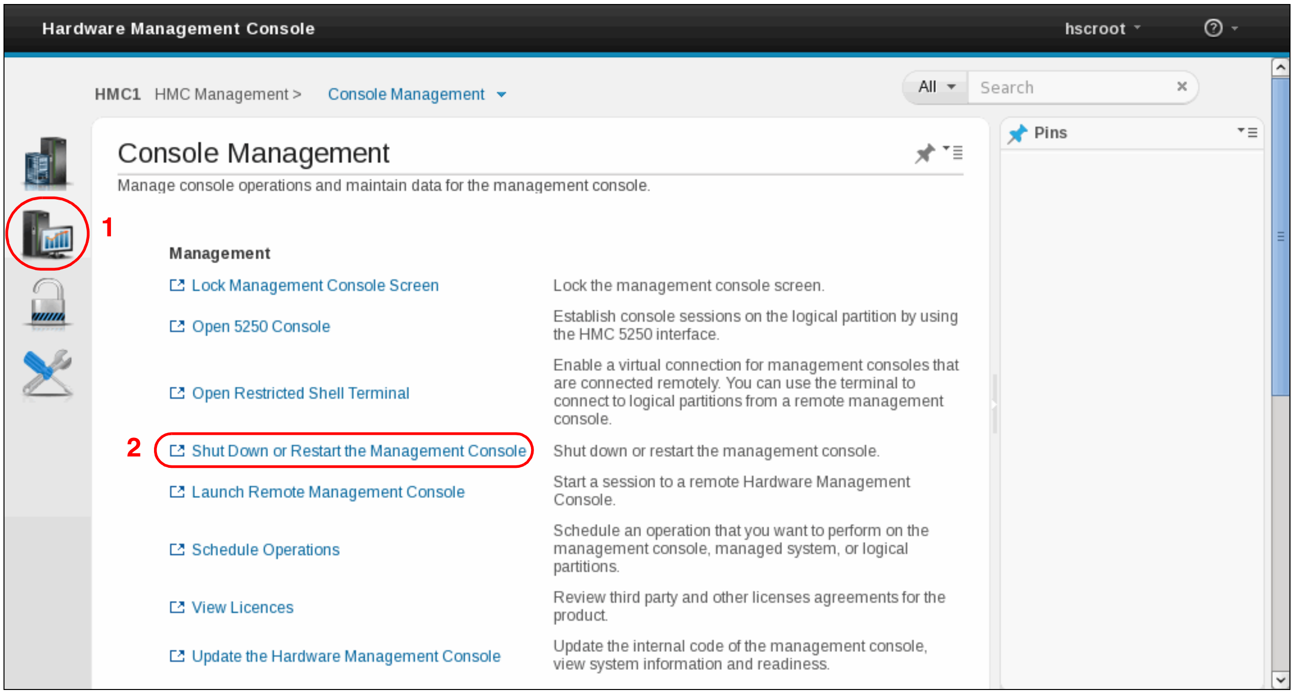
Update your HMC

Start using your Management Console now

hscroot
All
Search
Pins
Configure Systems from a Template
Create Partitions from a Template
View Managed Systems
AIX
LINUX

Figure 3-109 Getting started HMC panel

39. The first tasks are to restart the HMC and validate that it is properly running. Click the **HMC management** icon (1) in the left navigation pane (Figure 3-110), and click **Shut Down or Restart** (2).


Hardware Management Console
hscroot
HMC1 HMC Management > Console Management
All
Search
Pins
1
2

Console Management

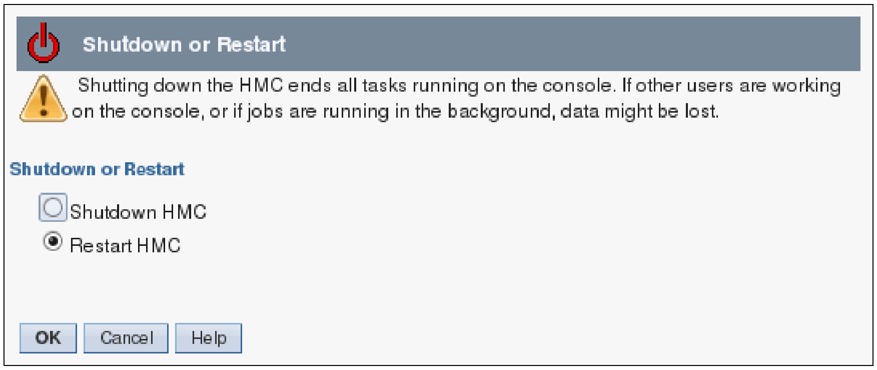
Manage console operations and maintain data for the management console.

Management

Lock Management Console Screen	Lock the management console screen.
Open 5250 Console	Establish console sessions on the logical partition by using the HMC 5250 interface.
Open Restricted Shell Terminal	Enable a virtual connection for management consoles that are connected remotely. You can use the terminal to connect to logical partitions from a remote management console.
Shut Down or Restart the Management Console	Shut down or restart the management console.
Launch Remote Management Console	Start a session to a remote Hardware Management Console.
Schedule Operations	Schedule an operation that you want to perform on the management console, managed system, or logical partitions.
View Licences	Review third party and other licenses agreements for the product.
Update the Hardware Management Console	Update the internal code of the management console, view system information and readiness.

Figure 3-110 HMC Management panel

40. Confirm to restart the HMC by selecting **Restart HMC** and clicking **OK** (Figure 3-111).



Shutting down the HMC ends all tasks running on the console. If other users are working on the console, or if jobs are running in the background, data might be lost.

Shutdown or Restart

○ Shutdown HMC

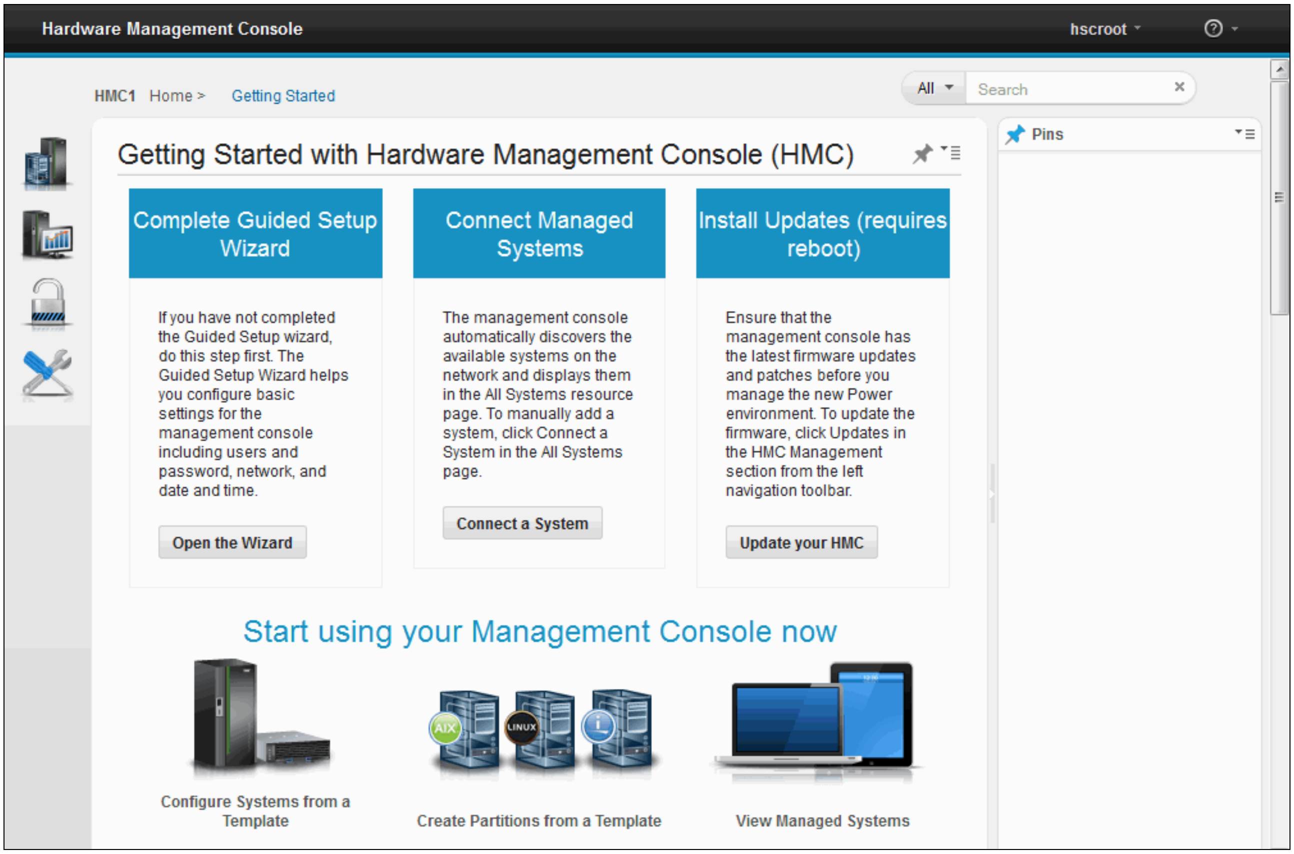
● Restart HMC

Figure 3-111 Restart the HMC

41. After the HMC reboots, you may direct your browser to the HMC’s IP address configured on the open network interface. In this example, it is as follows:

```
https://172.16.20.126
```

You can now use the HMC. After you log in to the console, the window looks like the one in Figure 3-112.



Getting Started with Hardware Management Console (HMC)

Complete Guided Setup Wizard

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

Connect Managed Systems

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Install Updates (requires reboot)

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Update your HMC
Start using your Management Console now
AIX
LINUX
Configure Systems from a Template
Create Partitions from a Template
View Managed Systems

Figure 3-112 HMC Enhanced+ Welcome panel

After the installation is complete, you may consider updating the HMC to the latest level of maintenance for the version and release of the HMC. The latest service pack and fixes are available from the IBM Fix Central website:

http://www.ibm.com/support/fixcentral

3.4 HMC update

This section covers the update of the HMC. Distinguishing between updating and upgrading a system is important. The terms are *not* synonymous.

- An *upgrade* is the method to bring the system to a higher *version or release* of HMC code. When the HMC's version number is incremented, such as going from Version 7 to Version 8, the upgrade method must be used in order to apply the new version of HMC code. To move from V8R3 to V8R4, an upgrade is also required.
- An *update* is indicated when you want to apply a service pack or a fix, and remain on the same version and release of the HMC.

The latest service pack and fixes are available from the IBM Fix Central website:

http://www.ibm.com/support/fixcentral

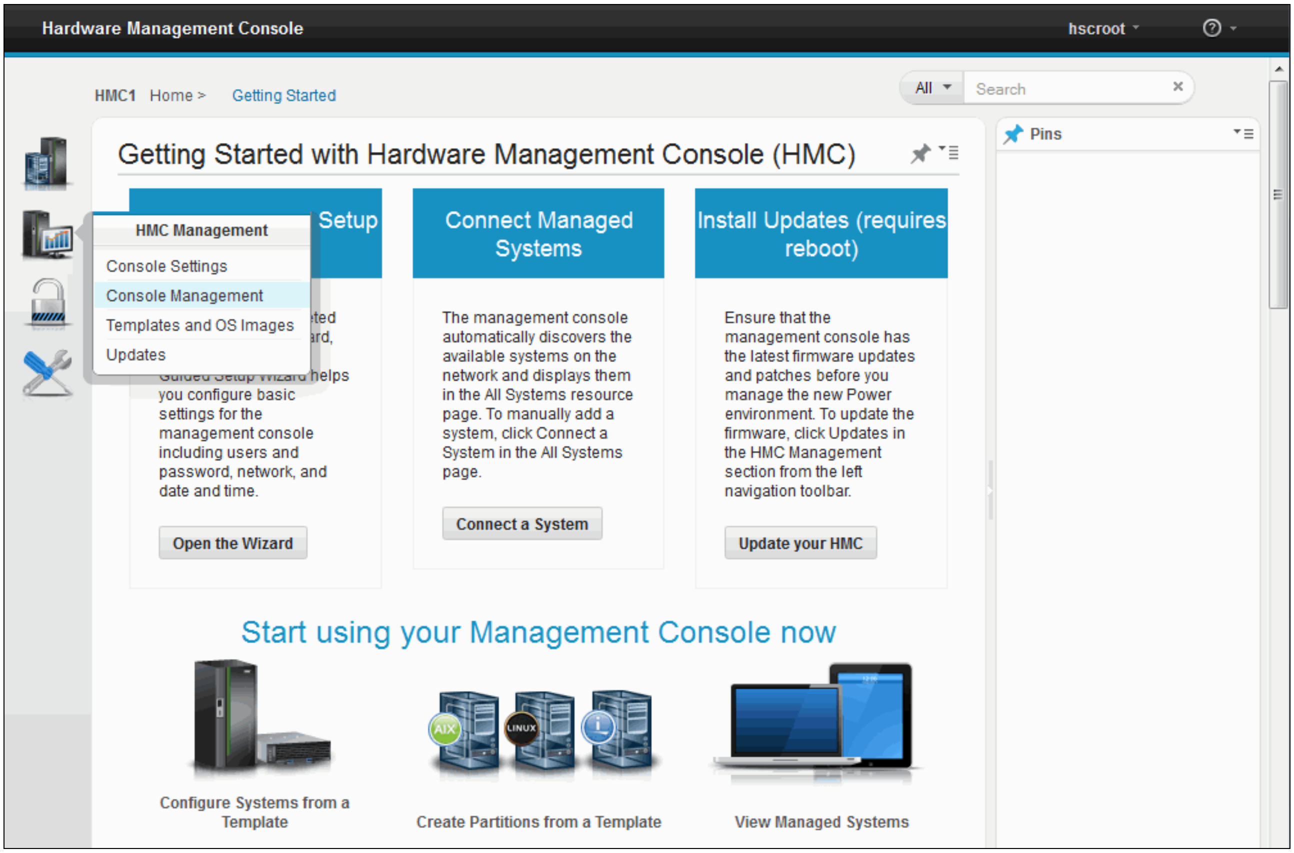
You may update the HMC with these methods:

- Update from the graphical user interface (GUI)
- Update from the command-line interface (CLI)

Update from the graphical user interface (GUI)

To update the HMC to a new fix level, use the following steps:

1. From the Welcome panel (Figure 3-113), click the **HMC Management** on the left and then select **Console Management**.


Hardware Management Console
hscroot
HMC1 Home > Getting Started
All
Search
Pins
Getting Started with Hardware Management Console (HMC)
HMC Management
Console Settings
Console Management
Templates and OS Images
Updates
Setup
Connect Managed Systems
Install Updates (requires reboot)
Open the Wizard
Connect a System
Update your HMC
Start using your Management Console now
Configure Systems from a Template
Create Partitions from a Template
View Managed Systems

...ted ...ard, Guided Setup wizard helps you configure basic settings for the management console including users and password, network, and date and time.

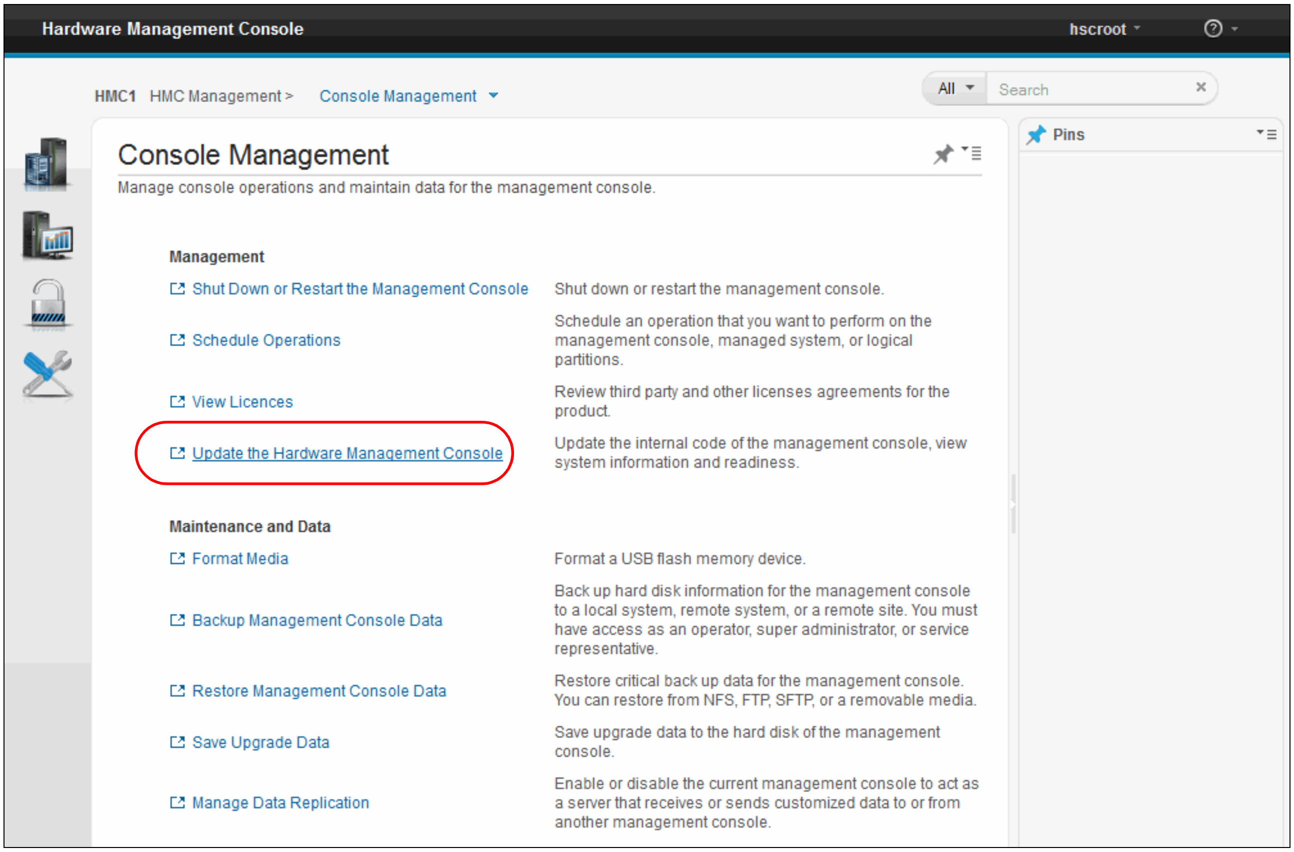
The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 3-113 Go to HMC Management

2. In the Console Management panel (Figure 3-114 on page 245), click **Update the Hardware Management Console**.

> **Note:** If your HMC was already connected to managed systems, and has an advanced configuration, you must back up your current configuration. This can be done with the *Backup Management Console Data* task, also shown in Figure 3-114 on page 245.


Hardware Management Console
hscroot
HMC1 HMC Management > Console Management
All
Search
Pins

Console Management

Manage console operations and maintain data for the management console.

Management

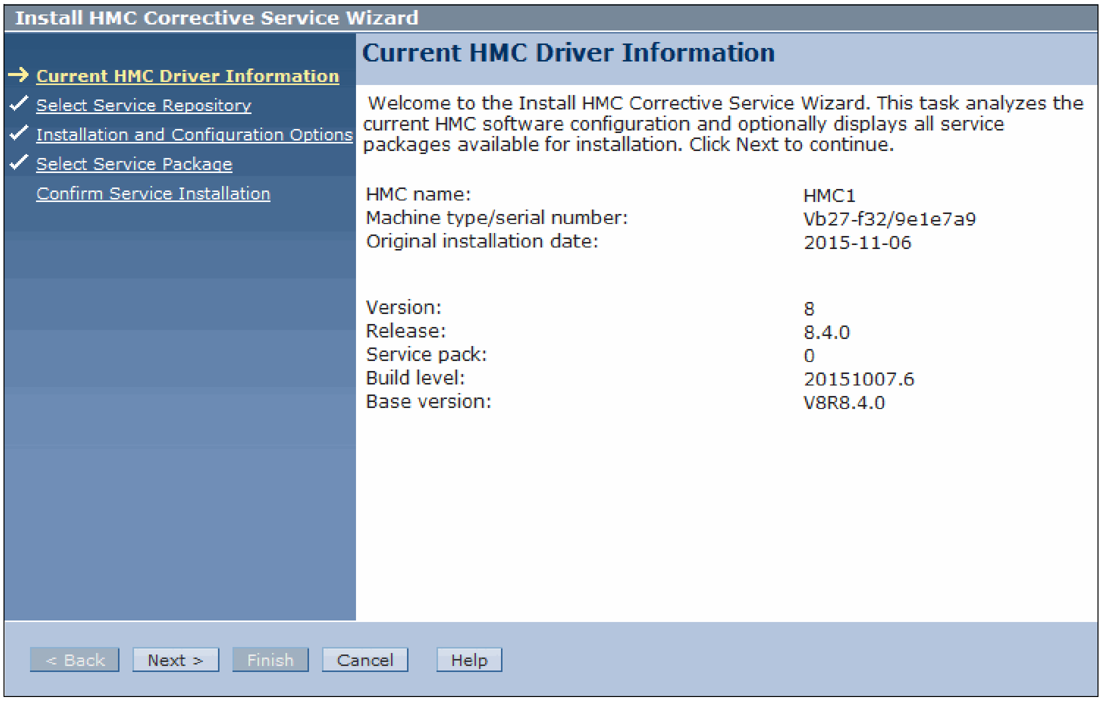
Shut Down or Restart the Management Console	Shut down or restart the management console.
Schedule Operations	Schedule an operation that you want to perform on the management console, managed system, or logical partitions.
View Licences	Review third party and other licenses agreements for the product.
Update the Hardware Management Console	Update the internal code of the management console, view system information and readiness.

Maintenance and Data

Format Media	Format a USB flash memory device.
Backup Management Console Data	Back up hard disk information for the management console to a local system, remote system, or a remote site. You must have access as an operator, super administrator, or service representative.
Restore Management Console Data	Restore critical back up data for the management console. You can restore from NFS, FTP, SFTP, or a removable media.
Save Upgrade Data	Save upgrade data to the hard disk of the management console.
Manage Data Replication	Enable or disable the current management console to act as a server that receives or sends customized data to or from another management console.

Figure 3-114 Update the HMC

3. The Current HMC Driver Information panel (Figure 3-115) provides the current level. Click **Next**.


Install HMC Corrective Service Wizard
Current HMC Driver Information
Select Service Repository
Installation and Configuration Options
Select Service Package
Confirm Service Installation
< Back
Next >
Finish
Cancel
Help

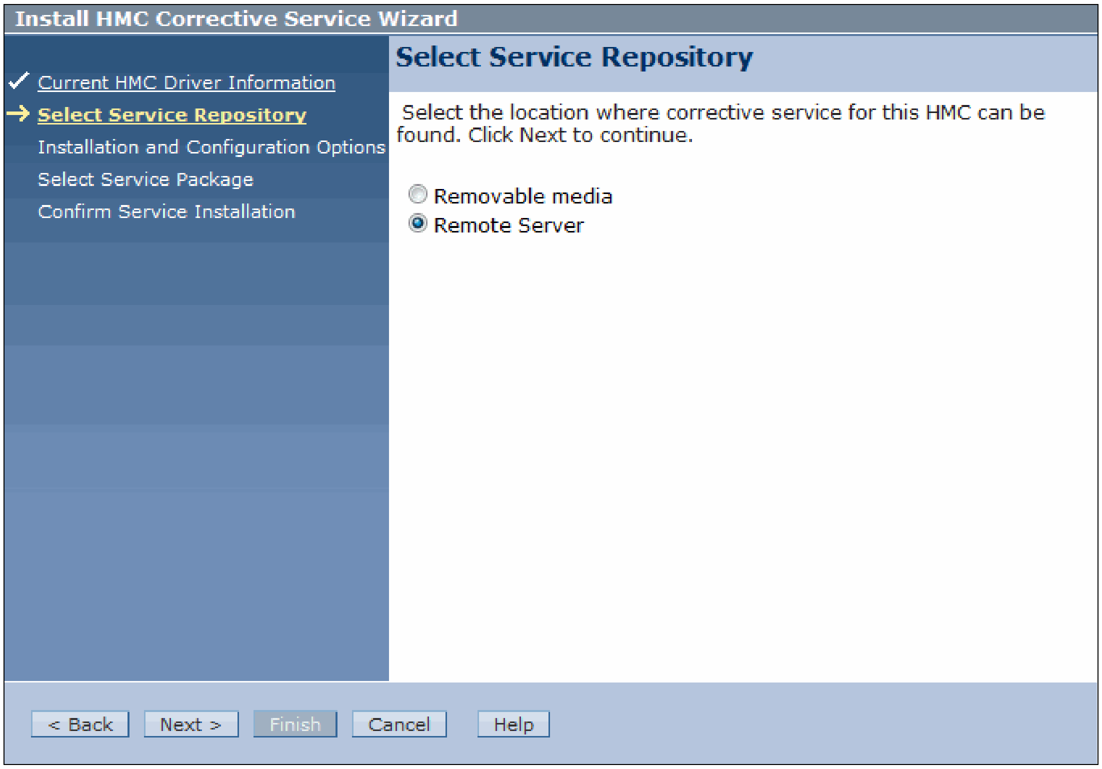
Current HMC Driver Information

Welcome to the Install HMC Corrective Service Wizard. This task analyzes the current HMC software configuration and optionally displays all service packages available for installation. Click Next to continue.

HMC name:	HMC1
Machine type/serial number:	Vb27-f32/9e1e7a9
Original installation date:	2015-11-06
Version:	8
Release:	8.4.0
Service pack:	0
Build level:	20151007.6
Base version:	V8R8.4.0

Figure 3-115 Current HMC Driver Information

4. This example uses a remote server. In the Select Repository panel (Figure 3-116), choose **Remote Server**, and click **Next**.



Install HMC Corrective Service Wizard

Select Service Repository

Select the location where corrective service for this HMC can be found. Click Next to continue.

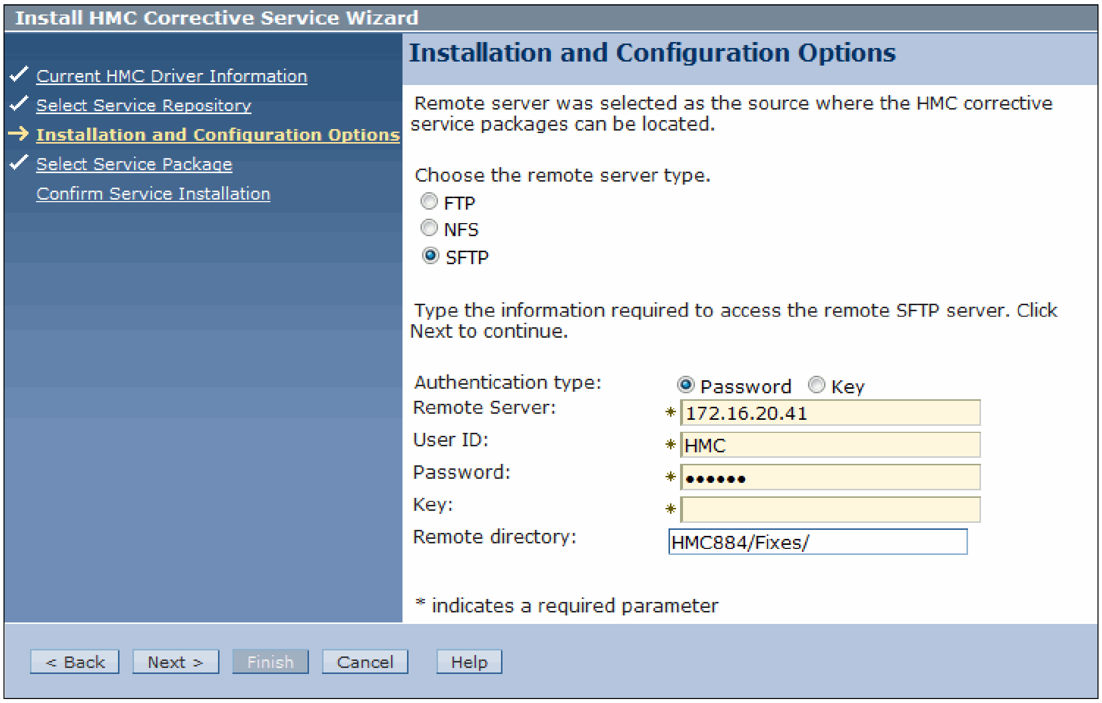
○ Removable media
● Remote Server

✓ Current HMC Driver Information
→ Select Service Repository
Installation and Configuration Options
Select Service Package
Confirm Service Installation
< Back
Next >
Finish
Cancel
Help

Figure 3-116 Select Service Repository

5. The Installation and Configuration Options panel (Figure 3-117) shows several remote server options.

   In this example, choose **SFTP**, and complete the information related to the repository server, user, password, and directory, and then click **Next**.



Install HMC Corrective Service Wizard

✓ Current HMC Driver Information
✓ Select Service Repository
→ Installation and Configuration Options
✓ Select Service Package
Confirm Service Installation

Installation and Configuration Options

Remote server was selected as the source where the HMC corrective service packages can be located.

Choose the remote server type.

○ FTP
○ NFS
● SFTP

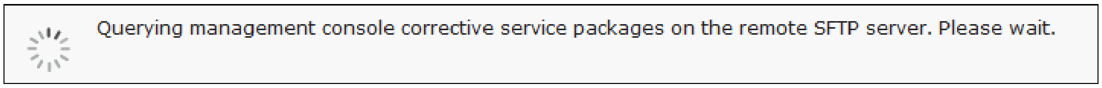
Type the information required to access the remote SFTP server. Click Next to continue.

Authentication type: ● Password ○ Key
Remote Server: * 172.16.20.41
User ID: * HMC
Password: * ••••••
Key: *
Remote directory: HMC884/Fixes/

* indicates a required parameter

Figure 3-117 Installation and Configuration Options

The HMC queries the repository server to search for service packages (Figure 3-118).

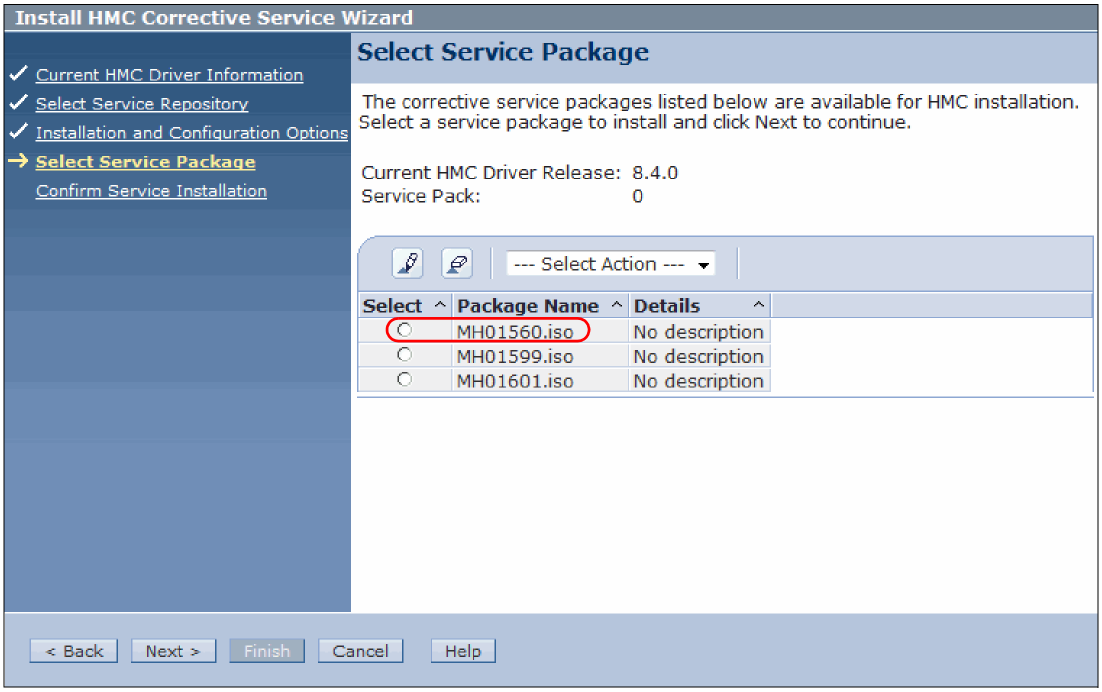


Querying management console corrective service packages on the remote SFTP server. Please wait.

Figure 3-118 Repository server query

6. In the Select Service Package panel (Figure 3-119), choose the fix in the Package Name column (in this example, it is the **MH01560** fix) and then click **Next**.

> **Note:** The package names listed in Figure 3-119 are valid *only* at the time of writing this publication. They might no longer be available on the Fix Central website.


Install HMC Corrective Service Wizard
✓ Current HMC Driver Information
✓ Select Service Repository
✓ Installation and Configuration Options
→ Select Service Package
Confirm Service Installation
--- Select Action ---
< Back
Next >
Finish
Cancel
Help

Select Service Package

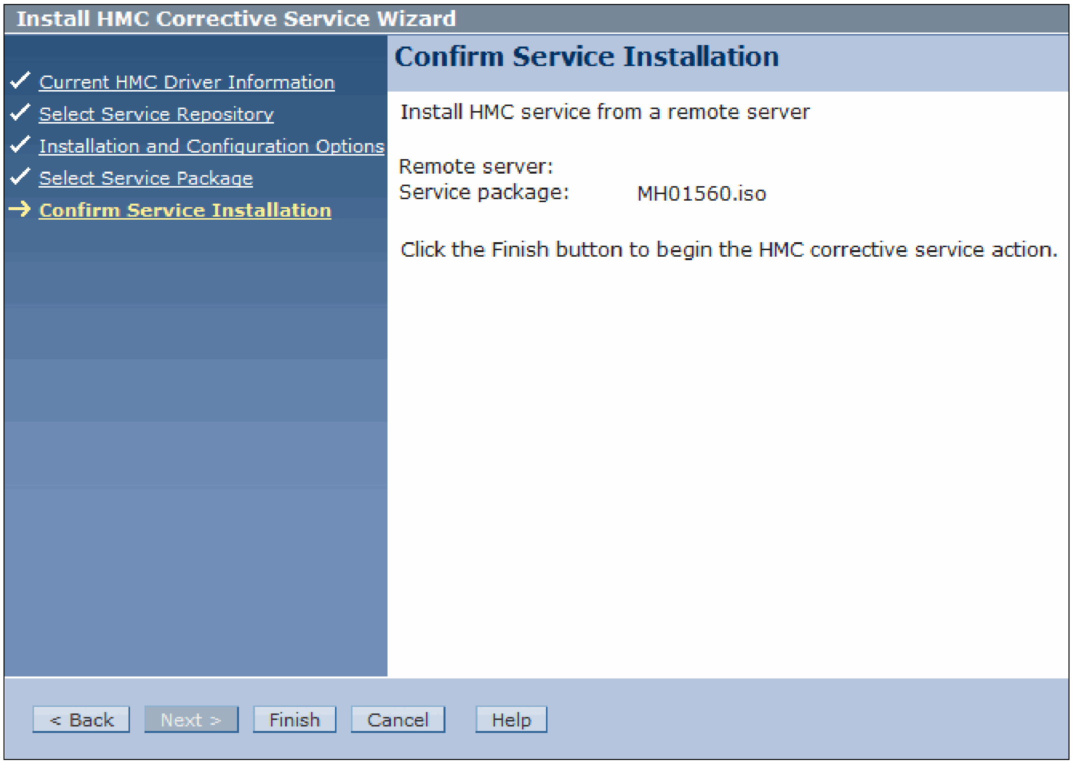
The corrective service packages listed below are available for HMC installation. Select a service package to install and click Next to continue.

Current HMC Driver Release: 8.4.0
Service Pack: 0

Select	Package Name	Details
○	MH01560.iso	No description
○	MH01599.iso	No description
○	MH01601.iso	No description

Figure 3-119 Select Service Package

7. Click **Finish** in the Confirm Service Installation panel (Figure 3-120).


Install HMC Corrective Service Wizard
✓ Current HMC Driver Information
✓ Select Service Repository
✓ Installation and Configuration Options
✓ Select Service Package
→ Confirm Service Installation
< Back
Next >
Finish
Cancel
Help

Confirm Service Installation

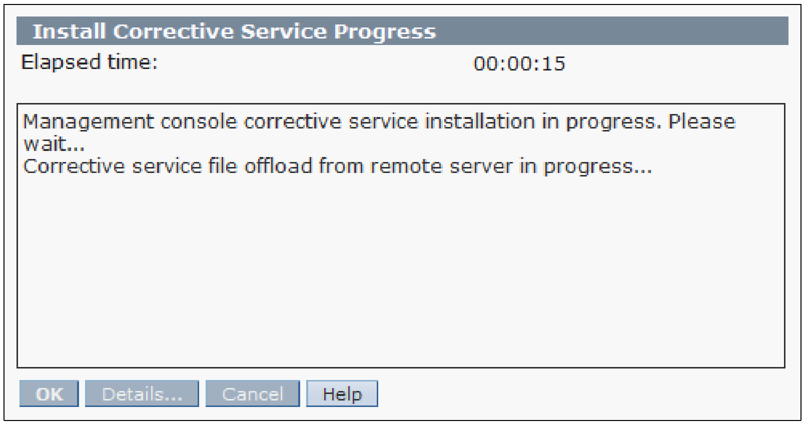
Install HMC service from a remote server

Remote server:
Service package: MH01560.iso

Click the Finish button to begin the HMC corrective service action.

Figure 3-120 Confirm Service Installation

Installation of the fix begins, and the installation progress is indicated (Figure 3-121).

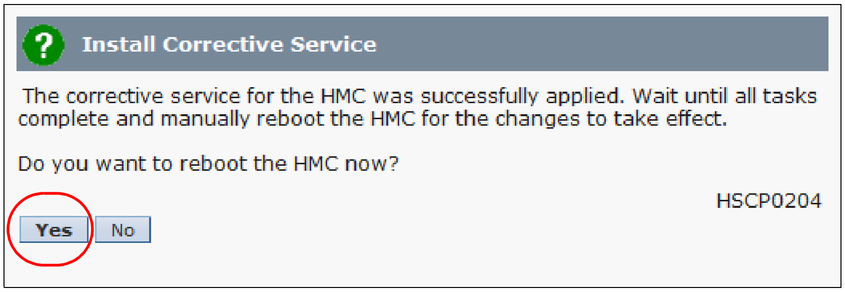


Elapsed time: 00:00:15

Management console corrective service installation in progress. Please wait...
Corrective service file offload from remote server in progress...

Figure 3-121 Install Corrective Service Progress

8. After the fix is successfully installed, click **Yes**, (Figure 3-122). You are logged off, and the HMC reboots.



Install Corrective Service

The corrective service for the HMC was successfully applied. Wait until all tasks complete and manually reboot the HMC for the changes to take effect.

Do you want to reboot the HMC now?

HSCP0204

Figure 3-122 Reboot HMC after service installation

The HMC now goes through post-installation steps installs the update, and reboots again.

After the reboot, the HMC is updated to the fix level that is applied.

Update from the command-line interface (CLI)

Example 3-31 shows an HMC update by using the **updhmc** command, from the HMC command line, followed by the **hmcshutdown -r** command to reboot the HMC.

Example 3-31 Update from CLI and reboot

```
hscroot@HMC1:~> updhmc -t sftp -h 172.16.20.41 -u HMC -p ******** -f \
                HMC884/Fixes/MH01560.iso
The corrective service file was successfully applied. A mandatory reboot is
required but was not specified on the command syntax.

hscroot@HMC1:~> hmcshutdown -r -t now
```

After the reboot, the new HMC level can be verified from the HMC prompt with the **lshmc -V** command as shown in Example 3-32.

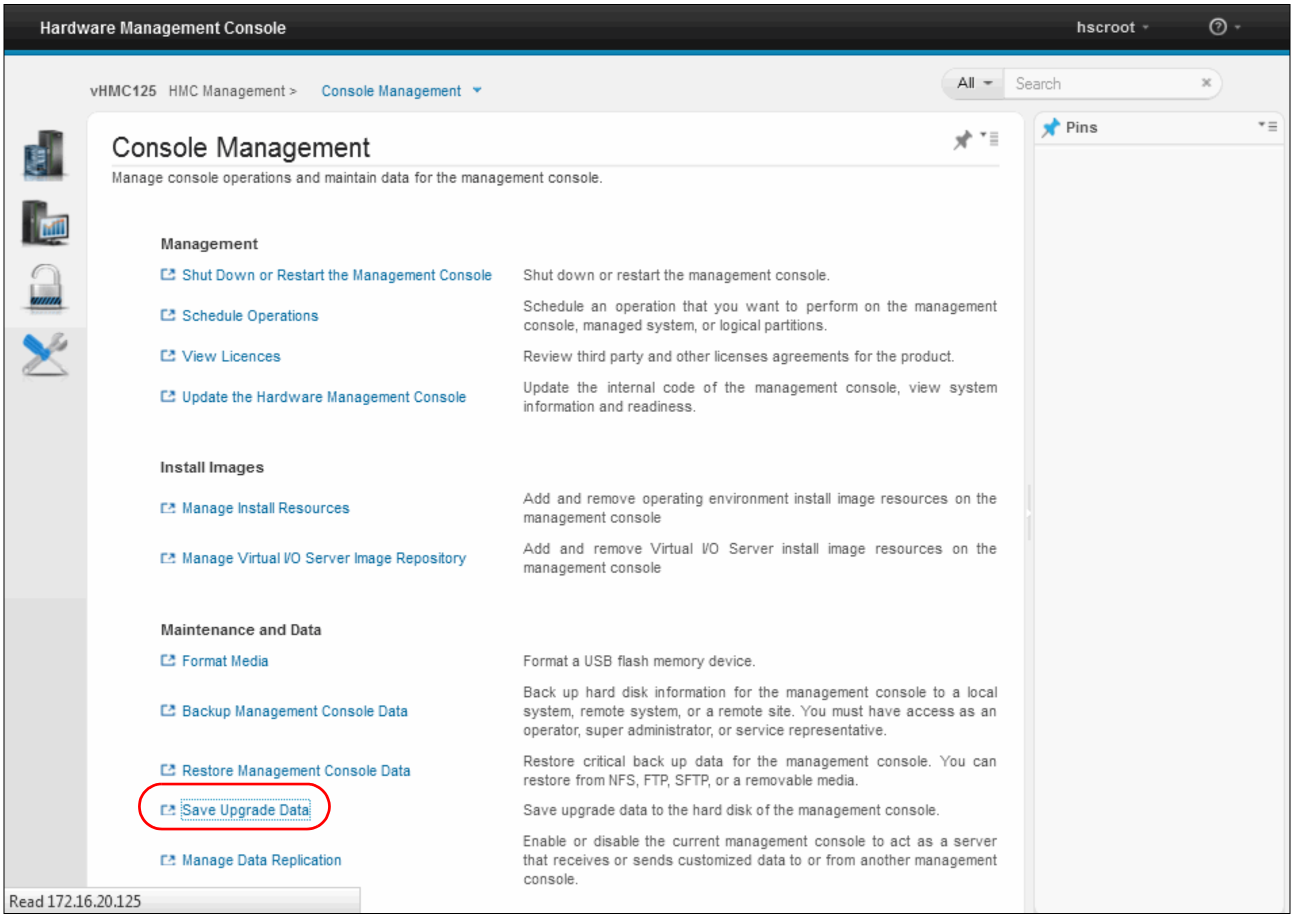
Example 3-32 Verify the HMC level

```
hscroot@HMC1:~> lshmc -V
"version= Version: 8
 Release: 8.4.0
 Service Pack: 0
HMC Build level 20151103.7
MH01560: Required fix for HMC V8R8.4.0 (11-04-2015)
","base_version=V8R8.4.0
"
```

3.5 HMC upgrade to a new software level

To upgrade the HMC to a new software level, complete the following steps:

1. In the navigation pane, click **HMC Management** → **Save Upgrade Data** (Figure 3-123).


Hardware Management Console
hscroot
vHMC125 HMC Management > Console Management
All
Search
Pins
Read 172.16.20.125

Console Management

Manage console operations and maintain data for the management console.

Management

Shut Down or Restart the Management Console	Shut down or restart the management console.
Schedule Operations	Schedule an operation that you want to perform on the management console, managed system, or logical partitions.
View Licences	Review third party and other licenses agreements for the product.
Update the Hardware Management Console	Update the internal code of the management console, view system information and readiness.

Install Images

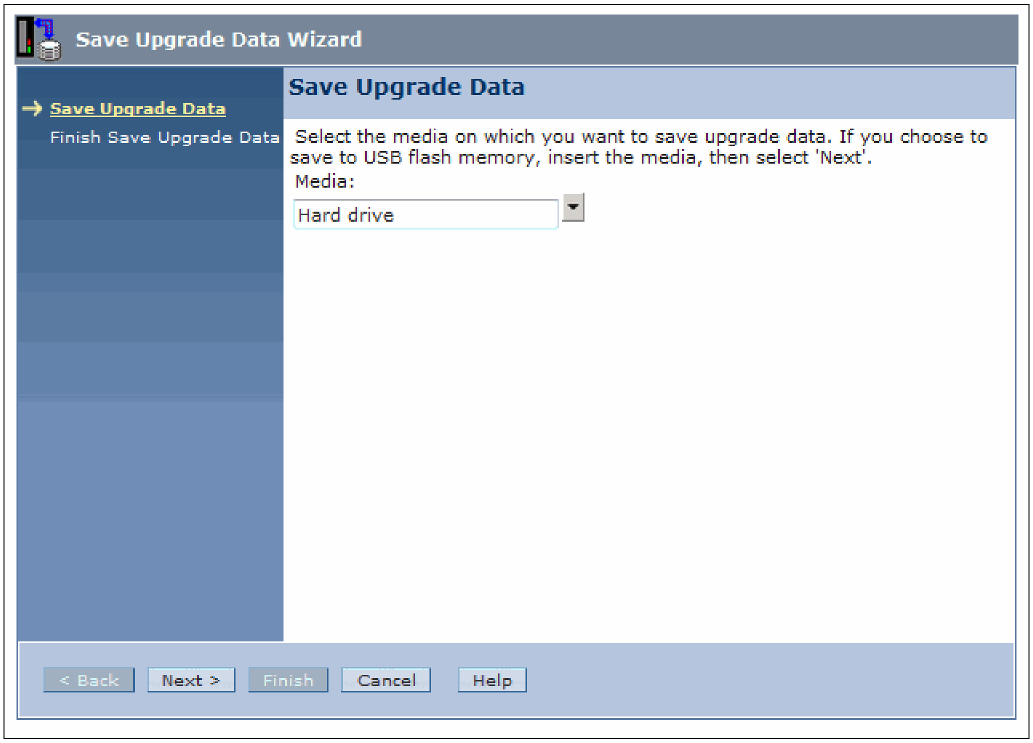
Manage Install Resources	Add and remove operating environment install image resources on the management console
Manage Virtual I/O Server Image Repository	Add and remove Virtual I/O Server install image resources on the management console

Maintenance and Data

Format Media	Format a USB flash memory device.
Backup Management Console Data	Back up hard disk information for the management console to a local system, remote system, or a remote site. You must have access as an operator, super administrator, or service representative.
Restore Management Console Data	Restore critical back up data for the management console. You can restore from NFS, FTP, SFTP, or a removable media.
Save Upgrade Data	Save upgrade data to the hard disk of the management console.
Manage Data Replication	Enable or disable the current management console to act as a server that receives or sends customized data to or from another management console.

Figure 3-123 Save Upgrade data

2. Select the type of media where you want to save the upgrade data (Figure 3-124). In this example, choose **Hard drive**, and click **Next**.



Save Upgrade Data Wizard

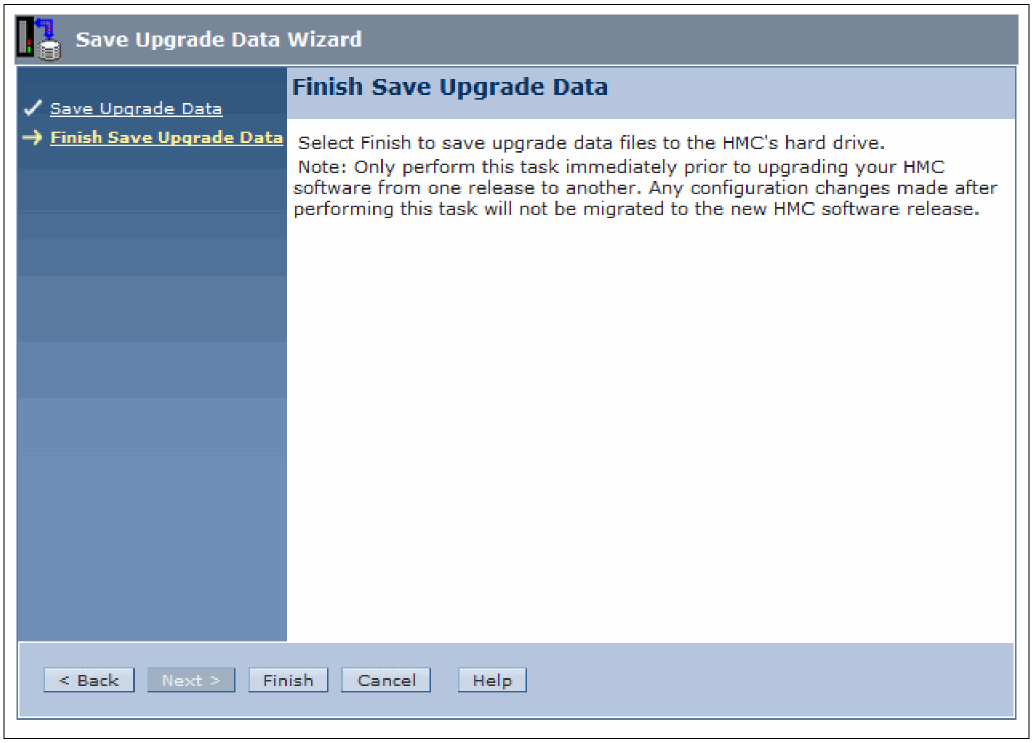
Save Upgrade Data

Select the media on which you want to save upgrade data. If you choose to save to USB flash memory, insert the media, then select 'Next'.

Media: Hard drive

Figure 3-124 Upgrade data location

3. Click **Finish** to confirm (Figure 3-125).



Save Upgrade Data Wizard

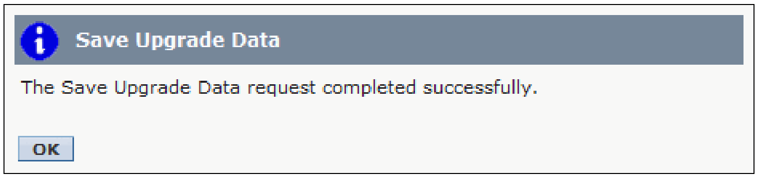
Finish Save Upgrade Data

Select Finish to save upgrade data files to the HMC's hard drive.

Note: Only perform this task immediately prior to upgrading your HMC software from one release to another. Any configuration changes made after performing this task will not be migrated to the new HMC software release.

Figure 3-125 Finish the Save Upgrade Data task

4. After the Save Upgrade Data task completes (Figure 3-126), put the HMC V8.8.4.0 recovery media into the HMC DVD drive, and reboot the HMC.

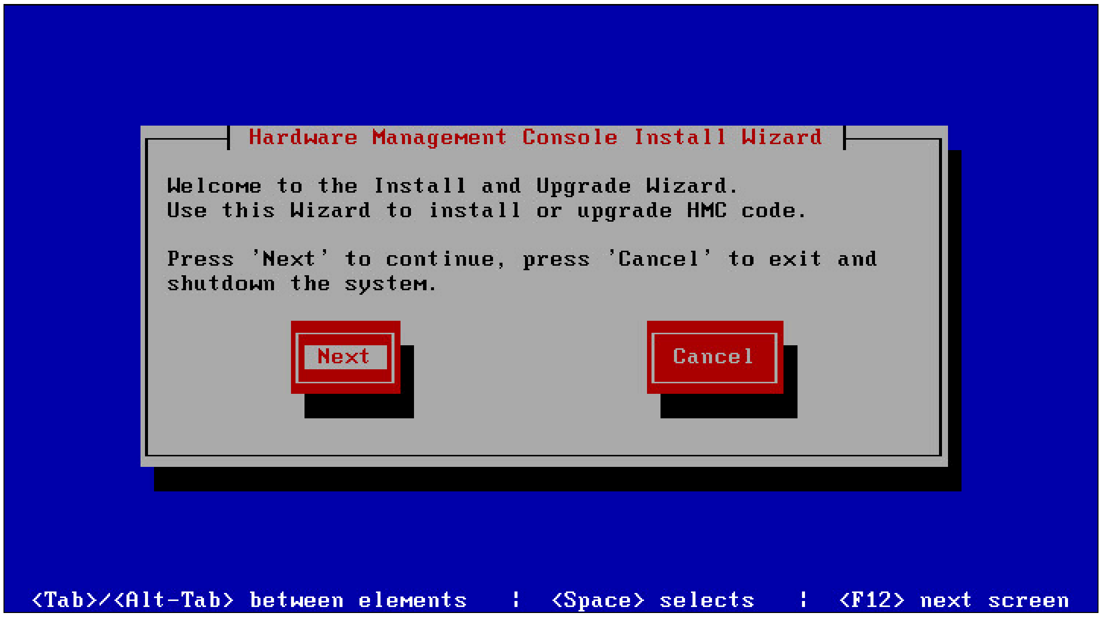


Save Upgrade Data

The Save Upgrade Data request completed successfully.

Figure 3-126 Upgrade Data Saved

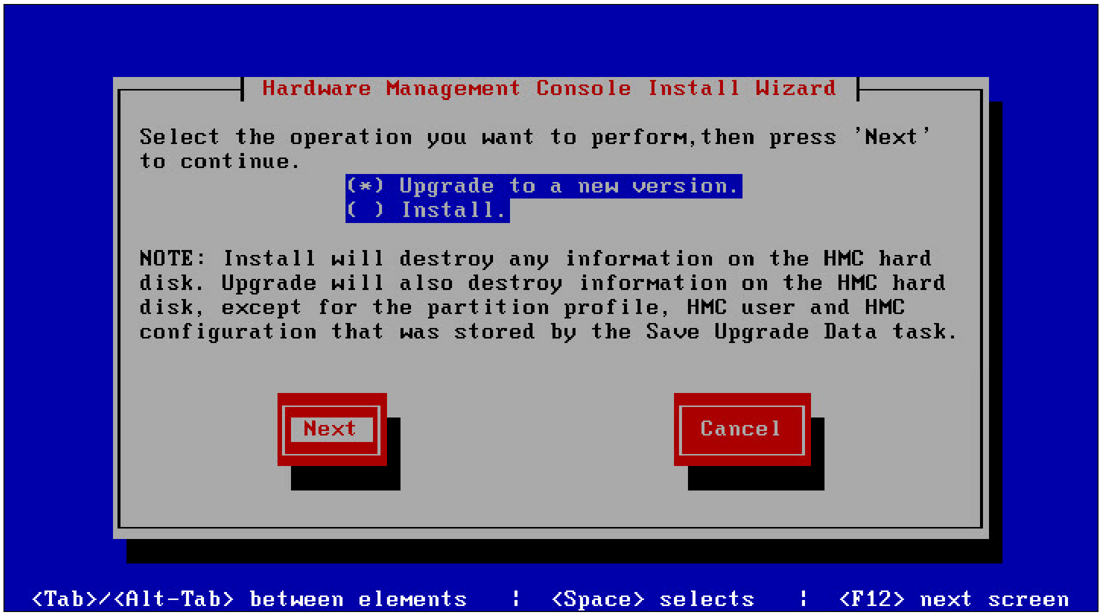
5. The HMC boots from the recovery media and starts the Install Wizard (Figure 3-127). The **Next** button is preselected; to cancel the installation, press the Tab key to select **Cancel** and then press the Enter key. Otherwise, press the Enter key to continue with the upgrade.



```
Hardware Management Console Install Wizard

Welcome to the Install and Upgrade Wizard.
Use this Wizard to install or upgrade HMC code.

Press 'Next' to continue, press 'Cancel' to exit and
shutdown the system.

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

Figure 3-127 HMC Install Wizard

6. Press the Tab key to select **Upgrade to a new version** (Figure 3-128). Then, select **Next**, and press the Enter key.



```
Hardware Management Console Install Wizard

Select the operation you want to perform,then press 'Next'
to continue.
                 (*) Upgrade to a new version.
                 ( ) Install.

NOTE: Install will destroy any information on the HMC hard
disk. Upgrade will also destroy information on the HMC hard
disk, except for the partition profile, HMC user and HMC
configuration that was stored by the Save Upgrade Data task.
```

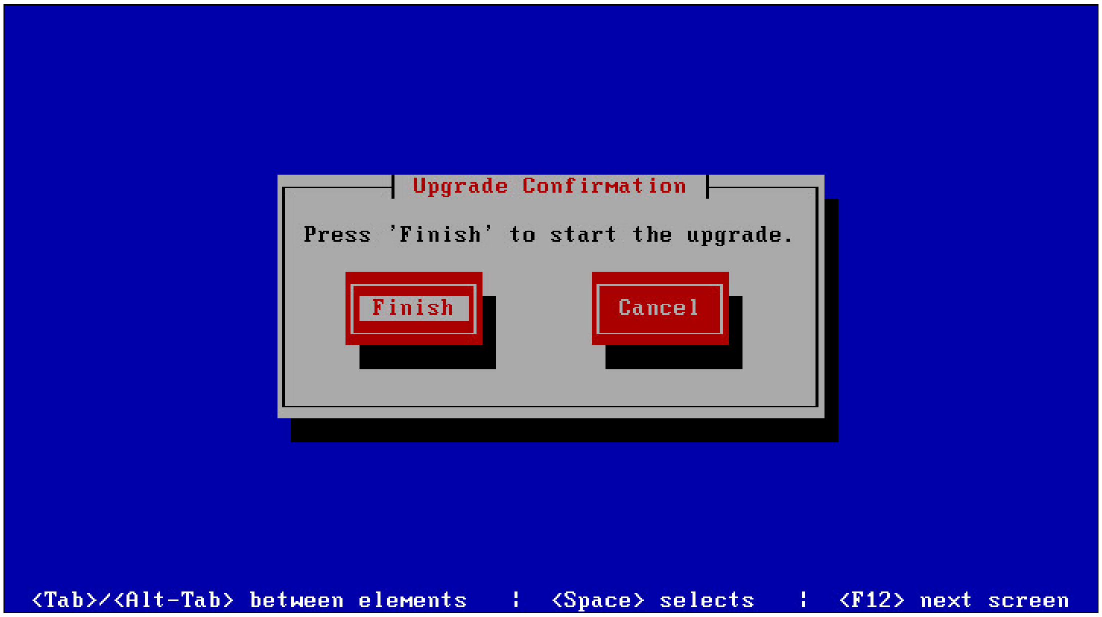
Next
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 3-128 Choose Upgrade

Attention: You can also perform an upgrade by selecting the **Install** operation. The Install operation destroys all the data on the hard disk, including the save upgrade data partition. If this task is used to perform the upgrade, the save upgrade data must be saved to an external USB device.

7. A confirmation window prompts you to confirm the upgrade (Figure 3-129). This is the last point at which the upgrade can be canceled.

   To continue with the upgrade, select **Finish** and press Enter. Otherwise, press the Tab key to select **Cancel** to exit the upgrade.



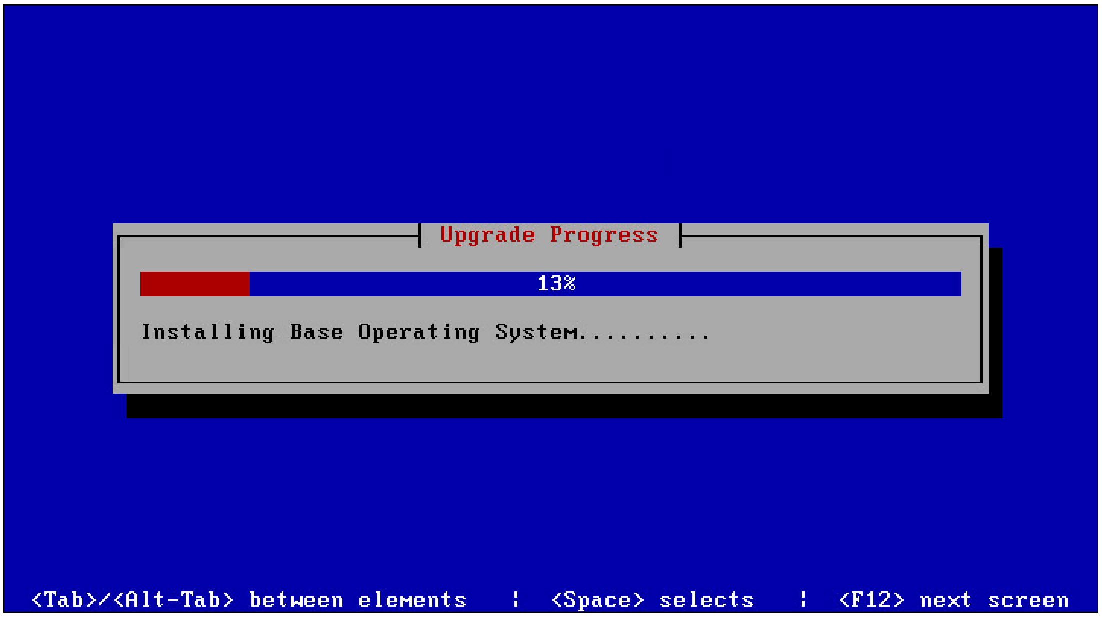
Upgrade Confirmation

Press 'Finish' to start the upgrade.

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 3-129   Upgrade Confirmation

The installation progress continues (Figure 3-130).



Upgrade Progress

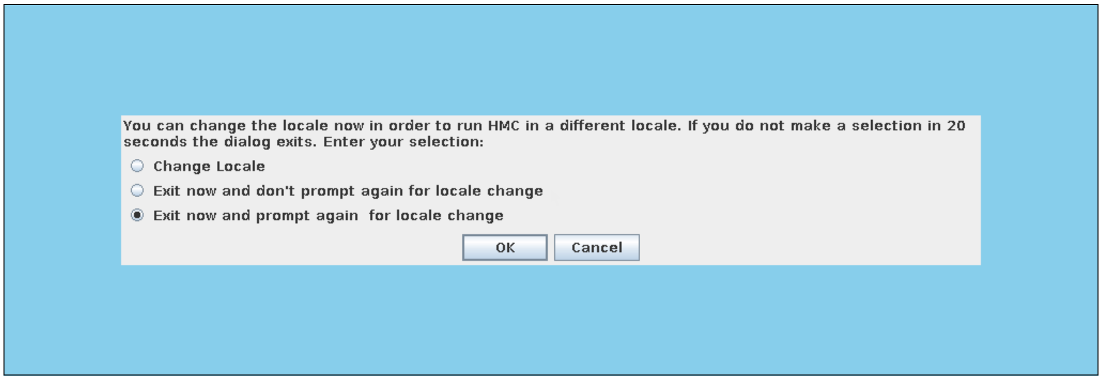
13%

Installing Base Operating System.........

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 3-130   Upgrade Progress

8. The HMC reboots and displays the locale selection dialog box (Figure 3-131). The default action is to display at every boot. It times out after 20 seconds. To change this action, select the appropriate entry from the three options and click **OK**.



You can change the locale now in order to run HMC in a different locale. If you do not make a selection in 20 seconds the dialog exits. Enter your selection:

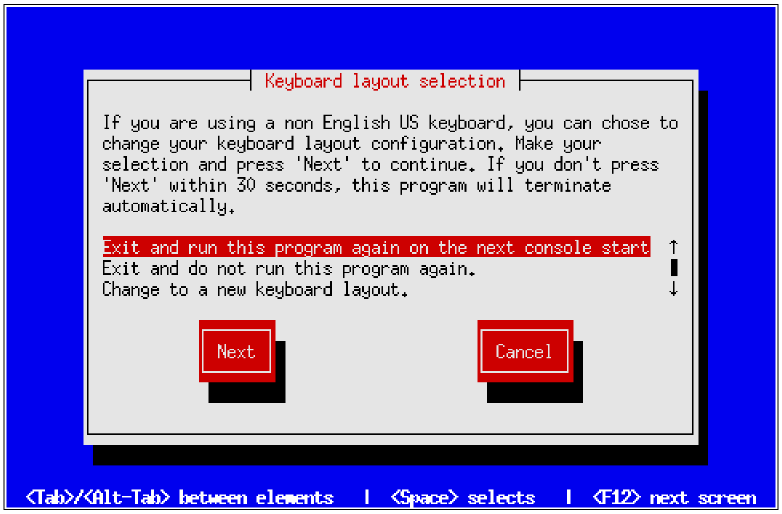
○ Change Locale

○ Exit now and don't prompt again for locale change

● Exit now and prompt again for locale change

Figure 3-131   Local prompt change

9. The Keyboard layout selection panel (Figure 3-132) allows for a non English US keyboard to be selected. You must make a selection within 30 seconds and select **Next** or **Cancel** The panel times out after 30 seconds.

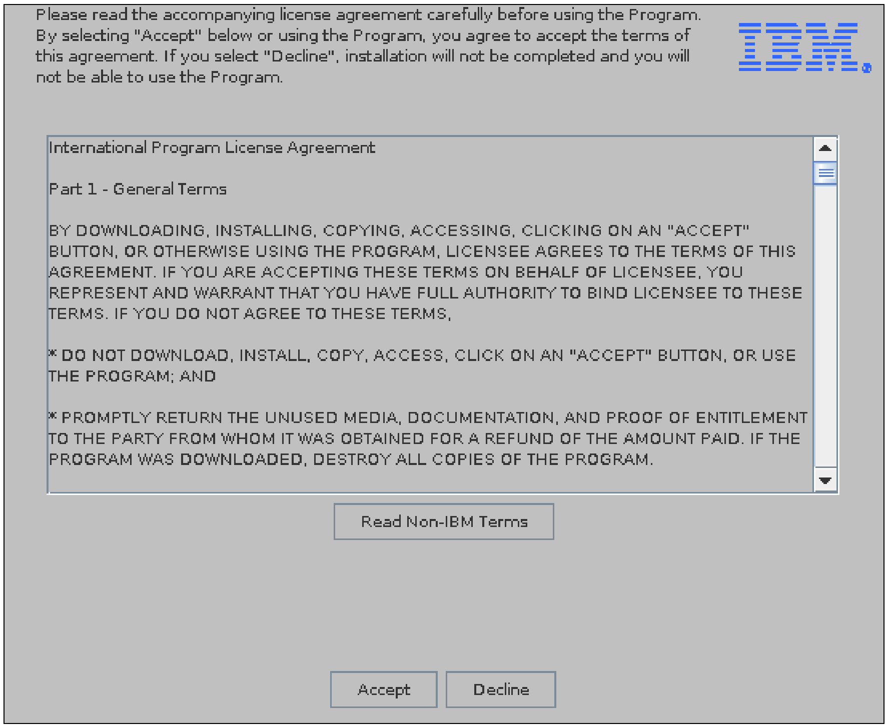


```
Keyboard layout selection

If you are using a non English US keyboard, you can chose to
change your keyboard layout configuration. Make your
selection and press 'Next' to continue. If you don't press
'Next' within 30 seconds, this program will terminate
automatically.

Exit and run this program again on the next console start
Exit and do not run this program again.
Change to a new keyboard layout.
```

Next
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 3-132   Keyboard Layout selection

10. Read the license agreement window and click **Accept** to accept the license and continue. A second license acceptance window opens (Figure 3-133).



Please read the accompanying license agreement carefully before using the Program. By selecting "Accept" below or using the Program, you agree to accept the terms of this agreement. If you select "Decline", installation will not be completed and you will not be able to use the Program.

International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND

* PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

Figure 3-133 Accept License

The HMC is now upgraded to V8.R8.4.0. You can either start to explore the new software level to ensure that your settings were maintained, or have it updated to the latest level of maintenance. For update, see 3.4, “HMC update” on page 243.

4

Configuring

This chapter provides an overview of the main configuration topics of the Hardware Management Console (HMC).

This chapter describes the following topics:

- Network configuration
- User management
- Systems and Console Security options
- Miscellaneous configurations

4.1 Network configuration

This section provides an overview of the types of network configurations for the HMC and explains how to configure HMC network settings. It also describes how to test network connections and obtain network diagnostic information.

4.1.1 Types of HMC network configurations

The HMC supports several network configurations:

- *HMC to managed system connection* performs most of the hardware management functions in which the HMC issues control function request through the service processor of the managed system.
- *HMC to logical partition connection* collects platform-related information such as hardware inventory, from the operating system running in the logical partitions. This communication also coordinates certain platform activities, such as dynamic logical partition (DLPAR) or concurrent maintenance with those operating systems.
- *HMC to remote users connection* provides remote users with access to HMC function. Remote users can access the HMC by using one of the following methods:
  - The remote operation to access all the HMC graphical user interface (GUI) functions remotely.
  - SSH to access the HMC command-line functions remotely.
  - A virtual terminal server for remote access to a virtual logical partition console.
- *HMC to service and support connection* transmits data such as hardware error reports, inventory data, and microcode updates, to and from your service provider. You can use this communication path to make automatic service calls.

All network configuration functions are available under **HMC Management** → **Console Settings**.

There you have three options listed under the Change Network Settings topic:

- View Network Topology
- Test Network Connectivity
- Change Network Settings

4.1.2 Configuring the HMC network settings

This section describes how you view or change the network configuration for the HMC. Select **Change Network Settings** under **HMC Management** → **Console Settings**. There are four tabs (see Figure 4-1 on page 261):

- Identification
- LAN Adapters
- Name Services
- Routing

Identification tab

The Identification tab provides information that is needed to identify the HMC in the network (Figure 4-1). It includes the following information:

- Console name

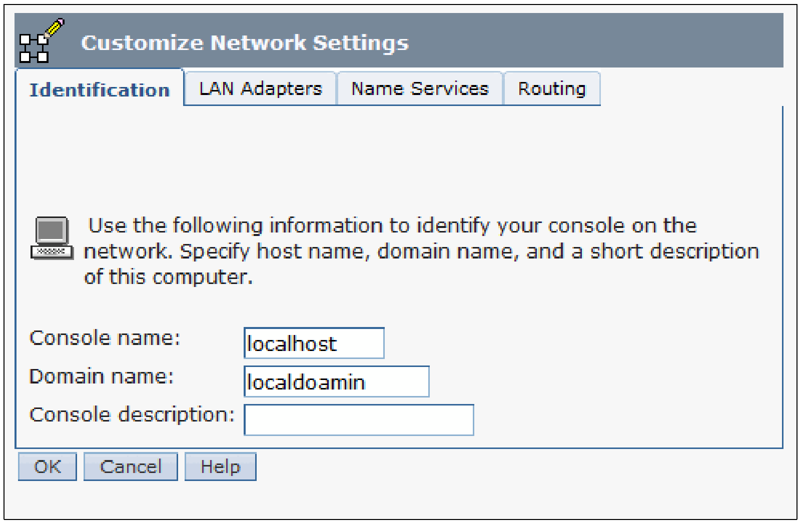
  HMC name that identifies the console to other consoles in the network. This name is the short host name.

- Domain name

  An alphabetic name that the Domain Name Server (DNS) can translate to the Internet Protocol (IP) address.

- Console description

  Short description for the HMC (for example the intended purpose).



Use the following information to identify your console on the network. Specify host name, domain name, and a short description of this computer.

Console name: localhost

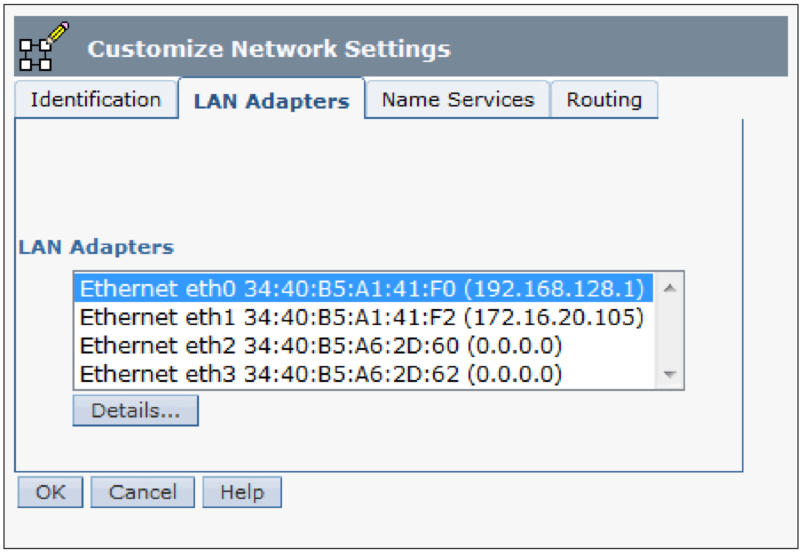
Domain name: localdoamin

Console description:

Figure 4-1 HMC Identification tab on Customize Network Settings pane

LAN Adapters tab

The LAN Adapters tab (Figure 4-2) lists all local area network (LAN) adapters that are installed on the HMC. You can view details of each LAN adapter by clicking **Details**, which starts a window where you can change LAN adapter configuration and firewall settings.

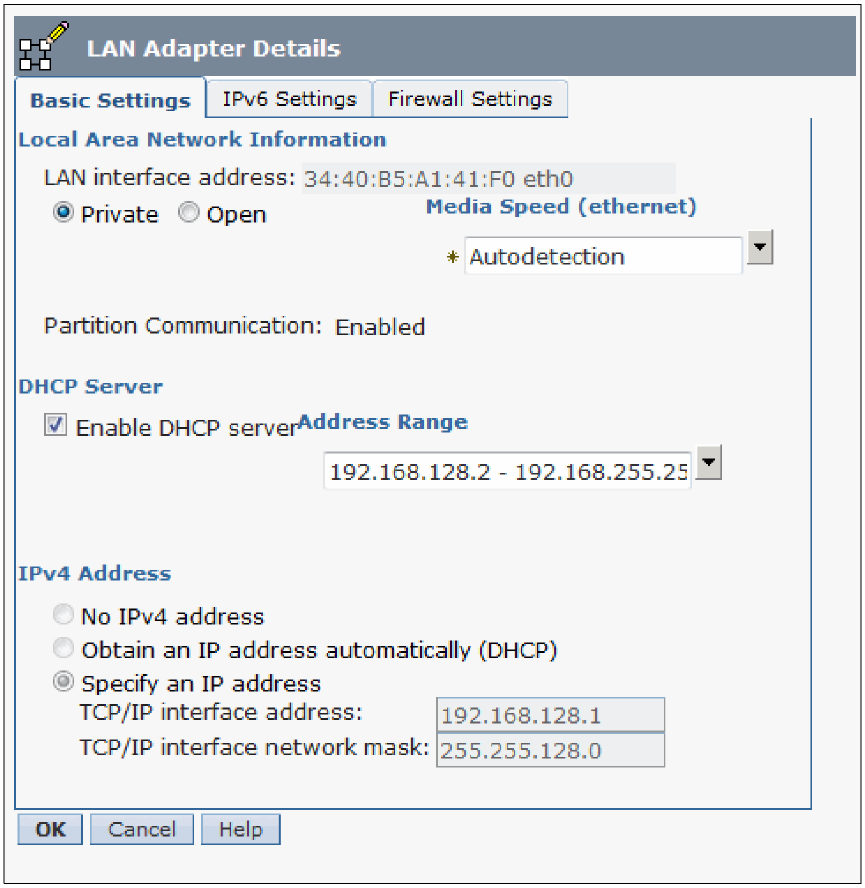


Ethernet eth0 34:40:B5:A1:41:F0 (192.168.128.1)
Ethernet eth1 34:40:B5:A1:41:F2 (172.16.20.105)
Ethernet eth2 34:40:B5:A6:2D:60 (0.0.0.0)
Ethernet eth3 34:40:B5:A6:2D:62 (0.0.0.0)

Figure 4-2 LAN adapters tab on Customize Network Settings pane

LAN Adapters Details - Basic Settings

If you click **Details** on the LAN Adapter tab (shown in Figure 4-2 on page 262), the LAN Adapters Details pane opens to the Basic Settings tab (Figure 4-3). The basic settings describe the LAN adapter configuration of Ethernet *eth0* on the LAN Adapters tab.



Local Area Network Information

LAN interface address: 34:40:B5:A1:41:F0 eth0

● Private ○ Open

Media Speed (ethernet)

* Autodetection

Partition Communication: Enabled

DHCP Server

☑ Enable DHCP server

Address Range

192.168.128.2 - 192.168.255.25

IPv4 Address

○ No IPv4 address

○ Obtain an IP address automatically (DHCP)

● Specify an IP address

TCP/IP interface address: 192.168.128.1

TCP/IP interface network mask: 255.255.128.0

Figure 4-3 Basic Settings tab on LAN Adapter Details pane

The Basic Settings tab of the LAN Adapter Details pane includes the following information:

- Local Area Network Information

  The LAN interface address shows the Media Access Control (MAC) address on the card and the adapter name. These values uniquely identify the LAN adapter. The private network is used by the HMC to communicate with a managed system, and an open network is used to connect the HMC outside the managed system.

- Media Speed

  Media Speed specifies the speed in duplex mode of an Ethernet adapter. The options are Autodetection, 10 Mbps Half Duplex, 10 Mbps Full duplex, 100 Mbps Half Duplex, 100 Mbps Full duplex, or 1000 Mbps Full duplex.

- DHCP Server

  Choose **Enable DHCP Server** only if this adapter is defined as a private network, then choose one range of addresses for the DHCP server to assign to its clients.

- Address Range

  The selectable address ranges include segments from the standard non-routable IP address ranges. Based on the range that is selected, the HMC network interface on the private network is automatically assigned the first IP address of that range, and the service processors are then assigned addresses from the rest of the range.

  The DHCP server in the HMC uses automatic allocation, which means that each unique service processor Ethernet interface is reassigned the same IP address each time it is started. This is done over a unique identifier built from the MAC address for each Ethernet interface, which allows the DHCP server to reassign the same IP parameters.

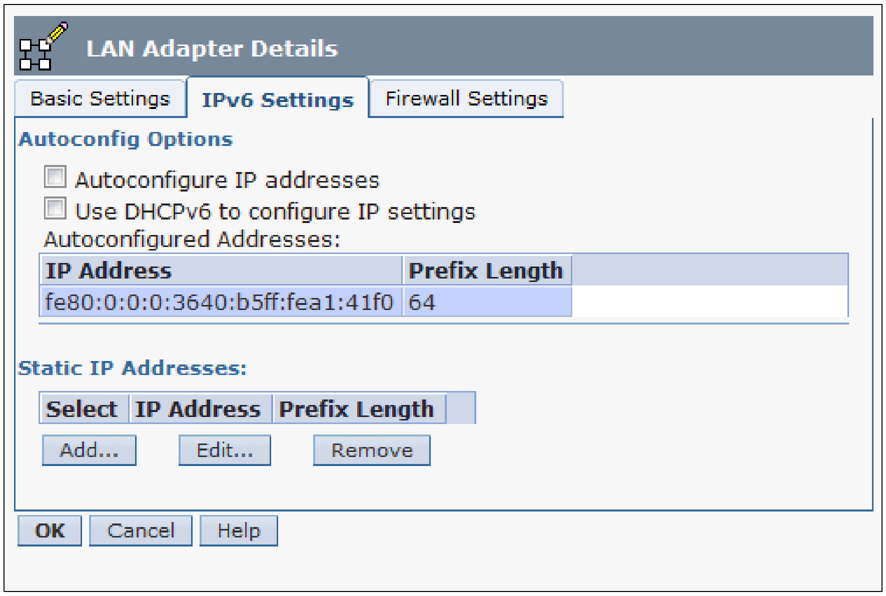
- IPv4 Address

  Three options are offered:

  - **No IPv4 address**: Select if you want to use IPv6.
  - **Obtain an IP address automatically**: Select if you want the HMC to obtain an available IP address automatically from another DHCP server.
  - **Specify an IP address**: Select if you want to specify an IP address, and then provide a TCP/IP interface address and TCP/IP interface network mask.

LAN Adapter Details: IPv6 Settings

The IPv6 Settings tab on the LAN Adapter Details pane (Figure 4-4) describes the IPv6 configuration of Ethernet *eth0* on the LAN Adapters tab.



Autoconfig Options

□ Autoconfigure IP addresses

□ Use DHCPv6 to configure IP settings

Autoconfigured Addresses:

IP Address	Prefix Length
fe80:0:0:0:3640:b5ff:fea1:41f0	64

Static IP Addresses:

Select	IP Address	Prefix Length

Figure 4-4 IPv6 Settings tab on LAN Adapter Details pane

The IPv6 Settings tab includes the following information:

- Autoconfig Options:
  - Autoconfigure IP addresses

    Select this option if you want the HMC to automatically configure IPv6 addresses. If this option is selected, the autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both).

- Use DHCPv6 to configure IP settings

  Select this option if you want to enable stateful autoconfiguration of IPv6 addresses using the DHCPv6 protocol if you have a DHCPv6 server.

- Autoconfigured IP Addresses

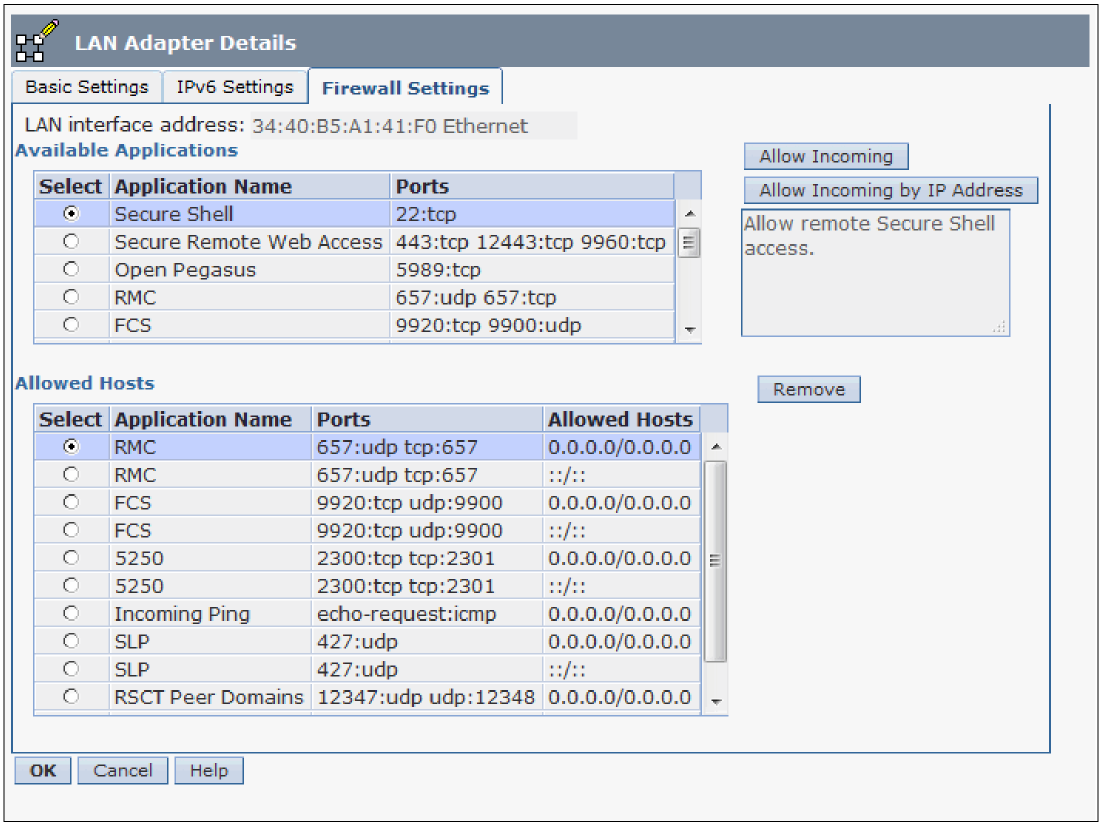
  This table lists the automatically configured IP addresses for this adapter.

- Static IP Addresses

  The table lists the statically configured IPv6 addresses for this adapter. Addresses can be added, selectively changed, or removed from this table through the **Add**, **Edit**, and **Remove** buttons.

LAN Adapters Details - Firewall Settings

The Firewall Settings tab on the LAN Adapters Details pane (Figure 4-5) describes the firewall configuration of Ethernet *eth0*. Use this tab to view and change current firewall adapter settings for the specified LAN interface address. Select an entry and click **Allow Incoming** to allow access to incoming network traffic from this address or click **Allow Incoming by IP Address** to allow access by incoming network traffic from hosts you specify by an IP Address and network mask.



LAN interface address: 34:40:B5:A1:41:F0 Ethernet

Available Applications

Select	Application Name	Ports
●	Secure Shell	22:tcp
○	Secure Remote Web Access	443:tcp 12443:tcp 9960:tcp
○	Open Pegasus	5989:tcp
○	RMC	657:udp 657:tcp
○	FCS	9920:tcp 9900:udp

Allow remote Secure Shell access.

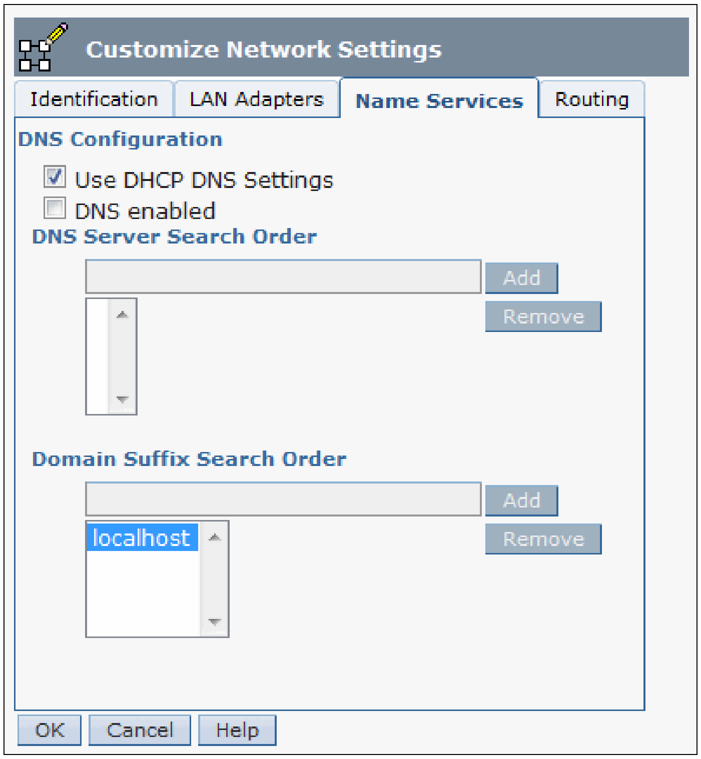
Allowed Hosts

Select	Application Name	Ports	Allowed Hosts
●	RMC	657:udp tcp:657	0.0.0.0/0.0.0.0
○	RMC	657:udp tcp:657	::/::
○	FCS	9920:tcp udp:9900	0.0.0.0/0.0.0.0
○	FCS	9920:tcp udp:9900	::/::
○	5250	2300:tcp tcp:2301	0.0.0.0/0.0.0.0
○	5250	2300:tcp tcp:2301	::/::
○	Incoming Ping	echo-request:icmp	0.0.0.0/0.0.0.0
○	SLP	427:udp	0.0.0.0/0.0.0.0
○	SLP	427:udp	::/::
○	RSCT Peer Domains	12347:udp udp:12348	0.0.0.0/0.0.0.0

Figure 4-5 Firewall Settings Tab on LAN Adapter Details pane

Name Services tab

On the Name Services tab, you can specify DNS for configuring the console network settings (Figure 4-6). DNS is a distributed database system for managing host names and their associated IP addresses.



DNS Configuration

☑ Use DHCP DNS Settings

☐ DNS enabled

DNS Server Search Order

Domain Suffix Search Order

localhost

Figure 4-6 Name Services tab on Customize Network Settings pane

The Name Services tab shows the following information:

- DNS Configuration
  - Use DHCP DNS Settings

    Select this option if you have a DHCP server and want the DNS settings be configured by the DHCP server.
  - DNS enabled

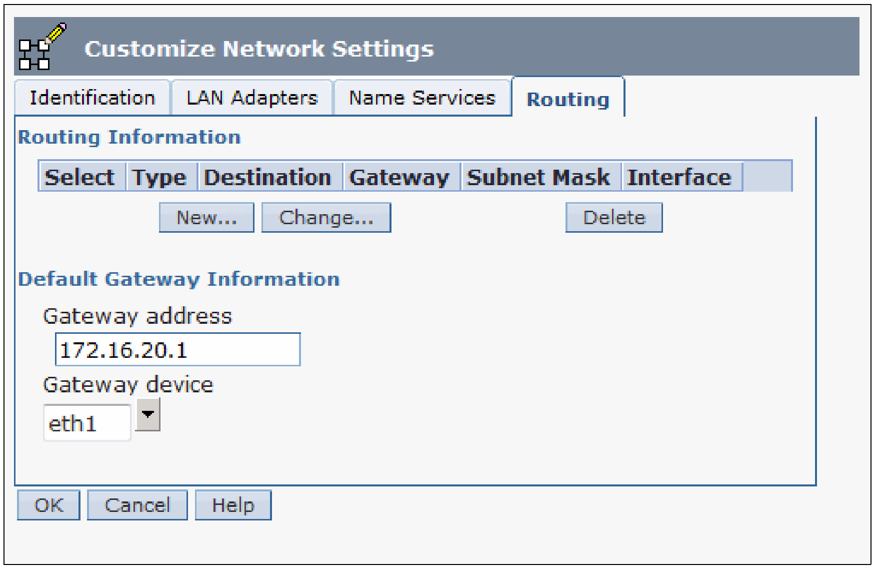
    Select this to enable or deselect to disable the DNS.
- DNS Server Search Order

  Use this area to add IP addresses to or remove them from the search list for mapping the host names to IP addresses. The top suffix will always be searched first.
- Domain Suffix Search Order

  Use this area to add a domain suffix to or remove it from the list to be searched. The top suffix will always be searched first.

Routing tab

Use the Routing tab to specify routing information by configuring the console network settings (Figure 4-7). You can add, delete, or change routing entries and specify routing options for the HMC.



Routing Information

Select	Type	Destination	Gateway	Subnet Mask	Interface

Default Gateway Information

Gateway address: 172.16.20.1

Gateway device: eth1

Figure 4-7 Routing tab on Customize Network Settings pane

The Routing Tab has the following details:

- Routing Information

  This item displays the current static routing information of the HMC. Click **New**, **Change**, or **Delete**, to add, edit, or remove routing entries and specify routing options for the HMC.

  The Routing Information table displays:

  – Net

    Specifies a network-specific route. With a net route, the destination address is the TCP/IP address of a particular network. All TCP/IP communications destined for the network are routed using the TCP/IP address of the router, unless a host route also applies for the communication to the destination host address. When a conflict occurs between a host and net route, the host route is used.

  – Host

    Specifies a host-specific destination. With a host route, the destination address is the TCP/IP address of a particular host. All TCP/IP communications destined for that host are routed through the router using the router address as the TCP/IP address.

  – Default

    Specifies all destinations not defined with another routing table entry. With a default route, the destination address is all zero. If no host or net route applies when communicating with a destination host address, the communications are routed through the default router using the TCP/IP address given by the router address.

  – Destination

    Displays the TCP/IP address of the destination host, network, or subnet.

  – Gateway

    Displays the TCP/IP address of the next hop in the path to the destination.

- Subnet Mask

  Displays the subnet mask used by the network interfaces to add routes.
- Interface

  Displays the name of the network interface which is associated with the table entry.

- Default Gateway Information:
  - Gateway Address

    This area displays the current gateway address. To change it, type a new gateway address in the field.
  - Gateway Device

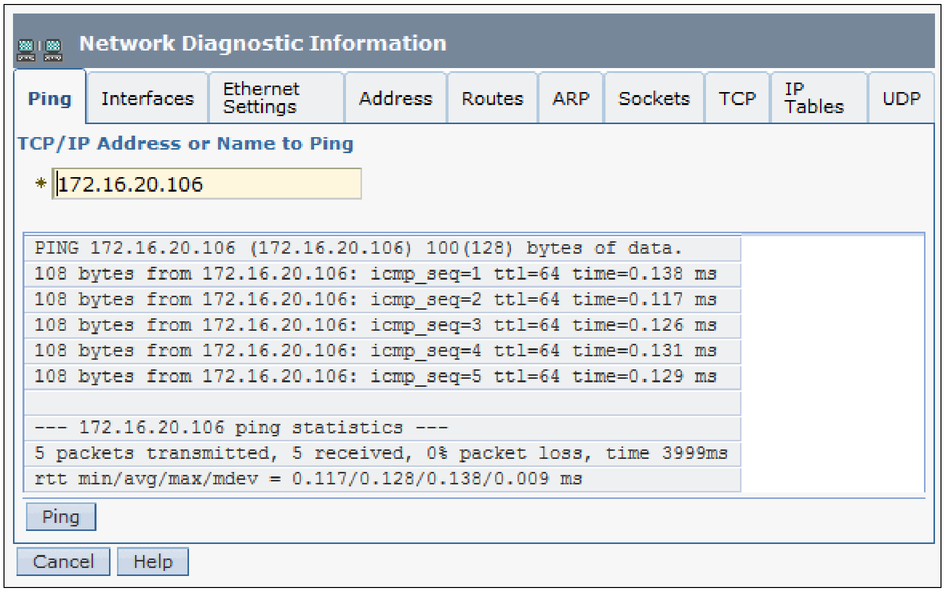
    This area displays the current gateway device. To change it, you can choose another Gateway device from the drop-down list.

4.1.3 Test network connectivity

When you click **Test Network Connectivity** on **HMC Management** → **Console Settings,** the Network Diagnostic Information pane opens (Figure 4-8). Ten Network Diagnostic Information tabs are available. Most of the tabs only display information, which can help you trace connection problems.

- Ping

  Use the Ping function on this tab (Figure 4-8) to send an echo request (`ping`) to a remote host to check whether the host is reachable and to receive information about that TCP/IP address or name. Specify any TCP/IP address or name (if you have DNS configured) in the **TCP/IP Address or Name to Ping** field, then click **Ping**.



TCP/IP Address or Name to Ping

* 172.16.20.106

```
PING 172.16.20.106 (172.16.20.106) 100(128) bytes of data.
108 bytes from 172.16.20.106: icmp_seq=1 ttl=64 time=0.138 ms
108 bytes from 172.16.20.106: icmp_seq=2 ttl=64 time=0.117 ms
108 bytes from 172.16.20.106: icmp_seq=3 ttl=64 time=0.126 ms
108 bytes from 172.16.20.106: icmp_seq=4 ttl=64 time=0.131 ms
108 bytes from 172.16.20.106: icmp_seq=5 ttl=64 time=0.129 ms

--- 172.16.20.106 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.117/0.128/0.138/0.009 ms
```

Figure 4-8 Ping Tab on Network Diagnostic Information pane

- Interfaces

  This tab displays the statistics for the network interfaces currently configured.
- Ethernet Settings

  This tab displays the settings for the Ethernet cards currently configured.

- Address

  This tab displays the TCP/IP addresses for the configured network interfaces. It also displays information and statistics such as the MAC address, dropped packets, packet overruns, and framing errors. This tab is useful for debugging network issues for the HMC.

- Routes

  This tab displays the Kernel IP and IPv6 routing tables and corresponding network interfaces.

- ARP (Address Resolution Protocol)

  This tab displays the contents of the Address Resolution Protocol (ARP) connections.

- Sockets

  This tab displays information about TCP/IP sockets.

- TCP (Transmission Control Protocol)

  This tab displays information about TCP connections.

- IP tables

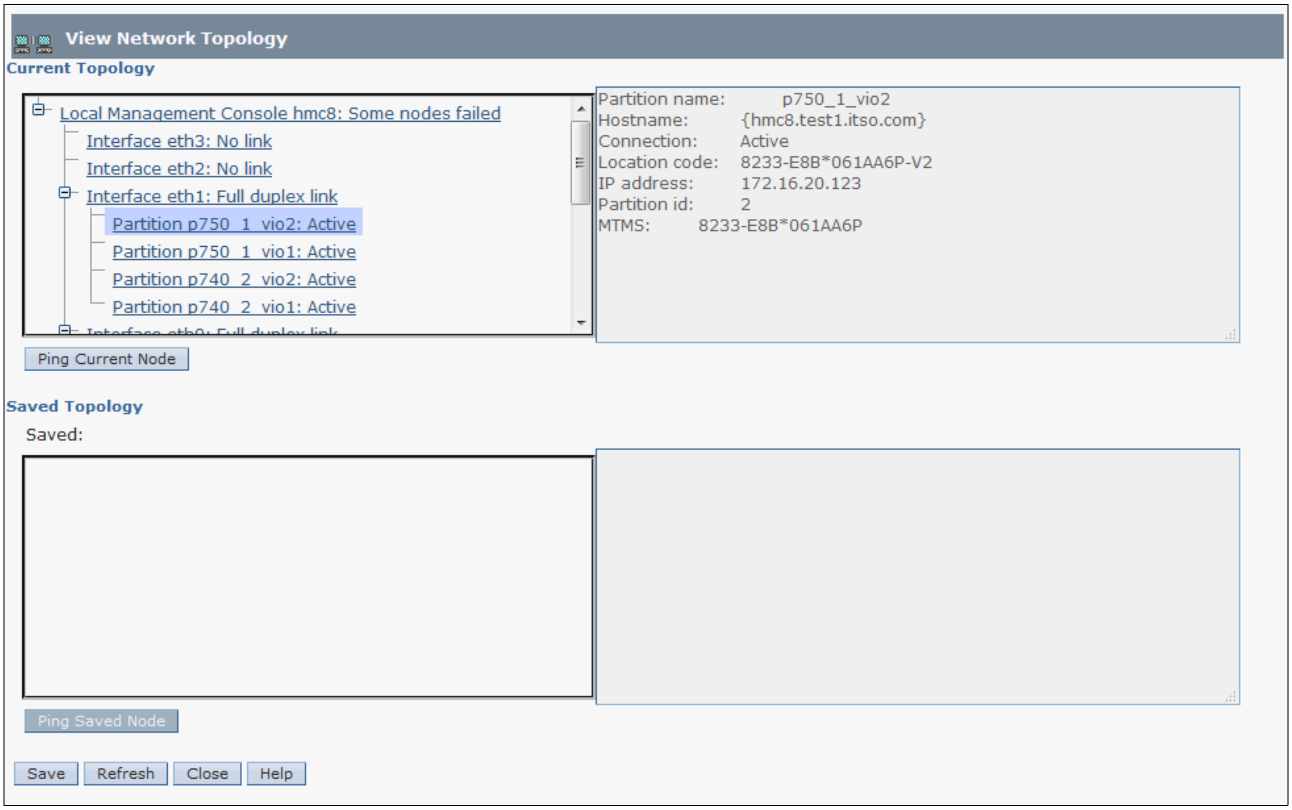
  This tab displays information (in table format) about the IP packet filter rules.

- UDP (User Datagram Protocol)

  This tab displays information about User Datagram Protocol (UDP) statistics.

4.1.4 View network topology

Click **View Network Topology** on the **HMC Management** → **Console Settings** to open the View Network Topology pane (Figure 4-9). This pane shows a tree view of the network nodes known to this HMC. Examples of nodes are managed systems, logical partitions, storage, and other HMCs. You can view attributes of a node by selecting the node in the tree view, under Current Topology. Attributes vary according to the type of node. Some examples are IP address, host name, location code, and status. Click **Refresh** to rediscover the topology and to query the nodes again for status and other attributes.



- Local Management Console hmc8: Some nodes failed
  - Interface eth3: No link
  - Interface eth2: No link
  - Interface eth1: Full duplex link
    - Partition p750_1_vio2: Active
    - Partition p750_1_vio1: Active
    - Partition p740_2_vio2: Active
    - Partition p740_2_vio1: Active
  - Interface eth0: Full duplex link

Partition name: p750_1_vio2
Hostname: {hmc8.test1.itso.com}
Connection: Active
Location code: 8233-E8B*061AA6P-V2
IP address: 172.16.20.123
Partition id: 2
MTMS: 8233-E8B*061AA6P

Figure 4-9 View Network Topology pane

Table 4-1 lists the possible status for each node.

> **Note:** *Unknown* is a possible status for any node where the node has been discovered, but for some reason, the status cannot be determined.

Table 4-1 Possible status for each node

Node	Possible status
Local HMC	All nodes OK; Some nodes failed; All nodes failed
Remote HMC	Online, Offline
Interface	No link; Half duplex link; Full duplex link
Storage Facility	Status not reported.
Managed system	Managed system status reported by the `lssyscfg` command (for example Operating, Running).

Node	Possible status
Service processor	Online, Offline
LPAR	LPAR status reported by the `lssyscfg` command. LPARs can also carry a "Connection status" to report their current network status as one of the following: Active, On, Off, Offline.
BPA (Bulk Power Assembly)	BPA status reported by the `lssyscfg` command
BPC (Bulk Power Controller)	Online, Offline

Each status has its meaning that is evaluated when the cumulative status for the Local HMC node is determined, as shown in Table 4-2.

Table 4-2 Meaning of node status

Status	Evaluation for cumulative status	Meaning
All nodes OK	OK	Child node states are OK.
Some nodes failed	Fail	One or more child node states failed.
All nodes failed	Fail	All child nodes states failed.
No link	Fail	No link detected on interface.
Half duplex link	OK	Half duplex link detected on interface.
Full duplex link	OK	Full duplex link detected on interface.
Active	OK	LPAR is pingable and known to RMC.
On	Fail	LPAR is pingable but not known to RMC.
Off	Fail	LPAR is neither pingable nor known to RMC.
Offline	Fail	► For LPARs: LPAR is not "pingable" but is known to RMC. ► For remote HMCs: Remote HMC is not pingable but is known to this HMC. ► For service processors, BPCs: service processor or BPC are not pingable.
Online	OK	Remote HMC is pingable. Service processor is pingable. BPC is pingable.
Unknown	Fail	Status cannot be determined.
Operating, Running, or any other text from `lssyscfg`	N/A	Not evaluated when determining cumulative status.

This task also allows you to save a snapshot of the current topology and to view that saved reference topology. You can view attributes of a node in those saved topology by selecting the node in the tree view, listed under Saved Topology.

To test network connectivity on a node, select the node in either the current or the saved topology and click **Ping current Node** or **Ping Saved Node**, which is available only for nodes that include an IP address or a host name.

4.2 User management

On an HMC, a user can be a member of various task roles. Each task role allows the user to access different parts of the HMC and to perform different tasks on the managed system. HMC task roles are either *predefined* or *customized*. When you create an HMC user, you must assign a task role to that user. Each task role allows the user varying levels of access to tasks that are available on the HMC interface.

You can assign managed systems and logical partitions to individual HMC users, allowing you to create a user that has access to managed system *A* but not to managed system *B*. Each grouping of managed resource access is called a *managed resource role*.

Table 4-3 lists the predefined HMC task roles, which are the default on the HMC.

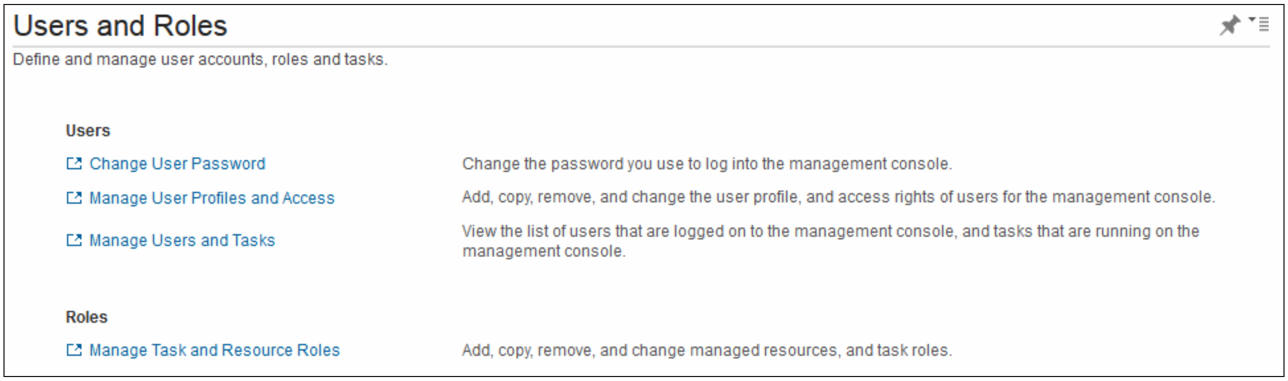
Table 4-3 Predefined HMC task roles

Task role	Description
hmcservicerep	A service representative is an employee who is at your location to install, configure, or repair the system.
hmcviewer	A viewer can view HMC information, but cannot change any configuration information.
hmcoperator	The operator is responsible for daily system operation.
hmcpe	A product engineer assists in support situations, but cannot access HMC user management functions. To provide support access for your system, you must create and administer user IDs with the product engineer role.
hmcsuperadmin	The super administrator acts as the root user or manager of the HMC system. The super administrator has unrestricted authority to access and modify most of the HMC system.

You can create customized HMC task roles by modifying predefined HMC task roles. Creating customized HMC Task Roles is useful for restricting or granting specific task privileges to a certain user.

To reach the user management tasks, select **Users and Security** → **Users and Roles**. The Users and Roles section (Figure 4-10 on page 273) has these options:

- Users: Change User Password
- Users: Manage User Profiles and Access
- Users: Manage Users and Tasks
- Roles: Manage Task and Resource Roles



Users and Roles

Define and manage user accounts, roles and tasks.

Users

Change User Password	Change the password you use to log into the management console.
Manage User Profiles and Access	Add, copy, remove, and change the user profile, and access rights of users for the management console.
Manage Users and Tasks	View the list of users that are logged on to the management console, and tasks that are running on the management console.

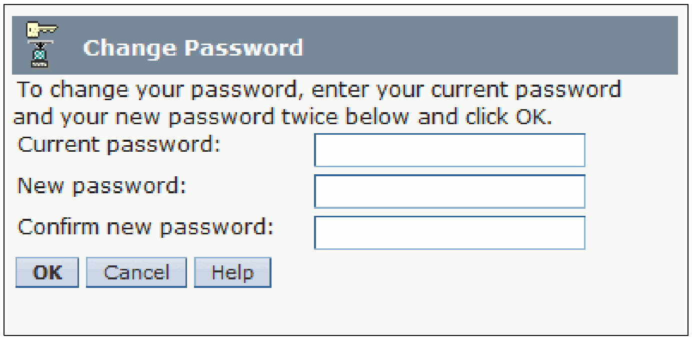
Roles

Manage Task and Resource Roles	Add, copy, remove, and change managed resources, and task roles.

Figure 4-10 Users and Roles options

4.2.1 Change User Password option

Use this option to change the password of the current user (Figure 4-11). The current password is needed for this option; the new password must differ from the current password.



Change Password

To change your password, enter your current password and your new password twice below and click OK.

Current password:

New password:

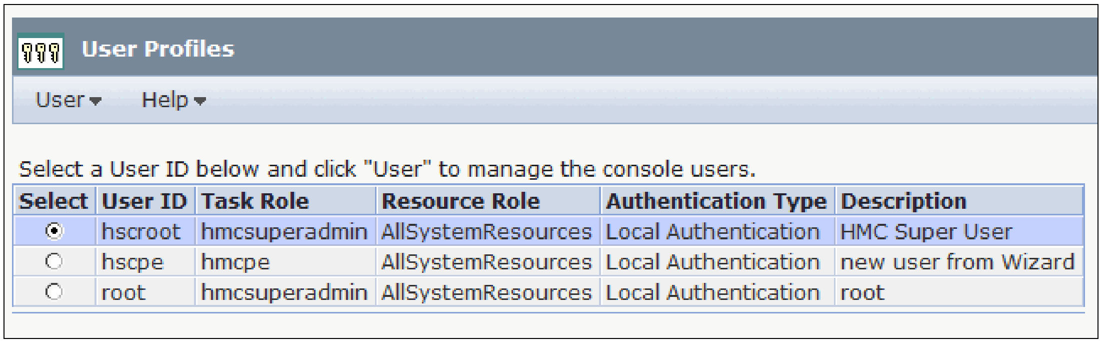
Confirm new password:

Figure 4-11 Change Password window

4.2.2 Manage User Profiles and Access option

Use this option to add, copy, remove, and modify user profiles. Except for the Add User task, you must first select a User ID in the User Profiles pane (Figure 4-12). From the User menu you can then select one of the actions:

- Add
- Copy
- Remove
- Modify/View



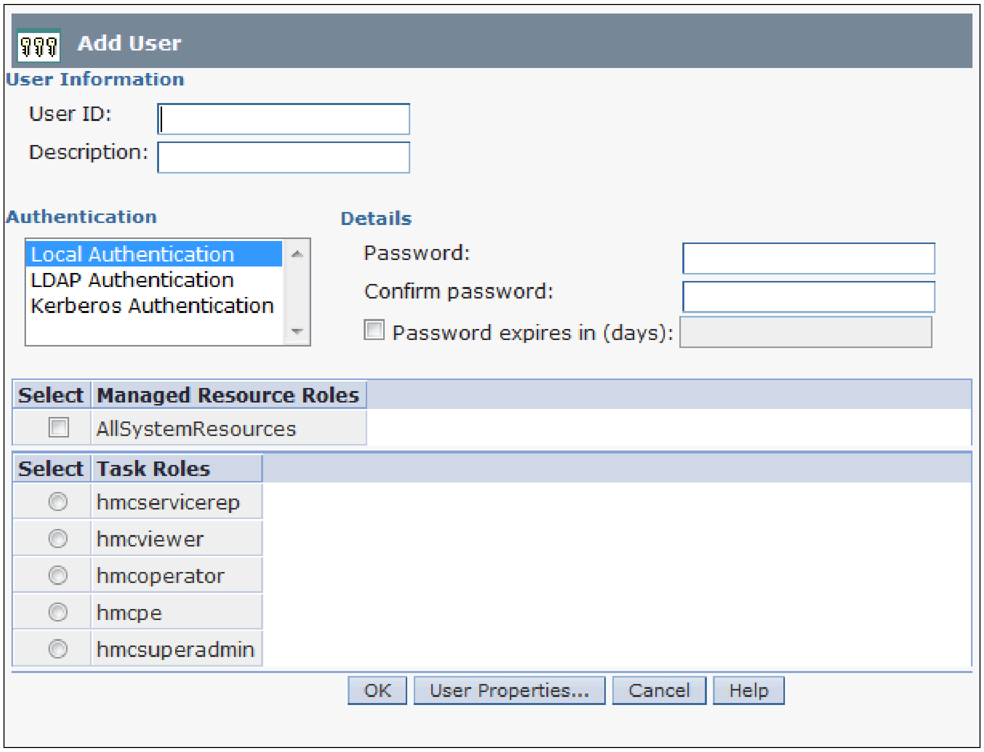
User Profiles

Select a User ID below and click "User" to manage the console users.

Select	User ID	Task Role	Resource Role	Authentication Type	Description
●	hscroot	hmcsuperadmin	AllSystemResources	Local Authentication	HMC Super User
○	hscpe	hmcpe	AllSystemResources	Local Authentication	new user from Wizard
○	root	hmcsuperadmin	AllSystemResources	Local Authentication	root

Figure 4-12 User Profiles pane

When you select **User** → **Add**, a window opens (Figure 4-13) where you specify a new User.



Select	Managed Resource Roles
□	AllSystemResources

Select	Task Roles
○	hmcservicerep
○	hmcviewer
○	hmcoperator
○	hmcpe
○	hmcsuperadmin

Figure 4-13 Add User window

The Add User window is where you can set the following properties:

- User Information:
  - User ID

    The User ID for the user profiles you are creating. The user name must start with an alphabetic character and consist of 1 to 32 characters.
  - Description

    Here you can type a meaningful description for your own records.
- Authentication

  Here you can define the authentication method used for the user ID. These are the valid authentication methods:
  - Local Authentication

    If you select Local Authentication, then in the Details fields, specify a password, confirm the password by specifying it again, and indicate the number of days before that the password is valid before it expires.
  - LDAP Authentication

    If you select LDAP Authentication, no additional information is required.

    Note: Use of LDAP authentication requires configuration of an LDAP server (see 4.3.2, “Manage LDAP option” on page 285).

- Kerberos Authentication

  If you select Kerberos Authentication, specify a Kerberos remote user ID.

  > **Note:** Use of Kerberos authentication requires configuration of a KDC server (see 4.3.3, “Manage KDC option” on page 286).

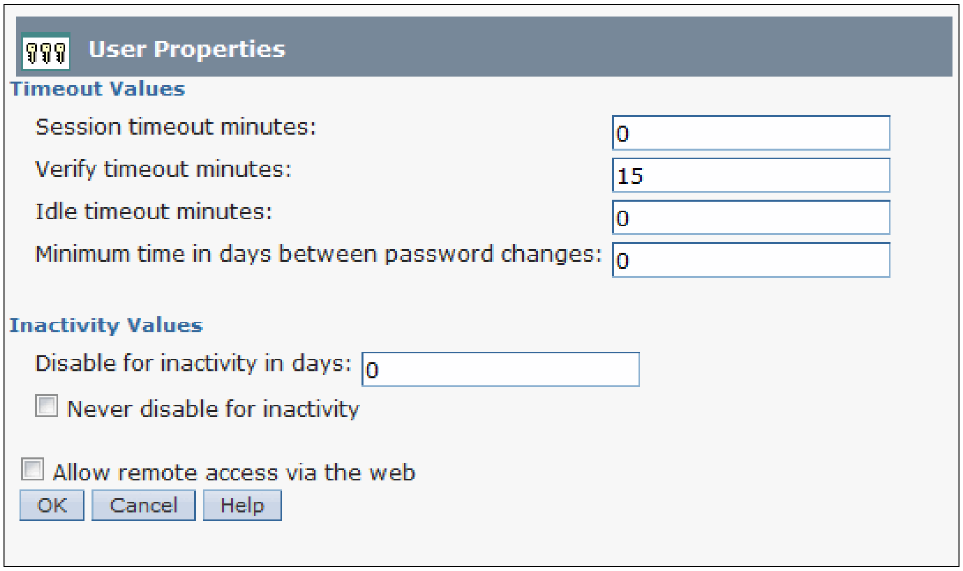
- Managed Resource Roles

  Lists the Managed Resource Roles currently available. Select one or more Managed Resource Roles to define access permissions for this user ID.

- Task Roles

  Lists the task roles currently available. Select one Task role for this user ID.

If you click **User Properties**, more choices are available for setting the properties of a user (Figure 4-14).



User Properties

Timeout Values

Session timeout minutes: 0

Verify timeout minutes: 15

Idle timeout minutes: 0

Minimum time in days between password changes: 0

Inactivity Values

Disable for inactivity in days: 0

□ Never disable for inactivity

□ Allow remote access via the web

Figure 4-14 User Properties window

The User Properties window has the following properties that you can set:

- Timeout Values:
  - Session timeout minutes

    Specifies the number of minutes, during a logon session, that a user is prompted for identity verification. If a password is not re-entered within the amount of time that was specified in the *Verify timeout minutes* field, then the session is disconnected. A zero (0) is the default and indicates no expiration. You can specify up to a maximum value of 525600 minutes (equivalent to one year).

  - Verify timeout minutes

    Specifies the amount of time that is required for the user to re-enter a password when prompted, if a value was specified in the *Session timeout minutes* field. If the password is not re-entered within the specified time, the session will be disconnected. A zero (0) indicates there is no expiration. The default is 15 minutes. You can specify up to a maximum value of 525600 minutes (equivalent to one year).

– Idle timeout minutes

  Specifies the number of minutes the user's session can be idle. If the user does not interact with the session in the specified amount of time, the session becomes disconnected. A zero (0) is the default and indicates no expiration. You can specify up to a maximum value of 525600 minutes (equivalent to one year).

– Minimum time in days between password changes

  Specifies the minimum amount of time in days that must elapse between changes for the user's password. A zero (0) indicates that a user's password can be changed immediately after it was just changed.

  Note: This field is not applicable to an LDAP user ID.

- Inactivity Values:

  – Disable for inactivity in days

    Specifies the amount of time in days a user is temporarily disabled after reaching the maximum amount of days of inactivity. A zero (0) indicates that the user is not disabled after reaching the maximum number of days of inactivity.

  – Never disable for inactivity

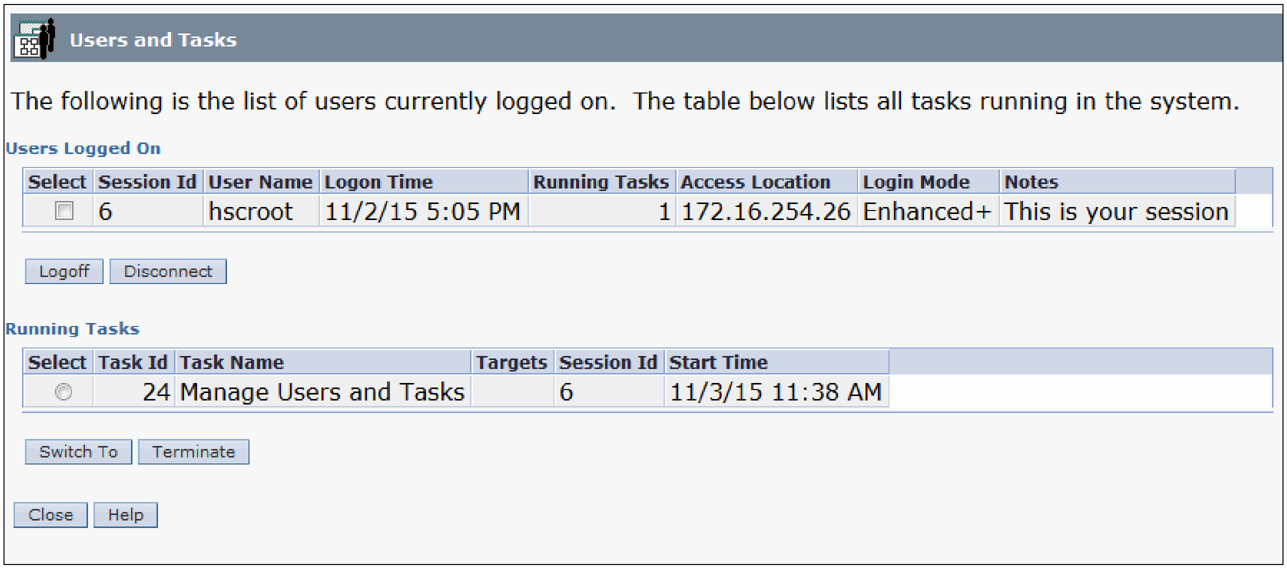
    To not disable user access based on inactivity, select **Never disable for inactivity**.

  – Allow remote access using the web

    To enable remote web server access for the user you are managing, select **Allow remote access via web**. Otherwise the user has access to the HMC only locally or over the command-line using an SSH session.

4.2.3 Manage Users and Tasks option

This option allows you to display a list of users who are currently logged on to the HMC in the Users and Tasks window (Figure 4-15). This window also lists tasks that are running.



Users and Tasks

The following is the list of users currently logged on. The table below lists all tasks running in the system.

Users Logged On

Select	Session Id	User Name	Logon Time	Running Tasks	Access Location	Login Mode	Notes
□	6	hscroot	11/2/15 5:05 PM	1	172.16.254.26	Enhanced+	This is your session

Running Tasks

Select	Task Id	Task Name	Targets	Session Id	Start Time
○	24	Manage Users and Tasks	6		11/3/15 11:38 AM

Figure 4-15 Users and Tasks

The Users and Tasks window has the following sections:

- Users Logged On:
  - Session Id

    Specifies the session identification number associated with the user who is logged on to the HMC.
  - User Name

    Specifies the name of the user who is logged on to the HMC.
  - Logon Time

    Specifies the time that the user logged on to the HMC.
  - Running Tasks

    Specifies the number of tasks currently running for the user.
  - Access Location

    Specifies the location from which the user is accessing the HMC.
  - Notes

    Contains additional and useful information pertaining to the session.

  A user who has the assigned role of Access Administrator can select a user from the list and click **Logoff** or **Disconnect**.
- Running Tasks:
  - Task ID

    Specifies a task identification number associated to the task that is running.
  - Task Name

    Specifies the name of the task that is running.
  - Targets

    Specifies (if any) the object name or names that are targeted for that task.
  - Session Id

    Specifies the identification number associated with the user running the task.
  - Start Time

    Specifies the time the task was started.

  Under the Running Tasks, two buttons are available to use *after* you select a task from the Running Tasks list:
  - **Switch To**: Click this button to switch to another task that is running in your session.
  - **Terminate:** Click this button to end a task that is running in your session. If your user ID has the assigned role of Access Administrator, you can end tasks that are in other sessions.

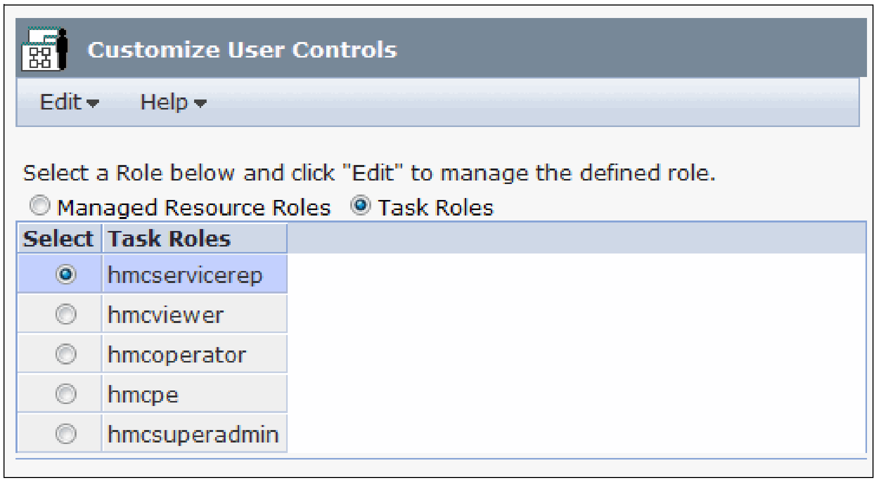
4.2.4 Manage Task and Resource Roles option

You can add, copy, remove, and change managed resources and task roles.

Select **Manage Task and Resource Roles**; the Customize User Controls window opens (Figure 4-16). It offers two options:

- Select **Managed Resource Roles** and select a role from the list of currently defined managed resource roles. Use click the **Edit** menu to add, copy, remove, or modify a managed resource role.
- Select **Task Roles** and select a role from the list of currently defined task roles. Click the **Edit** menu to add, copy, remove, or modify a task role.

> **Note:** Predefined roles (default roles) cannot be modified, but you can create a role that is based on a system defined role or on existing roles.



Select a Role below and click "Edit" to manage the defined role.

○ Managed Resource Roles ● Task Roles

Select	Task Roles
●	hmcservicerep
○	hmcviewer
○	hmcoperator
○	hmcpe
○	hmcsuperadmin

Figure 4-16 Customize User Controls window

Managed resource role tasks

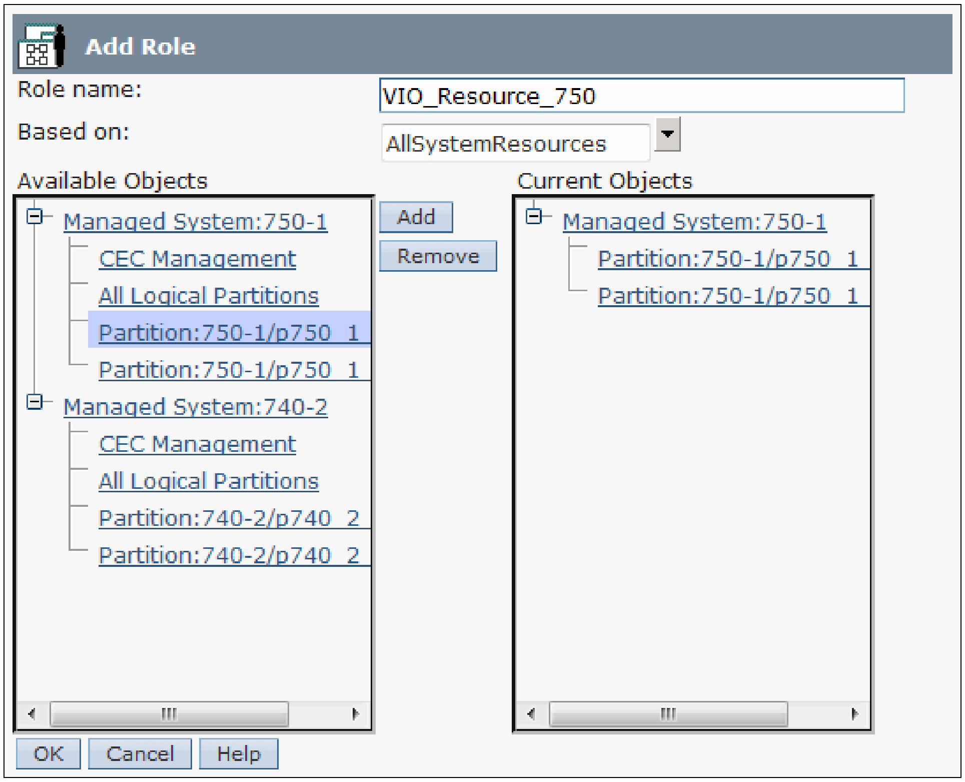
A managed resource role assigns permissions for a managed object or group of objects, such as a managed system or a logical partition. In a managed resource role, you can define access to a specific managed systems rather than all managed systems controlled by the HMC.

You can create a managed resource role, copy an existing managed resource role, modify existing managed resource roles, or delete an existing managed resource role from the Customize User Controls window. By default, only one managed resource role is available: *AllSystemResources*. Select **Managed Resource Roles**, then select an option from the **Edit** menu.

To create a managed resource role, use the following steps:

1. Click **Edit** → **Add**; the Add Role window opens.
2. Enter the name for the new managed resource role, and choose the resource role on which the new managed resource role objects will be based.
3. Select the objects that should be available for the new managed resource role, then click **Add** to add them to the new managed resource role current objects.
4. Click **OK** to create the managed resource role.

Figure 4-17 shows an example of creating a new managed resource role.


Add Role

Role name: VIO_Resource_750

Based on: AllSystemResources

Figure 4-17 Add a new managed resource role

To copy a managed resource role, select a managed resource role and select **Edit** → **Copy**. You cannot copy a user defined managed system role that is created from the **Add** menu, but you can copy system-defined managed resource roles, which are *AllSystemRoles*. From the Copy Role window, you can also customize the object configurations for a new copy of a managed resource role.

To modify existing managed resource roles, select a managed resource role that you want to change, and select **Edit** → **Modify**. You can change the configuration of the objects, then click **OK** to save the changes.

To delete a managed resource role, select the wanted managed resource role and select **Edit** → **Remove**. A message is displayed asking for a *Yes/No* verification.

Task roles

A task role defines the access level for a user to do tasks on the managed object or group of objects, such as managed system or logical partition. Five system-defined task roles exist:

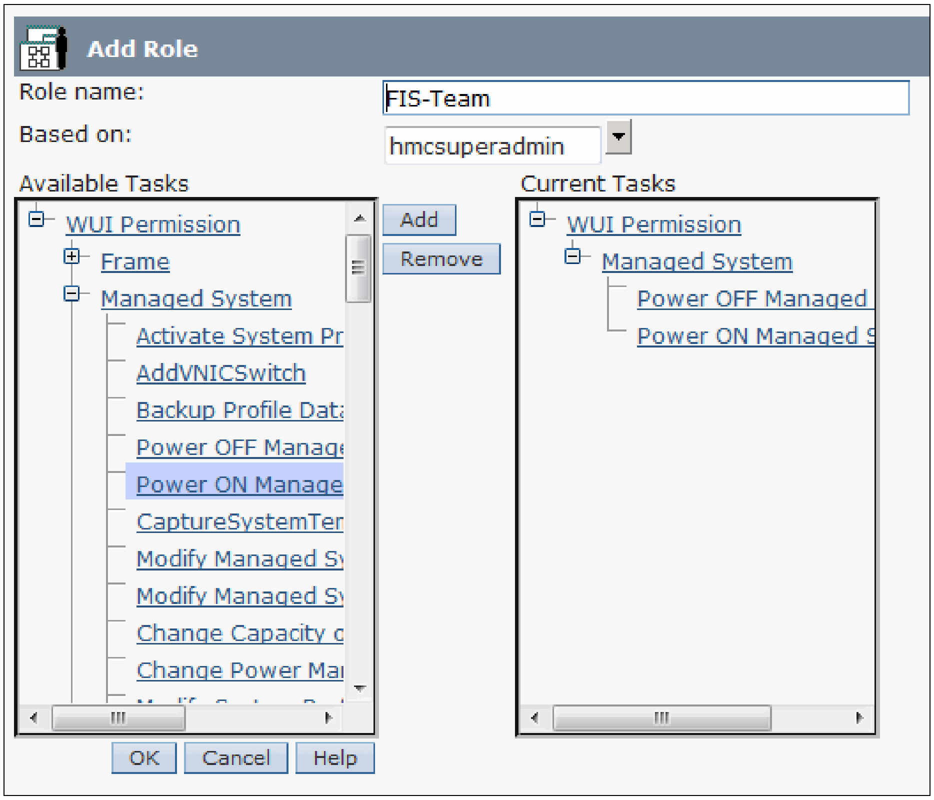
- hmcservicerep
- hmcviewer
- hmcoperator
- hmcpe
- hmcsuperadmin

You can create a task role, and copy, modify, or delete an existing task role from the Customized User Controls window. You cannot modify or remove system-defined task roles. Select **Task Roles**, then select a task from the **Edit** menu.

To create a user task role, use the following steps:

1. Click **Edit** → **Add**; the Add Role window opens.
2. Enter the name for the new managed resource role, and choose the task role on which the new task role objects will be based.
3. Select the objects that should be available for the new task role, and click **Add** to add them to the new task role current objects.
4. Click **OK** to create a task role.

Figure 4-18 shows an example of creating a task role.



Add Role

Role name: FIS-Team

Based on: hmcsuperadmin

Figure 4-18 Add a new task role

To copy a task role, select a task role and then select **Edit** → **Copy**. From the Copy Role window, you can also customize the object configurations for a copy of the task role.

To delete a task role, select a task role and then select **Edit** → **Remove**. A message box displays asking for a *Yes* or *No* verification.

To modify existing task roles, select a task role and then select **Edit** → **Modify**. You can change the configuration of the objects, and then click **OK** to save the changes.

4.2.5 User Password Policy

By default, no password policy is active on an HMC. Although a password policy cannot be enforced by using the GUI, command-line options are available that can enforce a password policy. These four commands are available:

- `chpwdpolicy`

  Activates, disables, or modifies a password policy.

- `lspwpolicy`

  Lists the available password policies.

- `mkpwdpolicy`

  Creates a new password policy. The password policy must be activated with the **`chpwdpolicy`** command.

- `rmpwdpolicy`

  Removes a password policy. Only user-defined password policies can be removed. The active password policy cannot be removed.

For a password policy, the following attributes are available:

- `name`

  The name of the password policy.

- `description`

  A meaningful description of the password policy.

- `min_pwage`

  The number of days that must elapse before a password can be changed.

- `pwage`

  The number of days that can elapse before a password expires and must be changed. A value of 99999 indicates no password expiration.

- `warn_pwaged`

  The number of days prior to password expiration when a warning message will begin to be displayed.

- `min_length`

  The minimum password length.

- `hist_size`

  The number of times a password must be changed before a password can be reused. This value cannot exceed 50.

- `min_digits`

  The minimum number of digits that a password must contain.

- `min_uppercase_chars`

  The minimum number of uppercase characters that a password must contain.

- `min_lowercase_chars`

  The minimum number of lowercase characters that a password must contain.

- `min_special_chars`

  The minimum number of special characters that a password must contain. Special characters include symbols, punctuation, and white space characters.

For a password policy you do not have to use this attributes all at once. You can make a password policy with a subset of the available attributes.

The HMC Medium Security Password Policy is defined by default but not activated. It has the following settings:

- `min_pwage=1`
- `pwage=180`
- `min_length=8`
- `hist_size=10`
- `warn_pwage=7`
- `min_digits=0`
- `min_uppercase_chars=1`
- `min_lowercase_chars=6`
- `min_special_chars=0`

The policy can be activated with the **`chpwpolicy`** command:

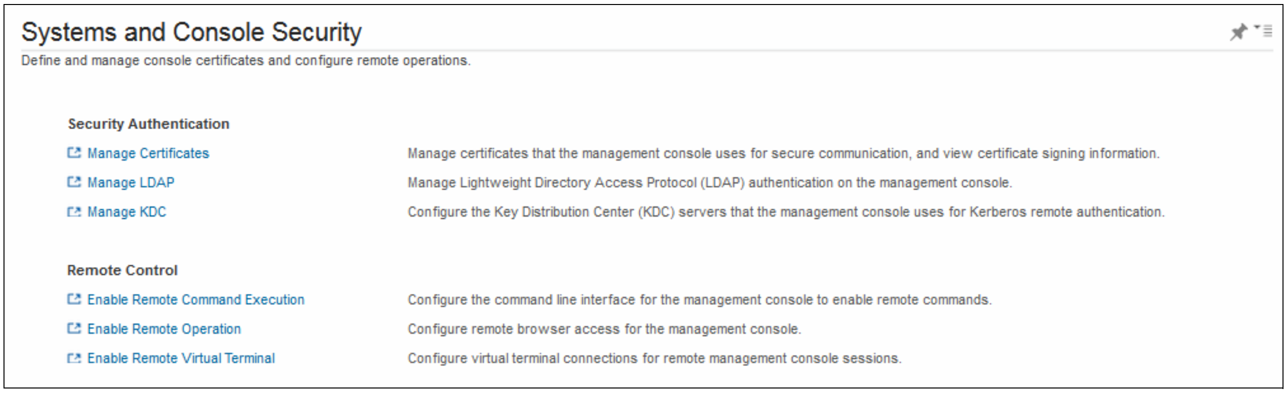
```
chpwdpolicy -o -n “HMC Medium Security Password Policy”
```

And deactivated as follows:

```
chpwdpolicy -o d
```

4.3 Systems and Console Security options

This section describes the security authentication mechanism available on the HMC and the remote control options. To reach the Systems and Console Security options menu (Figure 4-19) from the main window, select **Users and Security** → **Systems and Console Security**.



Systems and Console Security

Define and manage console certificates and configure remote operations.

Security Authentication

Manage Certificates	Manage certificates that the management console uses for secure communication, and view certificate signing information.
Manage LDAP	Manage Lightweight Directory Access Protocol (LDAP) authentication on the management console.
Manage KDC	Configure the Key Distribution Center (KDC) servers that the management console uses for Kerberos remote authentication.

Remote Control

Enable Remote Command Execution	Configure the command line interface for the management console to enable remote commands.
Enable Remote Operation	Configure remote browser access for the management console.
Enable Remote Virtual Terminal	Configure virtual terminal connections for remote management console sessions.

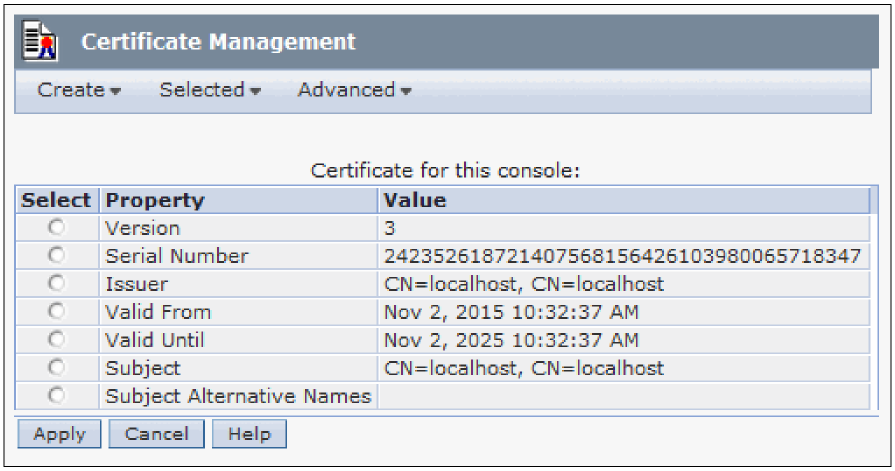
Figure 4-19 Systems and Console Security menu

4.3.1 Manage Certificates option

If you select **Manage Certificates** on the Systems and Console Security menu, the Certificate Management window opens (Figure 4-20 on page 283). Use this window to create, modify, import, or remove certificates.

Security certificates ensure that the HMC can operate securely in the client/server mode. The managed machines are servers and the managed users are clients. Server and client communicate over the Secure Sockets Layer (SSL) protocol, which provides server authentication, data encryption, and data integrity.

When a user wants remote access to the HMC user interface through a web browser, the user requests the secure page by using `https://hmc_hostname`. The HMC then presents its certificate to the remote client (web browser) when establishing connection with the HMC. The browser verifies that the certificate was issued by a trusted party, checks that the dates are still valid, and ensures that the certificate was created for that specific HMC.



Certificate for this console:

Select	Property	Value
○	Version	3
○	Serial Number	242352618721407568156426103980065718347
○	Issuer	CN=localhost, CN=localhost
○	Valid From	Nov 2, 2015 10:32:37 AM
○	Valid Until	Nov 2, 2025 10:32:37 AM
○	Subject	CN=localhost, CN=localhost
○	Subject Alternative Names	

Figure 4-20 Certificate Management window

Create a certificate

You can create a self-signed certificate or a certificate that is signed by a trusted third party. By default the HMC includes a self-signed certificate. Follow these steps to create a certificate that is signed by a certificate authority:

1. Select **Create** → **New Certificate** in the Certificate Management window.
2. You are given the option of creating a self-signed certificate or a certificate that is signed by a certificate authority. So select that the certificate is **Signed by a Certificate Authority**.
3. The New Certificate window opens. Complete the New Certificate form and click **OK**.
4. At the window prompt, choose a location in which to store the certificate:
   - **Removable media on the console**
   - **The file system on the system running the browser**
5. A message box asks for save verification. Click **OK** to save the Certificate Signing Request as a file. You are then prompted if you want to use a temporary self-signed certificate until your certificate is signed and returned. Clicking **Yes** creates a self-signed certificate. You are returned to the Certificate Management window (Figure 4-20). Many of the values will display as `Not available until changes applied`.
6. Click **Apply** to apply the new self signed certificate. The values are updated after the certificate is applied and the console is restarted. The next window asks for verification to replace the current certificate.
7. Click **Yes** to proceed. You are then presented with a message box asking if the certificate was replaced successfully or if any errors occurred.
8. Click **OK**. The console restarts.
9. After your certificate request is signed and returned, you have to import the certificate and apply by clicking **Advanced** → **Import Certificate** on the Certificate Management window that is shown in Figure 4-20. After the certificate is imported, apply it and restart the console.

Modifying existing certificates

You can modify certain properties of an existing certificate. To modify a certificate, select the radio button of the entry that you want to modify on the Certificate Management window, then click **Selected** → **Modify**. Modifiable properties include the following components:

- Valid Until
- Subject
- Subject Alternative Name

Advanced options for modifying existing certificates

Several advanced options are available for working with certificates under the Advanced menu on the Certificate Management window. You can do the following actions:

- Delete and Archive Certificate

  Remove the current certificate. After deleted, the certificate is archived on the HMC.

- Work with Archive Certificate

  View and restore archived certificates. To restore an archived certificate, select **Actions** → **Install**. A window displays asking for verification for restoring the certificate. Click **Yes** to proceed. The console will be restarted, if the installation is successful.

- Import certificate

  Import a certificate from media or a remote file system. Select the location of the certificate to import. After the certificate is uploaded, you must apply and restart the console.

- View Issuer certificate

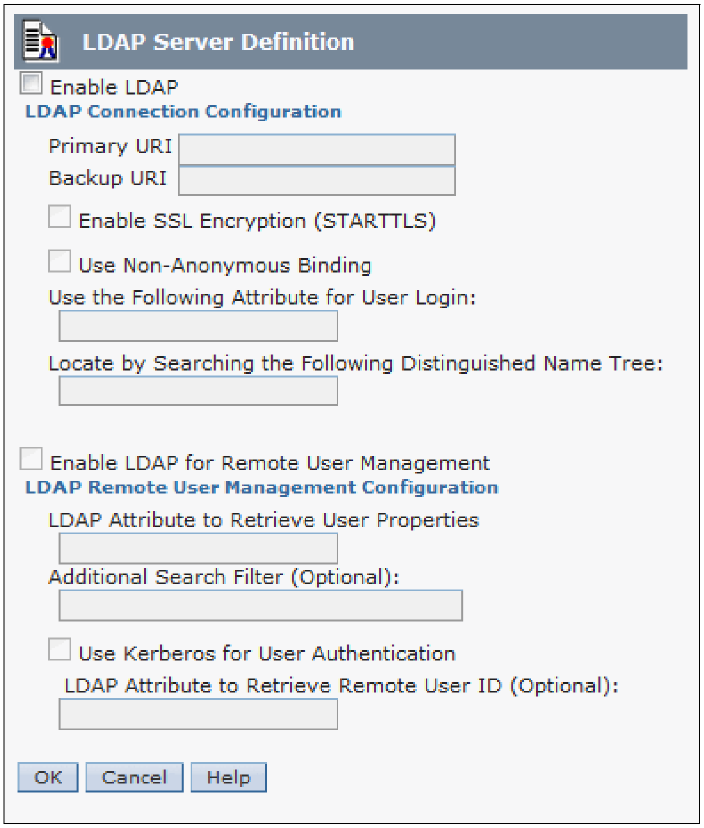
  Display the available information about the issuer of the certificate.

- Import Repository

  Import a keystore containing one or more certificates into the HMC keystore. You can import a keystore from media or a remote file system. Select the location of the keystore to import. When the keystore is imported, you must apply and restart the console.

4.3.2 Manage LDAP option

If you select **Manage LDAP** on the Systems and Console Security menu, the Lightweight Directory Access Protocol (LDAP) Server Definition window opens (Figure 4-21). Use this window to enable LDAP authentication on this HMC, to view LDAP servers that are used by this HMC for LDAP remote authentication, to add LDAP servers, or to remove LDAP servers from this HMC.



LDAP Server Definition

□ Enable LDAP

LDAP Connection Configuration

Primary URI

Backup URI

□ Enable SSL Encryption (STARTTLS)

□ Use Non-Anonymous Binding

Use the Following Attribute for User Login:

Locate by Searching the Following Distinguished Name Tree:

□ Enable LDAP for Remote User Management

LDAP Remote User Management Configuration

LDAP Attribute to Retrieve User Properties

Additional Search Filter (Optional):

□ Use Kerberos for User Authentication

LDAP Attribute to Retrieve Remote User ID (Optional):

Figure 4-21 LDAP Server definition window

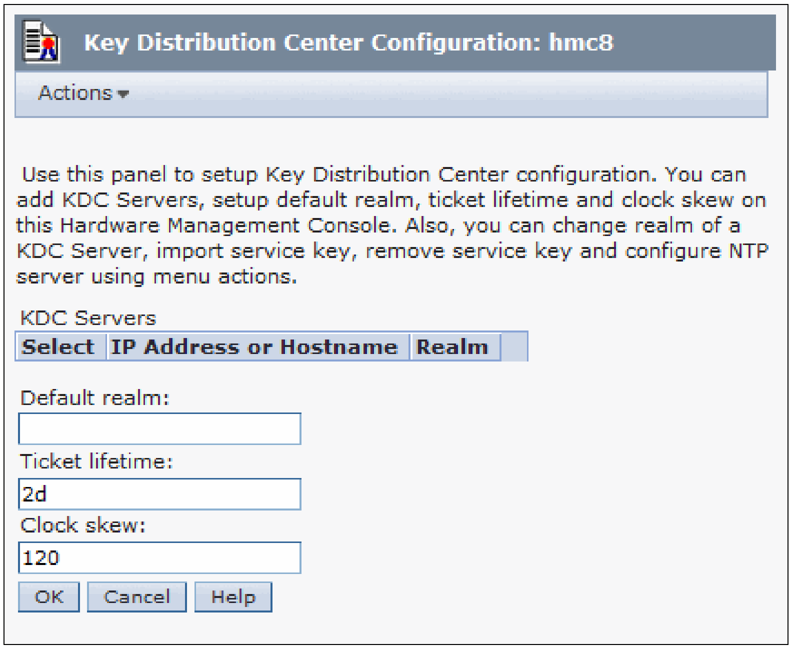
To use LDAP remote authentication for this HMC, complete the following prerequisites:

- Enable LDAP authentication from this window.
- Define an LDAP server to use for authentication by suppling at least a primary Uniform Resource Identifier (URI) for the LDAP server you want.
- Define the search base (distinguished name tree) for the LDAP server.
- For each remote person who will use LDAP authentication, set the user profile to use LDAP remote authentication instead of local authentication, even when the user logs on to the HMC locally. For changing user profiles, see 4.2.2, “Manage User Profiles and Access option” on page 273.
- Ensure that a working network connection exists between the HMC and the LDAP server.

The HMC authenticates with the LDAP server by means of an anonymous connection by default. You can use the **`chhmcldap`** command on the command line to set the bind distinguished name (DN) and bind password for non-anonymous binding with the LDAP server. You can use the **`ldapsearch`** command to verify the LDAP setup on the HMC.

4.3.3 Manage KDC option

If you select **Manage KDC** (Key Distribution Center) on the Systems and Console Security menu, the Key Distribution Center Configuration window opens (Figure 4-22). Use this window to view the KDC servers that are used by this HMC for Kerberos authentication, and to add KDC servers or remove KDC servers from this HMC. Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.



Use this panel to setup Key Distribution Center configuration. You can add KDC Servers, setup default realm, ticket lifetime and clock skew on this Hardware Management Console. Also, you can change realm of a KDC Server, import service key, remove service key and configure NTP server using menu actions.

KDC Servers

Select	IP Address or Hostname	Realm

Default realm:

Ticket lifetime: 2d

Clock skew: 120

Figure 4-22 Key Distribution Center Configuration window

To use Kerberos authentication for this HMC, complete the following prerequisites:

- Enable NTP service on the HMC and set the KDC servers to synchronize time with the same NTP server. For enabling NTP, see "NTP Configuration tab" on page 290.
- Set the user profile of each remote user, which shall authenticate with Kerberos, to use Kerberos authentication instead of local authentication. For changing user profile see 4.2.2, "Manage User Profiles and Access option" on page 273.
- Ensure that a working network connection exists between the HMC and the KDC server.

You can optionally import a service-key file into the HMC. The service-key file contains the host principal that identifies the HMC to the KDC server. Service-key files are also known as *keytabs*.

To add a new KDC server to this HMC, click **Actions** → **Add KDC Server**, and enter the realm and the host name or IP address of the KDC server.

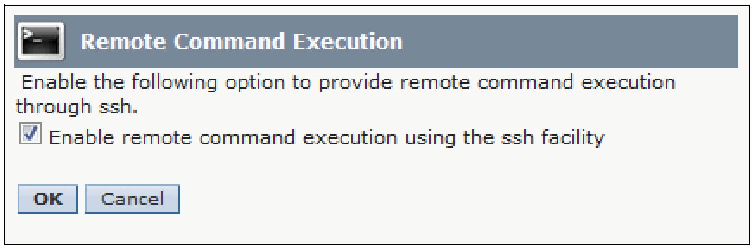
To remove a KDC server from this HMC, select the KDC server that you want to remove in the **KDC Servers table**, click **Actions** → **Remove KDC Server**.

To import a service-key file into this HMC, click **Actions** → **Import Service Key**. After importing a service-key file into the HMC, reboot the HMC for the change to take effect.

To delete a service-key file from this HMC, click **Actions** → **Remove Service Key**. Reboot the HMC after deleting a service-key file from the HMC.

4.3.4 Enable Remote Command Execution option

If you select **Enable Remote Command Execution** on the Systems and Console Security menu, the Remote Command Execution window opens (Figure 4-23). To enable command-line access to the HMC through SSH, select **Enable remote command execution using the ssh facility**.



Remote Command Execution

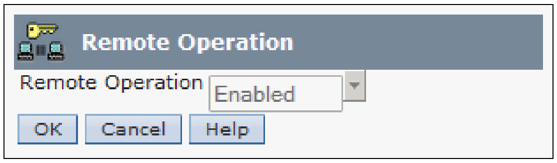
Enable the following option to provide remote command execution through ssh.

☑ Enable remote command execution using the ssh facility

Figure 4-23 Enable remote command execution

4.3.5 Enable Remote Operation option

If you select **Enable Remote Operation** on the Systems and Console Security menu, the Remote Operation window opens (Figure 4-24). Use this window to control whether the HMC can be operated by using a web browser from a remote workstation. By default, remote browser access to the HMC is disabled.



Remote Operation

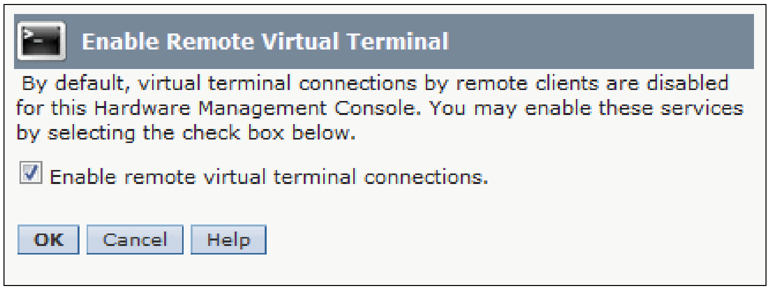
Remote Operation: Enabled

Figure 4-24 Enable remote operation

Note: If you access the HMC remotely, you cannot change the status in this task.

4.3.6 Enable Remote Virtual Terminal option

If you select **Enable Remote Virtual Terminal** on the Systems and Console Security menu, the Enable Remote Virtual Terminal window opens (Figure 4-25). Use this window to enable remote virtual terminal access for remote clients. A remote virtual terminal connection is a terminal connection to a logical partition from another remote HMC. To enable remote virtual terminal access, select **Enable remote virtual terminal connections**.



Enable Remote Virtual Terminal

By default, virtual terminal connections by remote clients are disabled for this Hardware Management Console. You may enable these services by selecting the check box below.

☑ Enable remote virtual terminal connections.

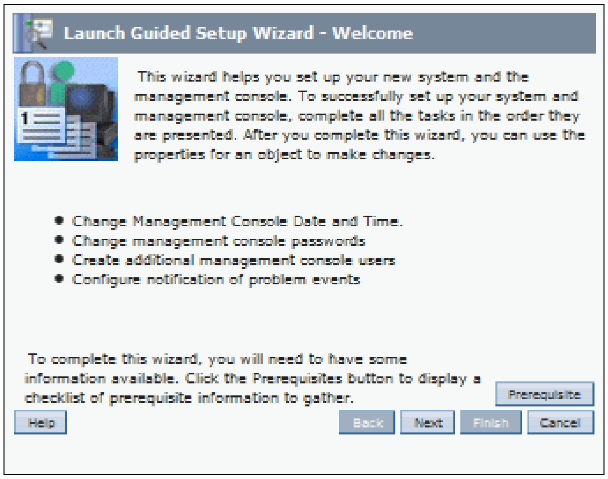
Figure 4-25 Enable remote virtual terminal

4.4 Miscellaneous configurations

This section describes further configuration topics for the HMC.

4.4.1 Launch Guided Setup Wizard selection

From the main window, select **HMC Management** → **Console Settings** → **Launch Guided Setup Wizard**. The Launch Guided Setup Wizard welcome window opens (Figure 4-26). Use the wizard to create additional users, change passwords, change date and time, and configure customer notifications for problem events.



Launch Guided Setup Wizard - Welcome

This wizard helps you set up your new system and the management console. To successfully set up your system and management console, complete all the tasks in the order they are presented. After you complete this wizard, you can use the properties for an object to make changes.

- Change Management Console Date and Time.
- Change management console passwords
- Create additional management console users
- Configure notification of problem events

To complete this wizard, you will need to have some information available. Click the Prerequisites button to display a checklist of prerequisite information to gather.

Figure 4-26 Launch Guided Setup Wizard welcome page

You must have certain information available before you can complete the wizard. To see what you need, click **Prerequisite** to view the list of prerequisites.

The panels of the wizard are explained in 3.3, “HMC Install Wizard” on page 223. However, the wizard follows this chronological list of the panels:

- Change Management Console Date and Time
- Change hscroot Password
- Change root Password
- Create Additional management console users
- Configure HMC network settings (not from a remote session available)
- Configure Notification of Problem Events
- Summary

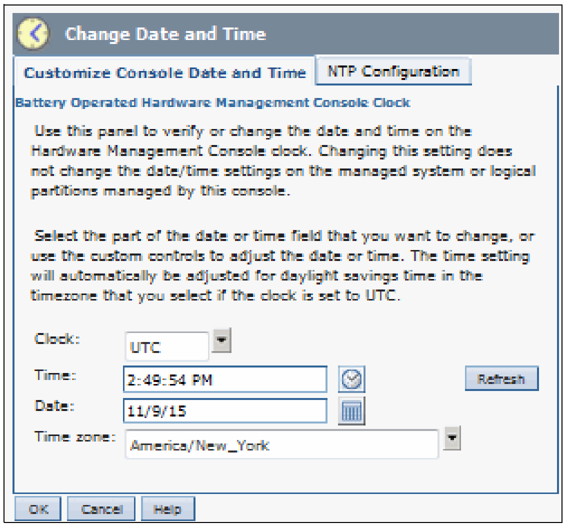
If you are satisfied with the changes you made, click **Finish**. A window opens from which you can launch the Call-Home Setup Wizard (see 6.4, “Connectivity” on page 434).

4.4.2 Change Performance Monitoring Settings selection

From the main window select **HMC Management** → **Console Settings** → **Change Performance Monitoring Settings** to view or change performance monitoring settings. For more information, see 7.2, “Enabling Performance and Capacity Monitor data collection” on page 512.

4.4.3 Change Date and Time selection

From the main window select **HMC Management** → **Console Settings** → **Change Date and Time** to set the date and time of the battery-operated clock on the HMC, and to add or remove time servers for the Network Time Protocol (NTP) service. The Change Date and Time window opens (Figure 4-27).



Change Date and Time

Battery Operated Hardware Management Console Clock

Use this panel to verify or change the date and time on the Hardware Management Console clock. Changing this setting does not change the date/time settings on the managed system or logical partitions managed by this console.

Select the part of the date or time field that you want to change, or use the custom controls to adjust the date or time. The time setting will automatically be adjusted for daylight savings time in the timezone that you select if the clock is set to UTC.

Clock: UTC
Time: 2:49:54 PM
Date: 11/9/15
Time zone: America/New_York

Figure 4-27 Change Date and Time window

The window has two tabs:

- Customize Console Date and Time
- NTP Configuration

Customize Date and Time tab

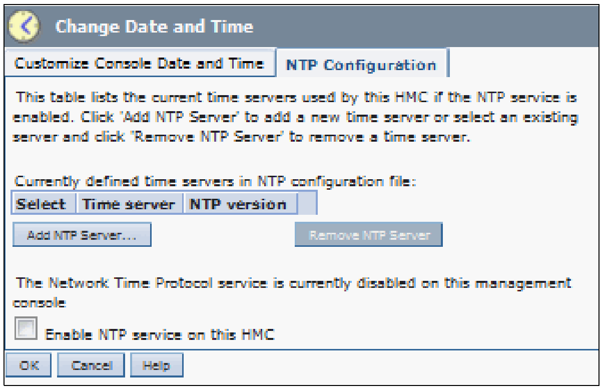
Use the Customize Date and Time tab to change the date, time, and time zone settings for the battery-operated clock on the HMC. The time setting adjusts automatically for daylight savings time in the time zone you select.

You generally use this tab in the following situations:

- The battery is replaced in the HMC.
- Your system is physically moved to a different time zone.

NTP Configuration tab

Use the NTP Configuration tab (Figure 4-28) to enable or disable NTP service for this HMC and to add or remove defined time servers in the NTP configuration file.



This table lists the current time servers used by this HMC if the NTP service is enabled. Click 'Add NTP Server' to add a new time server or select an existing server and click 'Remove NTP Server' to remove a time server.

Currently defined time servers in NTP configuration file:

Select	Time server	NTP version

The Network Time Protocol service is currently disabled on this management console

□ Enable NTP service on this HMC

Figure 4-28 NTP Configuration tab

NTP was developed as an Internet protocol to synchronize the clocks of computers to some time reference. NTP synchronizes time between systems to ensure various items, for example that transactions and recovery procedures have the same time reference.

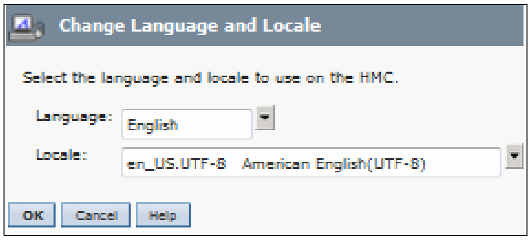
To enable NTP, select the **Enable NTP on this HMC** check box; if you do not select this option, NTP is disabled on this HMC.

The currently defined time servers in the NTP configuration file are listed in the tab's table.

- To add a time server host name or IP address to the NTP configuration file, click **Add NTP Server** and specify the host name or IP address.
- To delete an NTP server from the configuration file and from the list, select a server from the list and click **Remove NTP Server**.

4.4.4 Change Language and Locale selection

From the main window, select **HMC Management** → **Console Settings** → **Change Language and Locale** to set the language and locale for the HMC. The Change Language and Locale window opens (Figure 4-29). First, select a language, and then select a locale associated with that language. The language and local settings determine the language, the character set, and other settings specific to the country or region (such as formats for date, time, numbers, and monetary units). The settings are effective after a reboot of the HMC.



Select the language and locale to use on the HMC.

Language: English

Locale: en_US.UTF-8 American English(UTF-8)

Figure 4-29 Change Language and Locale window

> **Note:** Changes made in this window affect only the language and locale for the HMC. If you access the HMC remotely, the language and locale settings on your browser determine the settings that the browser uses to display the HMC interface.

5

Operating

This chapter describes a general overview of the Hardware Management Console (HMC) operation, including resource (server, partition, frame) management, HMC management, remote access logical partitions from HMC, and partition data management.

This chapter describes the following topics:

- User interfaces
- Management of the HMC
- Console Management
- Resource management
- Systems Management for Servers
- Partition management
- Dynamic partitioning
- Virtual Network management
- Virtual Storage management
- Managing hardware-virtualized I/O adapters
- Capacity on Demand (CoD)

5.1 User interfaces

You can use the various available interfaces to manage the HMC and Power Server resources.

5.1.1 Web-based user interface

This section demonstrates how to use the web-based user interface of the HMC.

HMC V8.R8.1 brought a major change to the existing web-based user interface. With the new Enhanced+ interface, the HMC is now meet today's cloud requirements.

Web browser considerations

HMC web browser support has these requirements:

- HTML 2.0, Javascript 1.0, Java Virtual Machine (JVM), Java Runtime Environment (JRE) Version 8 U45 or later.
- The web browser must use HTTP 1.1.
- Cookie support, pop-ups and Javascript must be enabled for your HMC.

The following browsers were tested with HMC V8.R8.4.0:

- Google Chrome Version 43
- Microsoft Internet Explorer 11
- Mozilla Firefox Version 31 Extended Support Release (ESR)
- Mozilla Firefox Version 38 Extended Support Release (ESR)

For other untested browsers, session cookies must be enabled in order for the Advanced System Management Interface (ASMI) to work.

Log in to the HMC

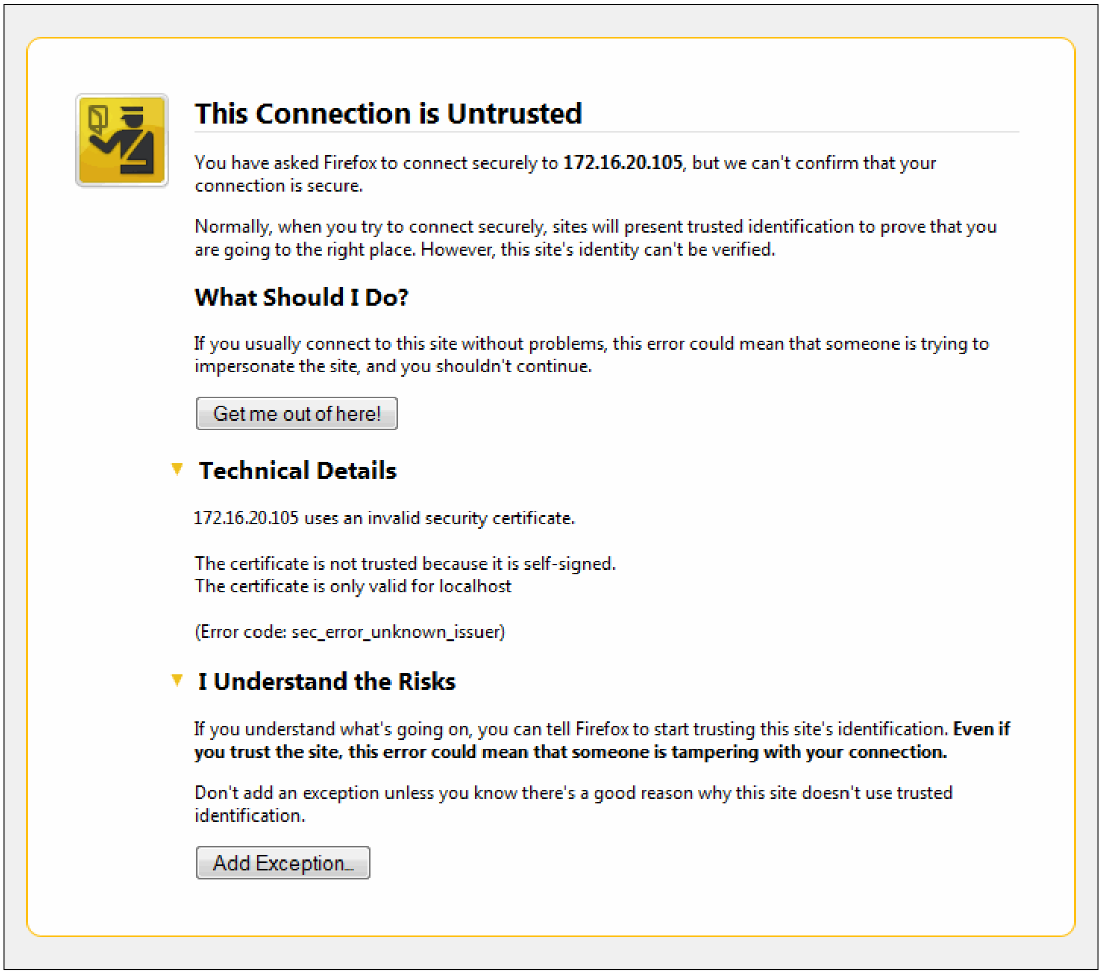
You can log in to the HMC using either the physical graphical console on a physical HMC, the VM console for a virtual HMC, or one of the remote browsers listed above. The HMC includes a web browser and shows the exact same graphical interface and login window as the one included with a remote web browser.

Complete the following steps:

1. Boot the HMC.
2. After the HMC is booted, you can direct your remote web browser to the IP address or fully qualified domain name prefixed by `https://` as in the following example:

   ```
   https://hmc8.itso.ibm.com or https://172.16.20.105
   ```

3. The first time you connect to the HMC, you are prompted for certificate acceptance (Figure 5-1). Click **Add Exception** to accept the certificate.



This Connection is Untrusted

You have asked Firefox to connect securely to **172.16.20.105**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Technical Details

172.16.20.105 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is only valid for localhost

(Error code: sec_error_unknown_issuer)

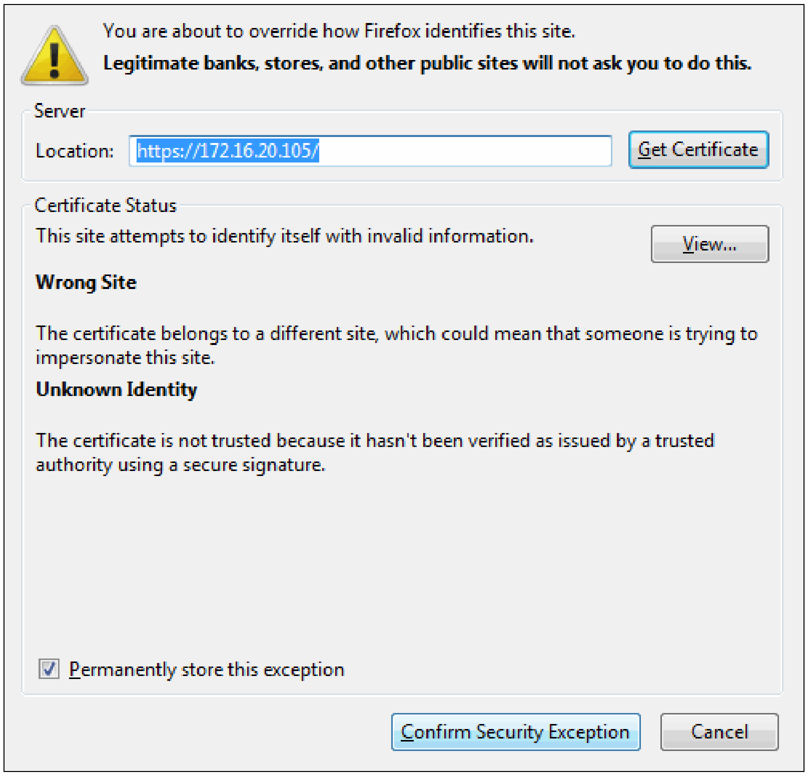
I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Figure 5-1 HMC certificate

4. You are prompted for a confirmation (Figure 5-2). Click **Confirm Security Exception** for this HMC.



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://172.16.20.105/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

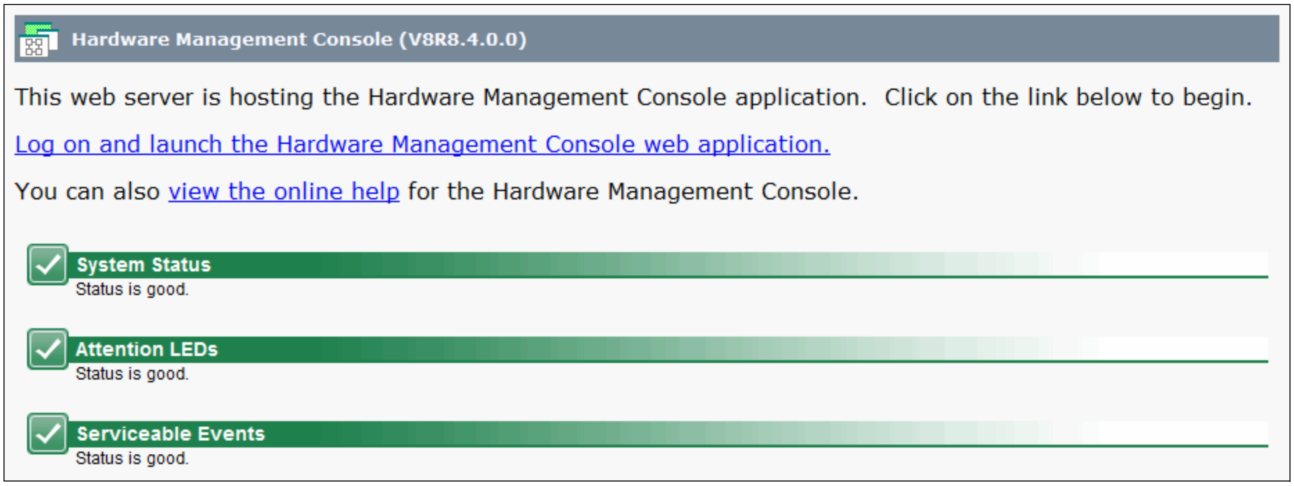
Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

Figure 5-2 Confirm security exception

5. To log in to the HMC, click **Log on and launch the Hardware Management Console web application** from the Welcome window (Figure 5-3).



Hardware Management Console (V8R8.4.0.0)

This web server is hosting the Hardware Management Console application. Click on the link below to begin.

Log on and launch the Hardware Management Console web application.

You can also view the online help for the Hardware Management Console.

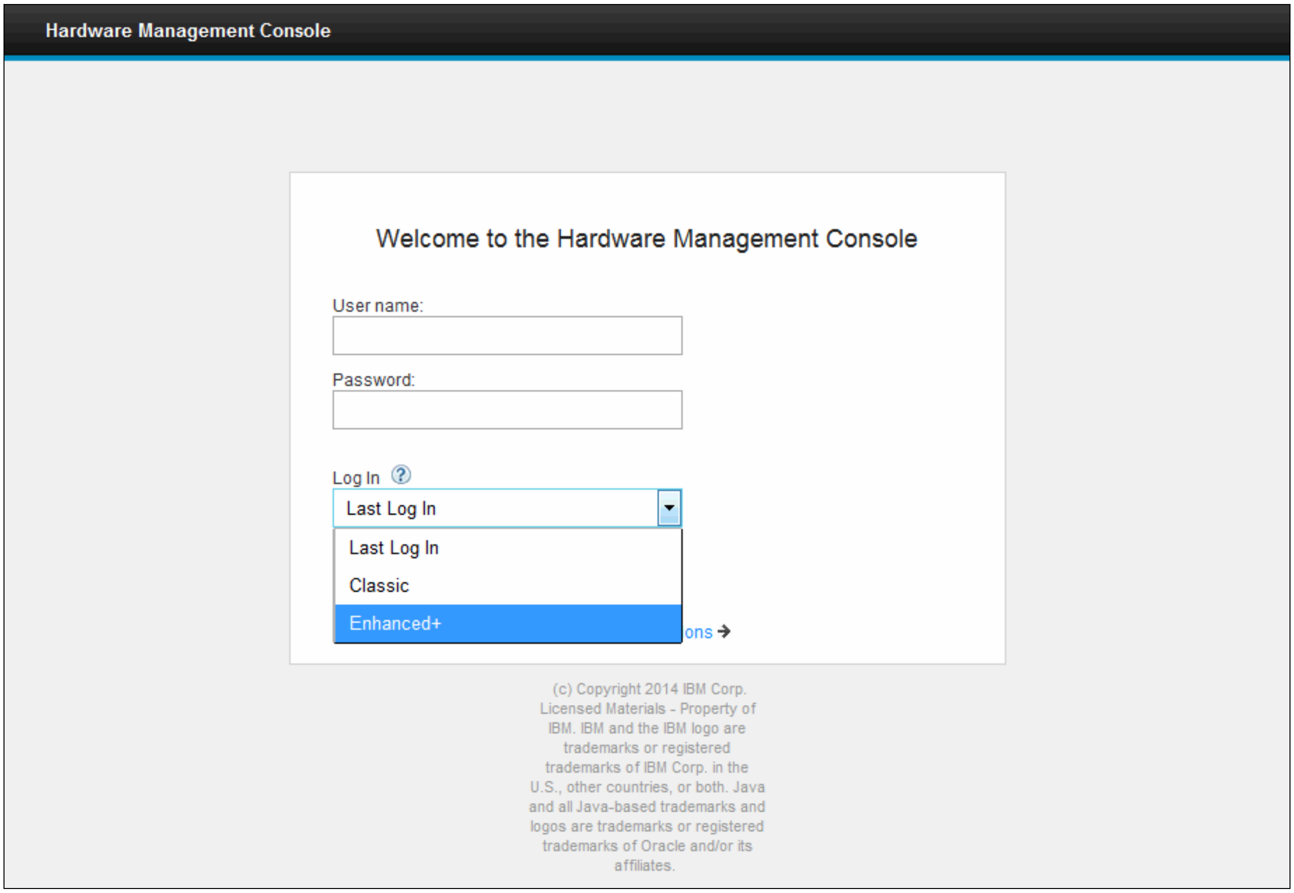
✓ System Status
Status is good.

✓ Attention LEDs
Status is good.

✓ Serviceable Events
Status is good.

Figure 5-3 Welcome console panel

6. The log in panel opens (Figure 5-4). The HMC is supplied with a predefined user ID, `hscroot`, and a default password, `abc123`, which is six characters. After you update the password for `hscroot`, you can no longer keep it at six characters. The minimum length for a changed password is seven characters.



Hardware Management Console

Welcome to the Hardware Management Console

User name:

Password:

Log In

Last Log In

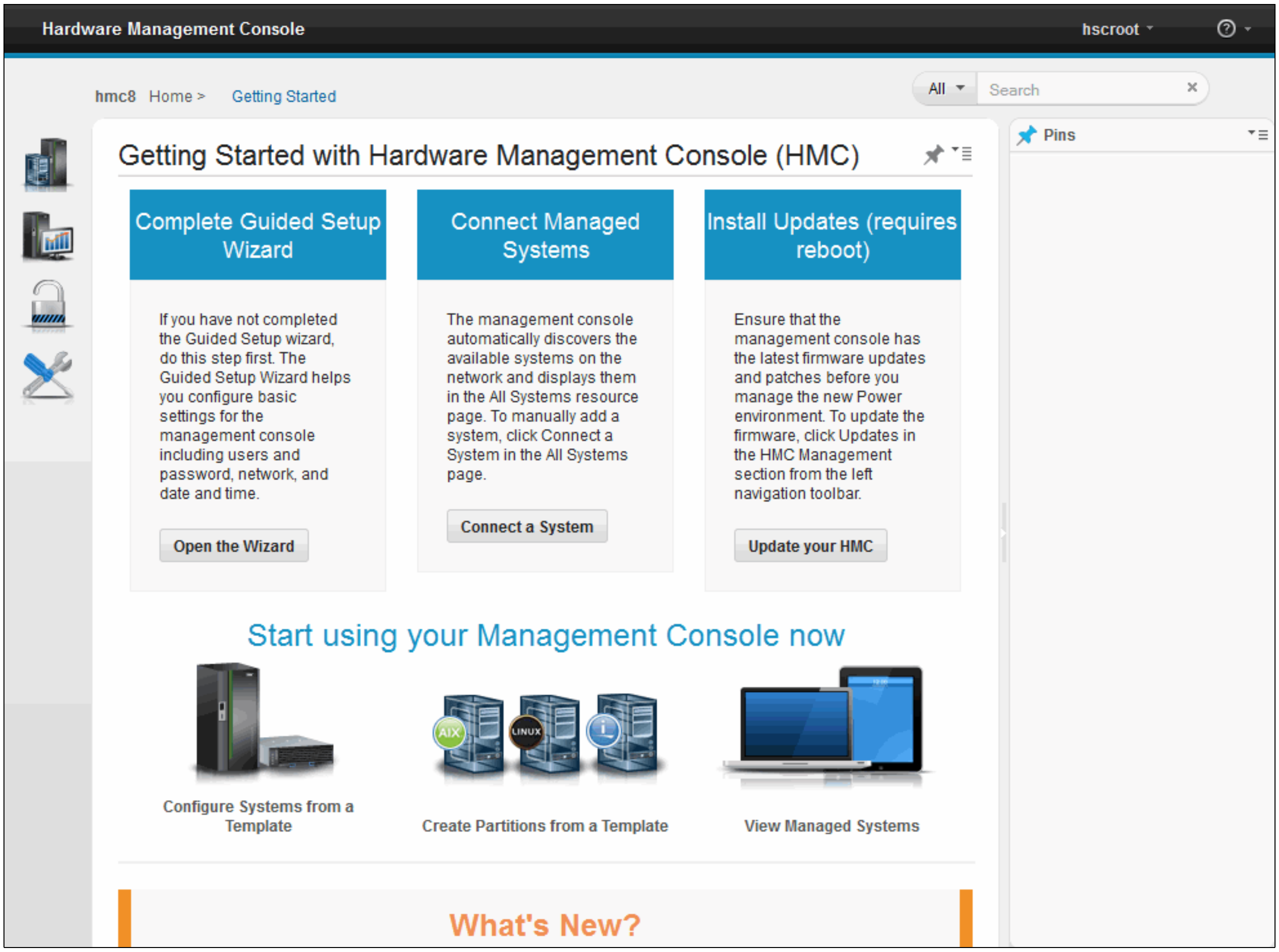
(c) Copyright 2014 IBM Corp. Licensed Materials - Property of IBM. IBM and the IBM logo are trademarks or registered trademarks of IBM Corp. in the U.S., other countries, or both. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Figure 5-4 Login panel

Since the HMC V8.R8.4.0, you can use the *Enhanced+* user interface. This is now the preferred interface to manage the HMC. Nevertheless, the *Classic* user interface is still available from the list. You are encouraged to switch to the Enhanced+ rather than the Classic user interface. For more information about the Classic HMC user interface, see *IBM Power Systems HMC Implementation and Usage Guide*, SG24-7491.

Enter the user and password, select **Enhanced+** type login and click **Login**.

7. When you first log in to the HMC V8R8.4.0, the Getting Started with HMC panel opens (Figure 5-5).


Hardware Management Console
hscroot
hmc8 Home > Getting Started
All
Search
Pins
Getting Started with Hardware Management Console (HMC)
Complete Guided Setup Wizard

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

Open the Wizard
Connect Managed Systems

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Update your HMC
Start using your Management Console now
AIX
LINUX
Configure Systems from a Template
Create Partitions from a Template
View Managed Systems
What's New?

Figure 5-5 Getting Started with HMC

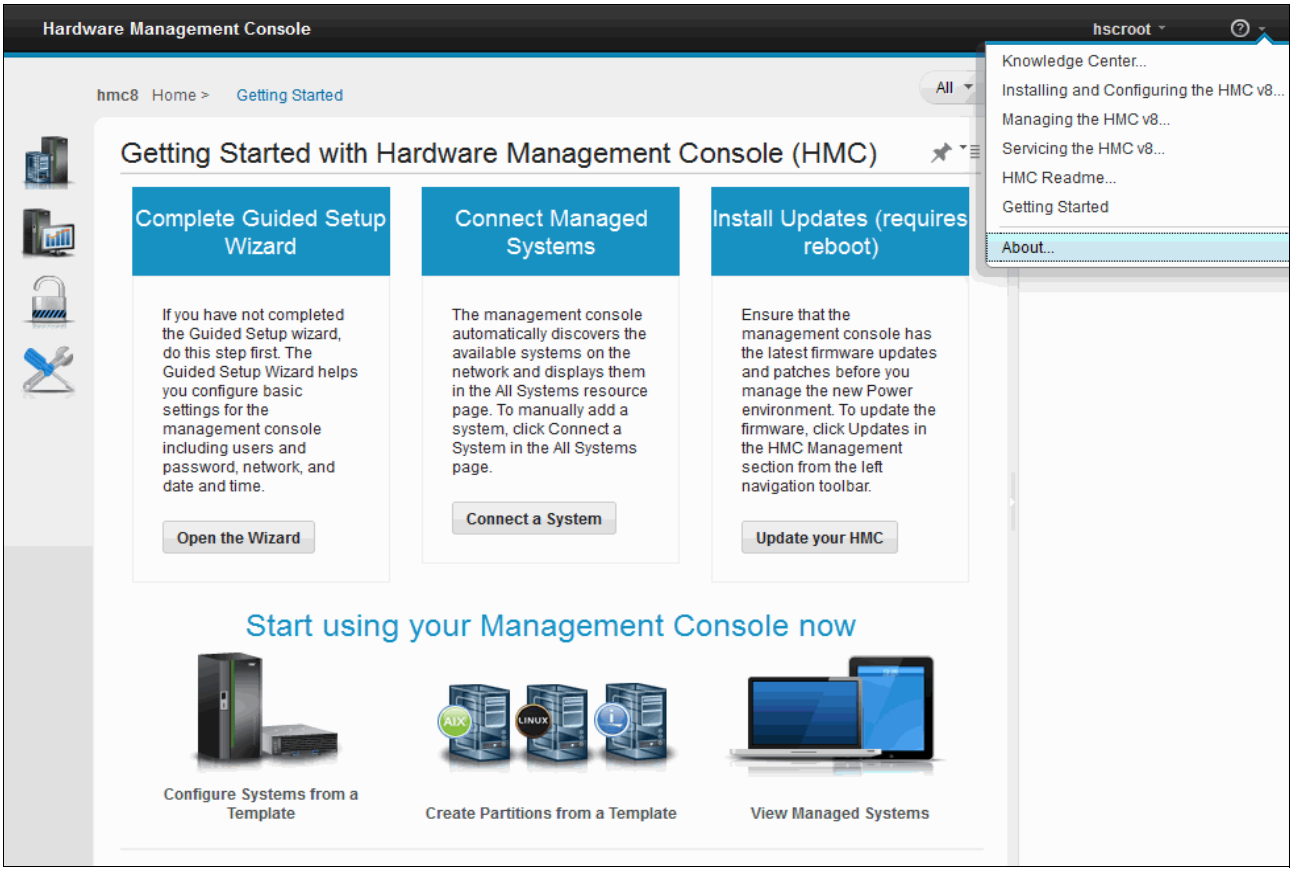
Getting Started with Hardware Management Console (HMC) window

This section describes how to start the tasks available from the new Getting Started window. More details are available in dedicated sections of this chapter.

Getting help

The Help button (Figure 5-6 on page 297) offers information about various topics, such as these, for example:

- Accessing the IBM Knowledge Center
- HMC installation and configuration
- Managing the HMC
- Servicing the HMC


Hardware Management Console
hscroot
Knowledge Center...
Installing and Configuring the HMC v8...
Managing the HMC v8...
Servicing the HMC v8...
HMC Readme...
Getting Started
About...
hmc8 Home > Getting Started
All
Complete Guided Setup Wizard
Connect Managed Systems
Install Updates (requires reboot)
Open the Wizard
Connect a System
Update your HMC
Start using your Management Console now
Configure Systems from a Template
Create Partitions from a Template
View Managed Systems

Getting Started with Hardware Management Console (HMC)

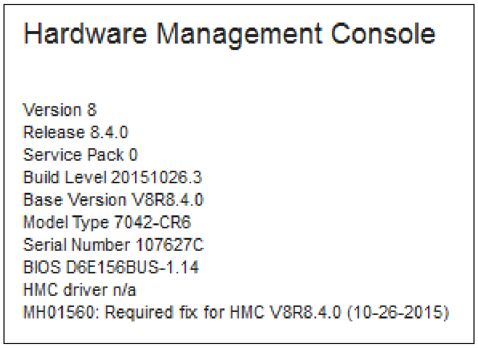
If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-6 The help button

Select **About** to find version and maintenance level information about the HMC (Figure 5-7).



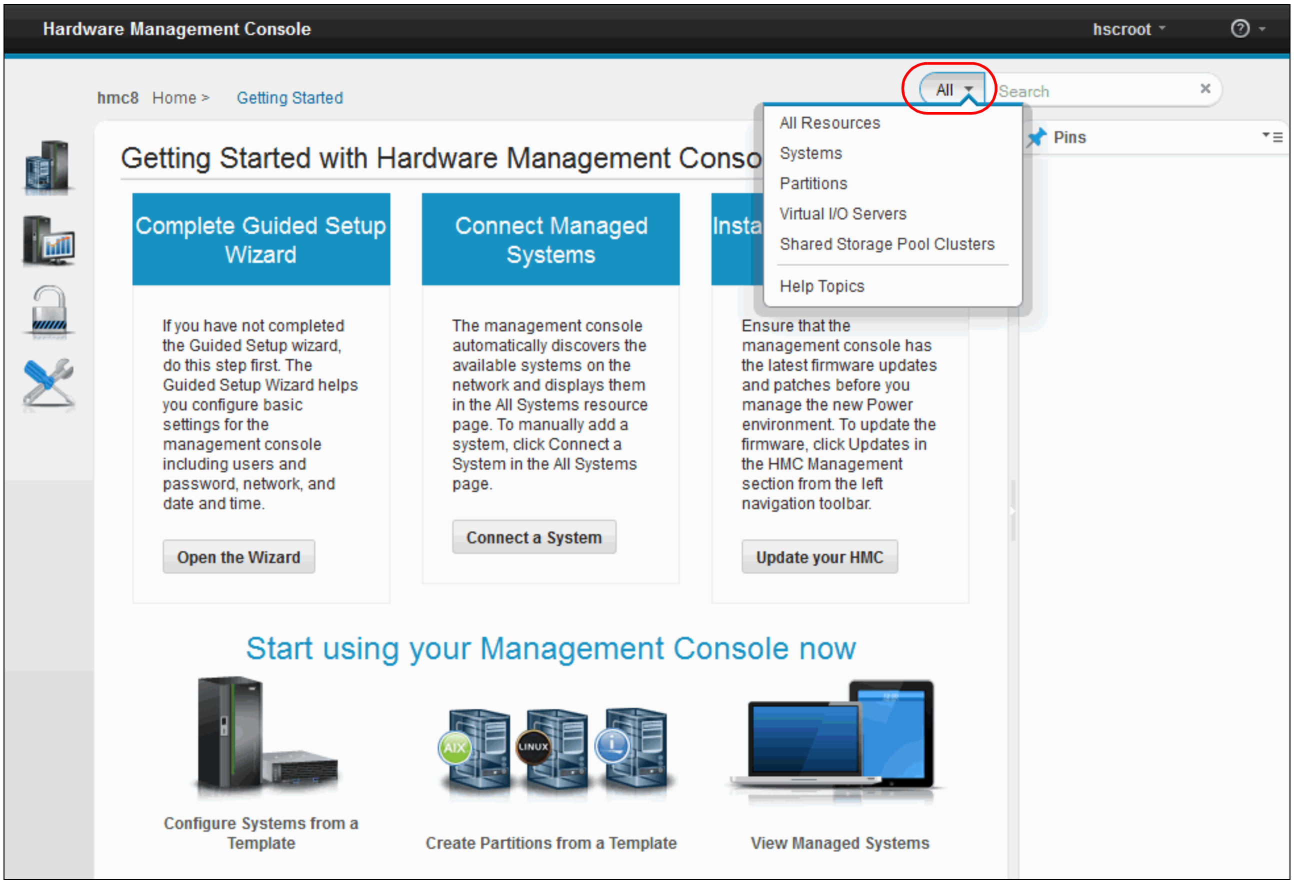
Hardware Management Console

Version 8
Release 8.4.0
Service Pack 0
Build Level 20151026.3
Base Version V8R8.4.0
Model Type 7042-CR6
Serial Number 107627C
BIOS D6E156BUS-1.14
HMC driver n/a
MH01560: Required fix for HMC V8R8.4.0 (10-26-2015)

Figure 5-7 HMC maintenance level

Search bar

The HMC has a search bar (Figure 5-8) to help you find All Resources, Systems, Partitions, Virtual I/O Servers, and Shared Storage Pool Clusters.


Hardware Management Console
hscroot
hmc8 Home > Getting Started
All
Search
All Resources
Systems
Partitions
Virtual I/O Servers
Shared Storage Pool Clusters
Help Topics
Pins
Getting Started with Hardware Management Conso
Complete Guided Setup Wizard
Connect Managed Systems
Insta
Open the Wizard
Connect a System
Update your HMC
Start using your Management Console now
AIX
LINUX
Configure Systems from a Template
Create Partitions from a Template
View Managed Systems

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-8 Search bar

Figure 5-9 shows search results for Virtual I/O Servers.

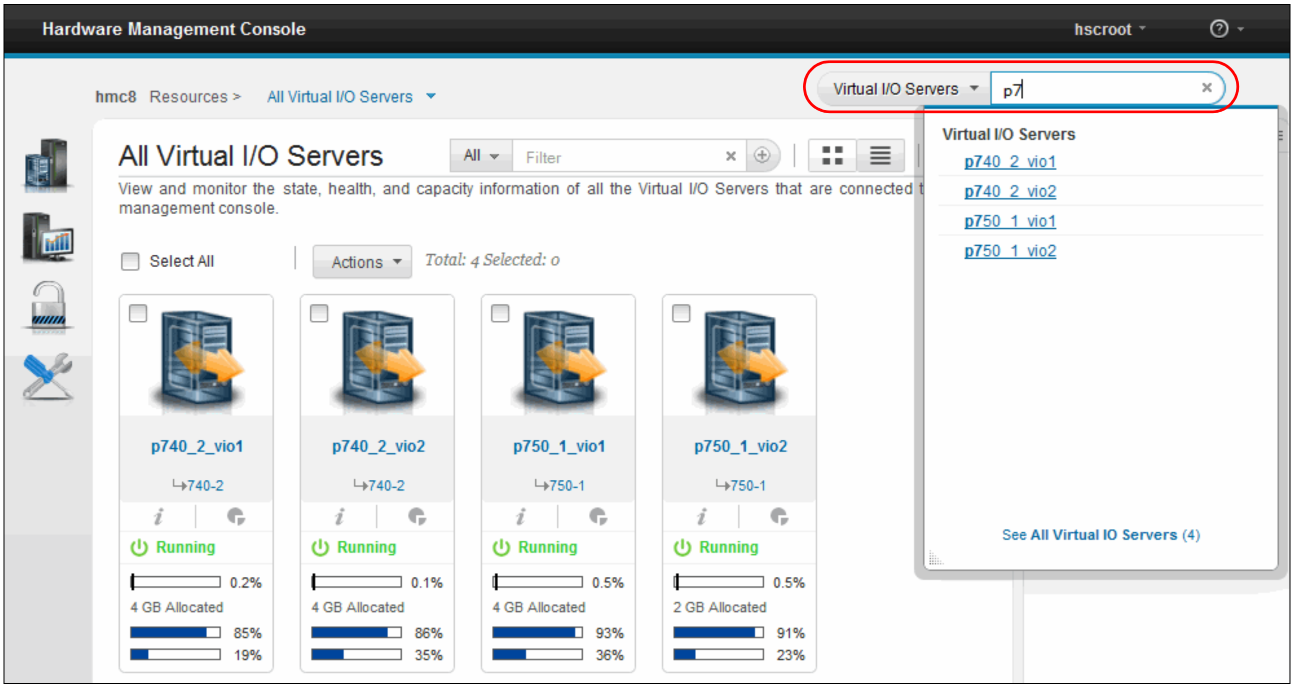
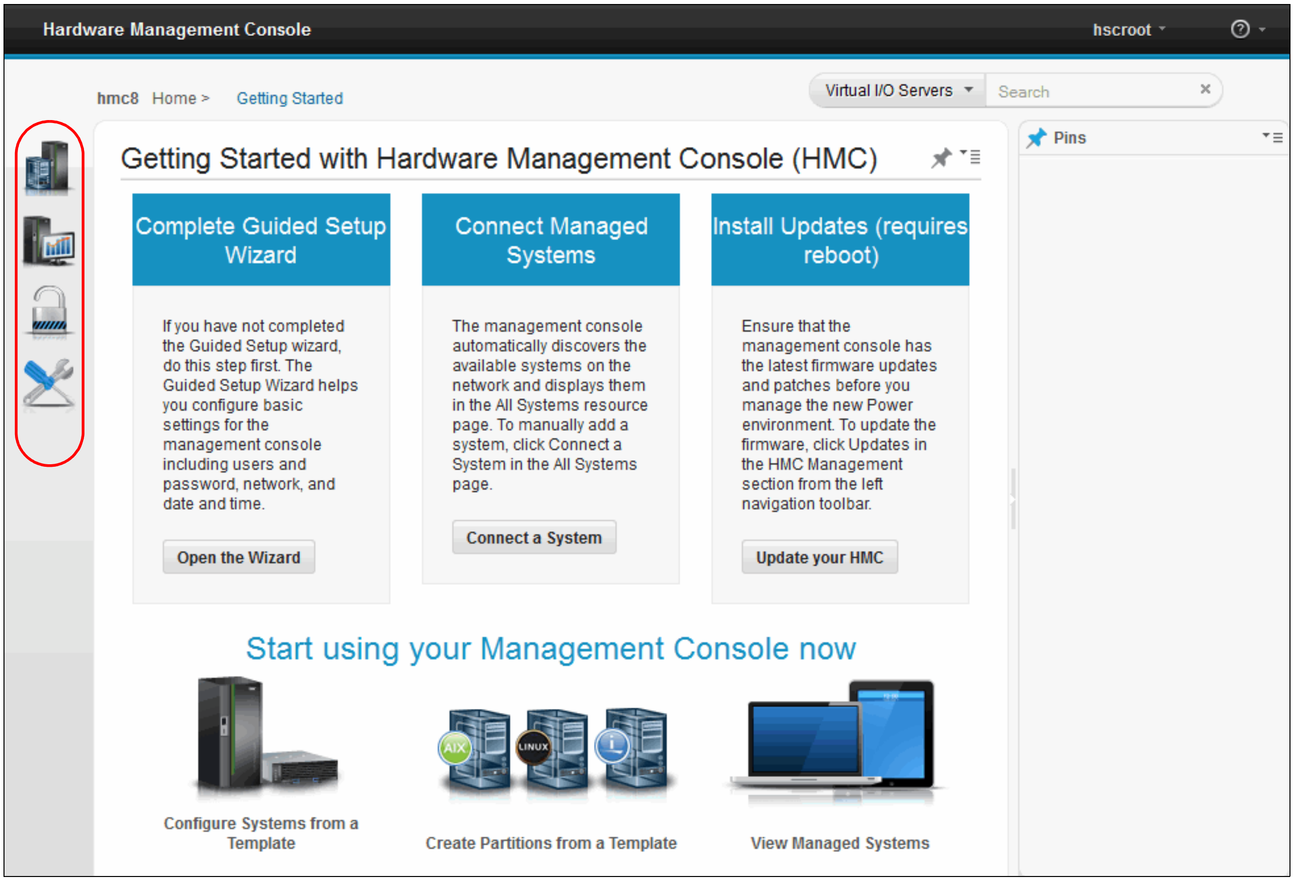


Figure 5-9 Search result

Navigation pane

Use the Navigation pane at the left side of the main HMC panel to access various resources and management tasks (Figure 5-10).



Hardware Management Console

hscroot

hmc8 Home > Getting Started

Virtual I/O Servers

Search

Pins

Getting Started with Hardware Management Console (HMC)

Complete Guided Setup Wizard

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

Open the Wizard

Connect Managed Systems

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Connect a System

Install Updates (requires reboot)

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Update your HMC

Start using your Management Console now

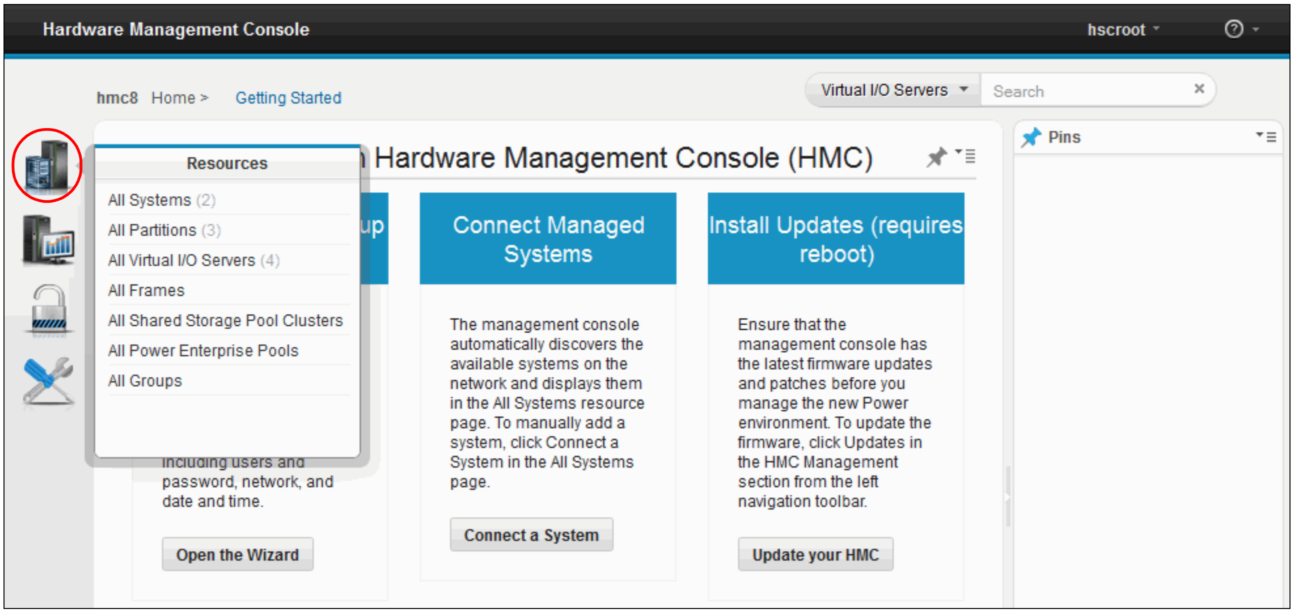
Configure Systems from a Template

Create Partitions from a Template

View Managed Systems

Figure 5-10 Navigation pane

Click the **Resources** icon to access the resources (Figure 5-11).


Hardware Management Console
hscroot
hmc8 Home > Getting Started
Virtual I/O Servers
Search
Pins
Resources
All Systems (2)
All Partitions (3)
All Virtual I/O Servers (4)
All Frames
All Shared Storage Pool Clusters
All Power Enterprise Pools
All Groups
Hardware Management Console (HMC)
up
Connect Managed Systems
Install Updates (requires reboot)
Open the Wizard
Connect a System
Update your HMC

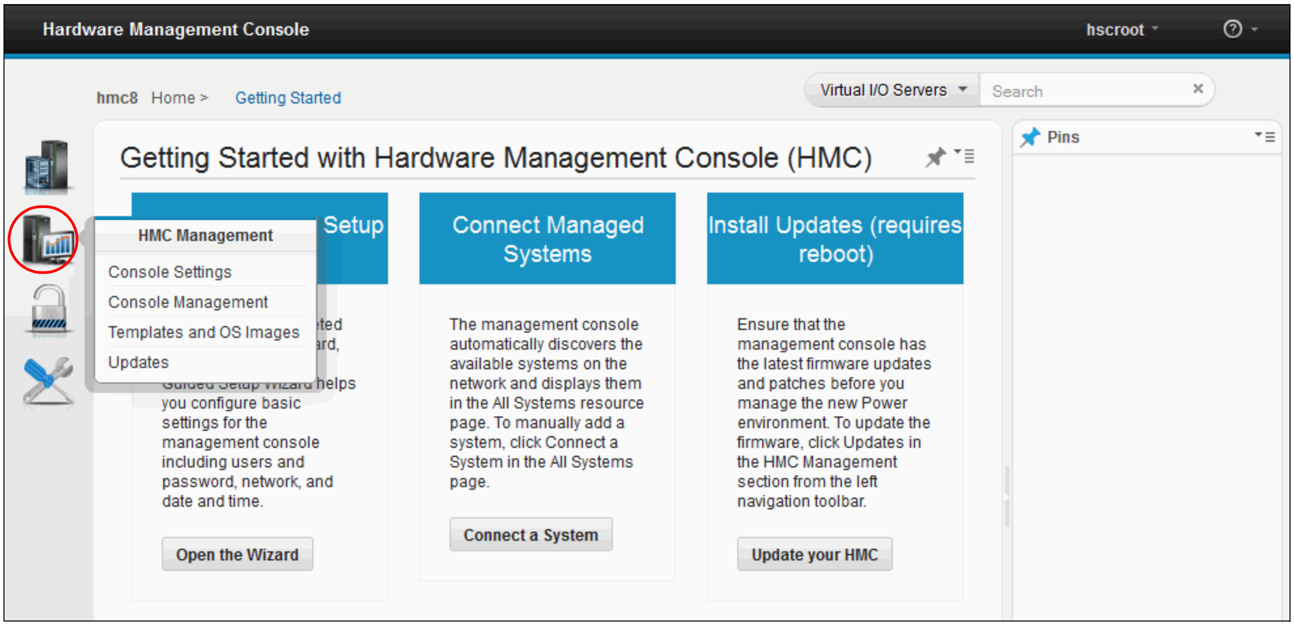
including users and password, network, and date and time.

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-11 Resources

Click the **HMC Management** icon to access the HMC management tasks (Figure 5-12).



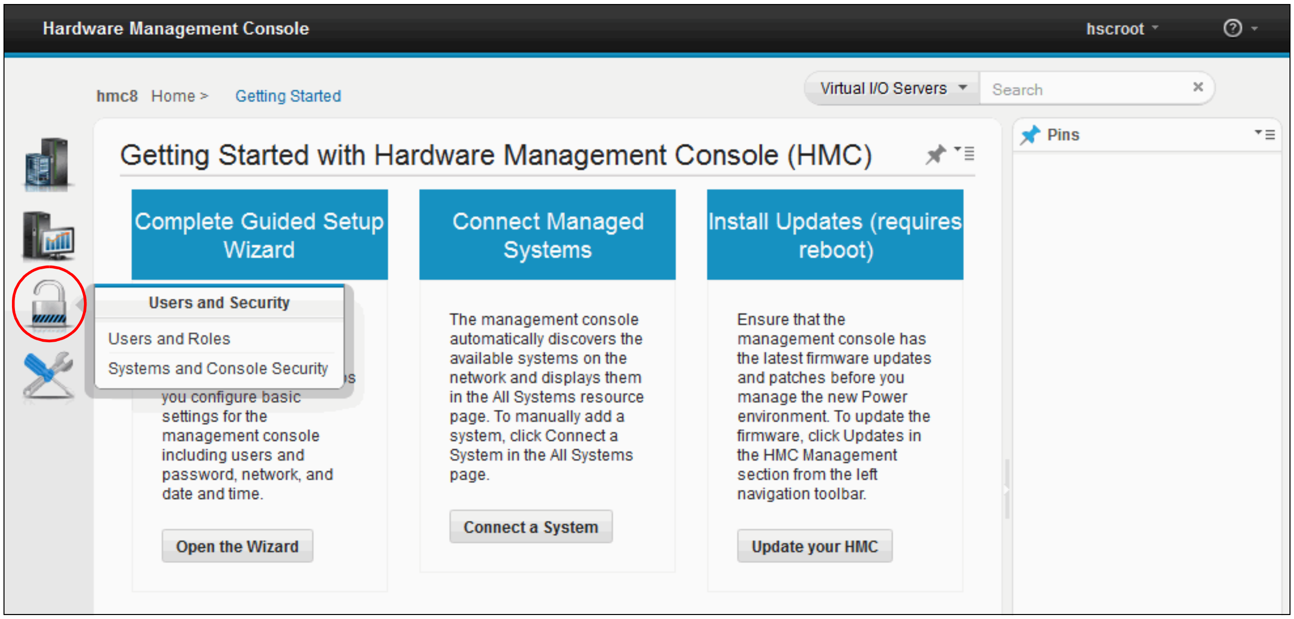
Guided Setup wizard helps you configure basic settings for the management console including users and password, network, and date and time.

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-12 HMC Management

Click the **Users and Security** icon to manage the HMC users and security settings (Figure 5-13), by clicking the **Users and Security** icon.


Hardware Management Console
hscroot
hmc8 Home > Getting Started
Virtual I/O Servers
Search
Pins
Getting Started with Hardware Management Console (HMC)
Complete Guided Setup Wizard
Connect Managed Systems
Install Updates (requires reboot)
Users and Security
Users and Roles
Systems and Console Security
Open the Wizard
Connect a System
Update your HMC

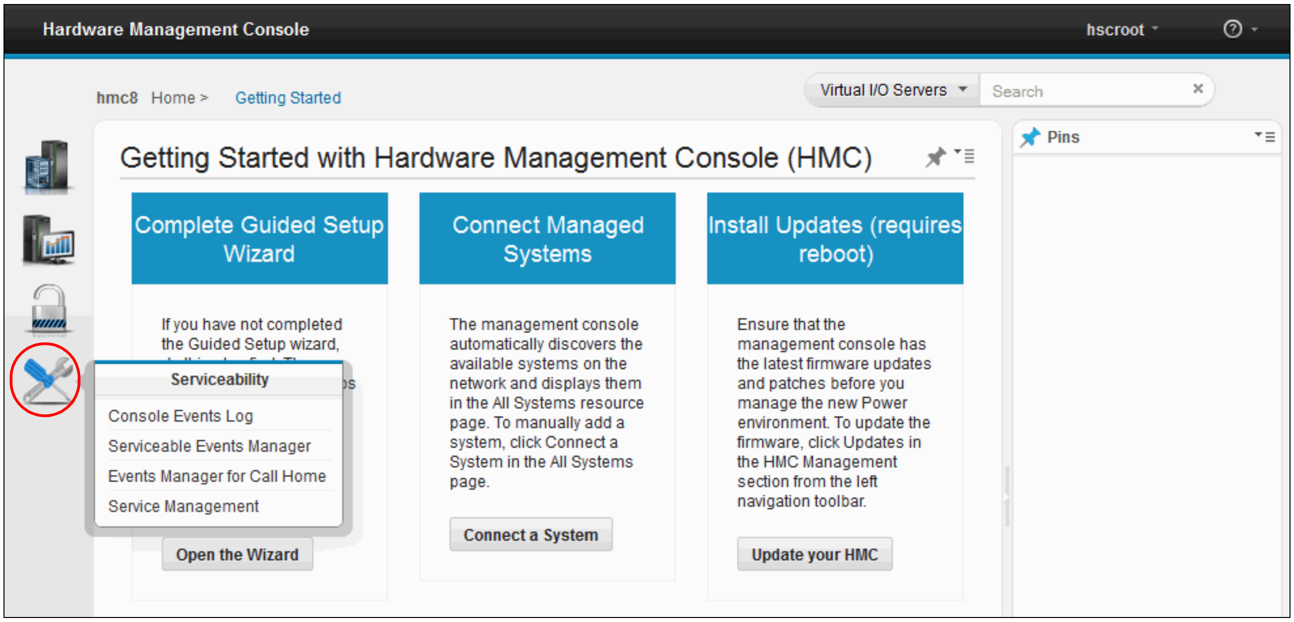
...s you configure basic settings for the management console including users and password, network, and date and time.

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-13 HMC Users and Security

Click the **Serviceability** icon to manage HMC events and service (Figure 5-14).


Hardware Management Console
hscroot
hmc8 Home > Getting Started
Virtual I/O Servers
Search
Pins
Getting Started with Hardware Management Console (HMC)
Complete Guided Setup Wizard
Connect Managed Systems
Install Updates (requires reboot)
Serviceability
Console Events Log
Serviceable Events Manager
Events Manager for Call Home
Service Management
Open the Wizard
Connect a System
Update your HMC

If you have not completed the Guided Setup wizard, ...ps

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

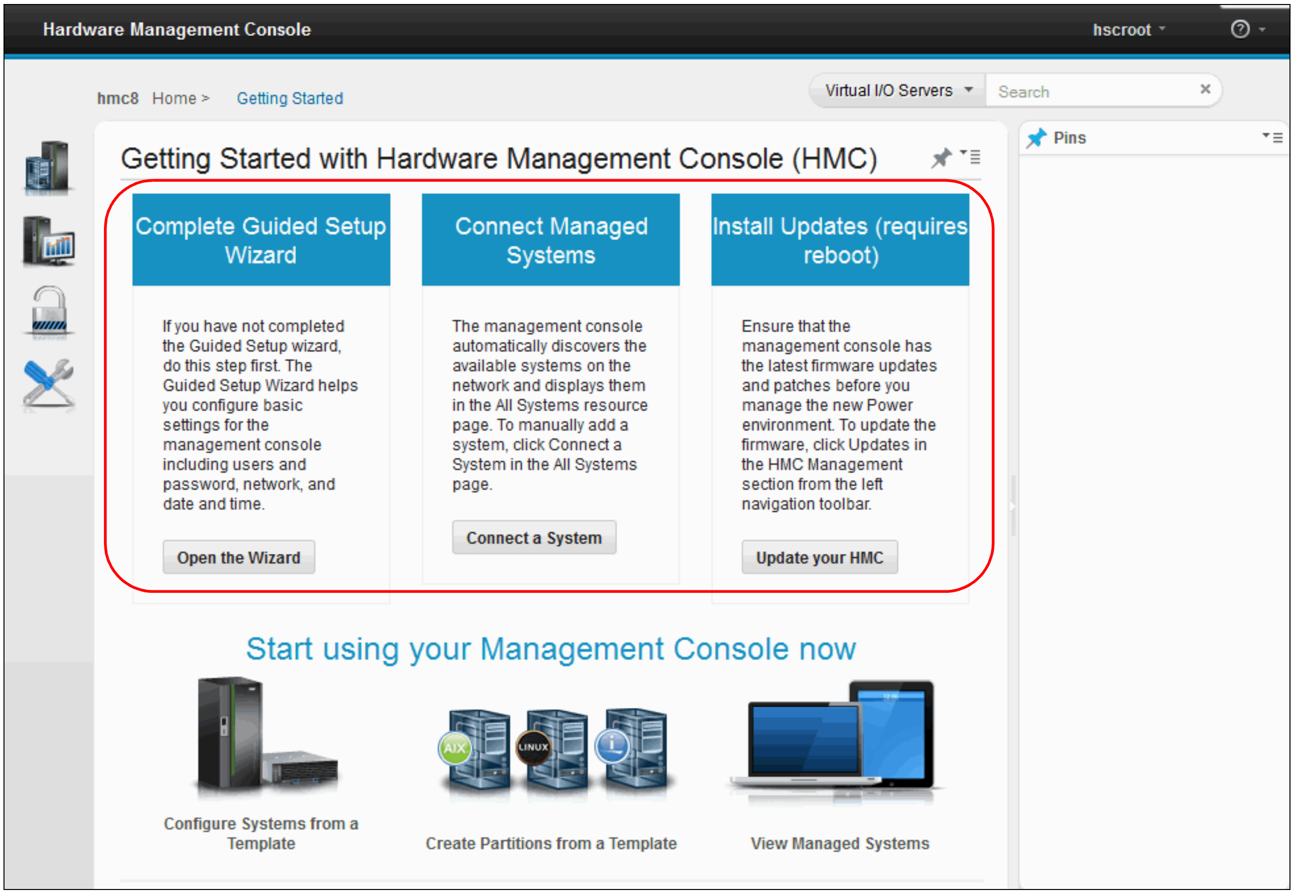
Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-14 Serviceability

Center pane

The center pane (highlighted in Figure 5-15) provides access to other setup, configuration, and management tasks:

- Complete Guided Setup Wizard
- Connect Managed Systems
- Install Updates



Getting Started with Hardware Management Console (HMC)

Complete Guided Setup Wizard

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

Open the Wizard

Connect Managed Systems

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Connect a System

Install Updates (requires reboot)

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Update your HMC

Start using your Management Console now

Configure Systems from a Template

Create Partitions from a Template

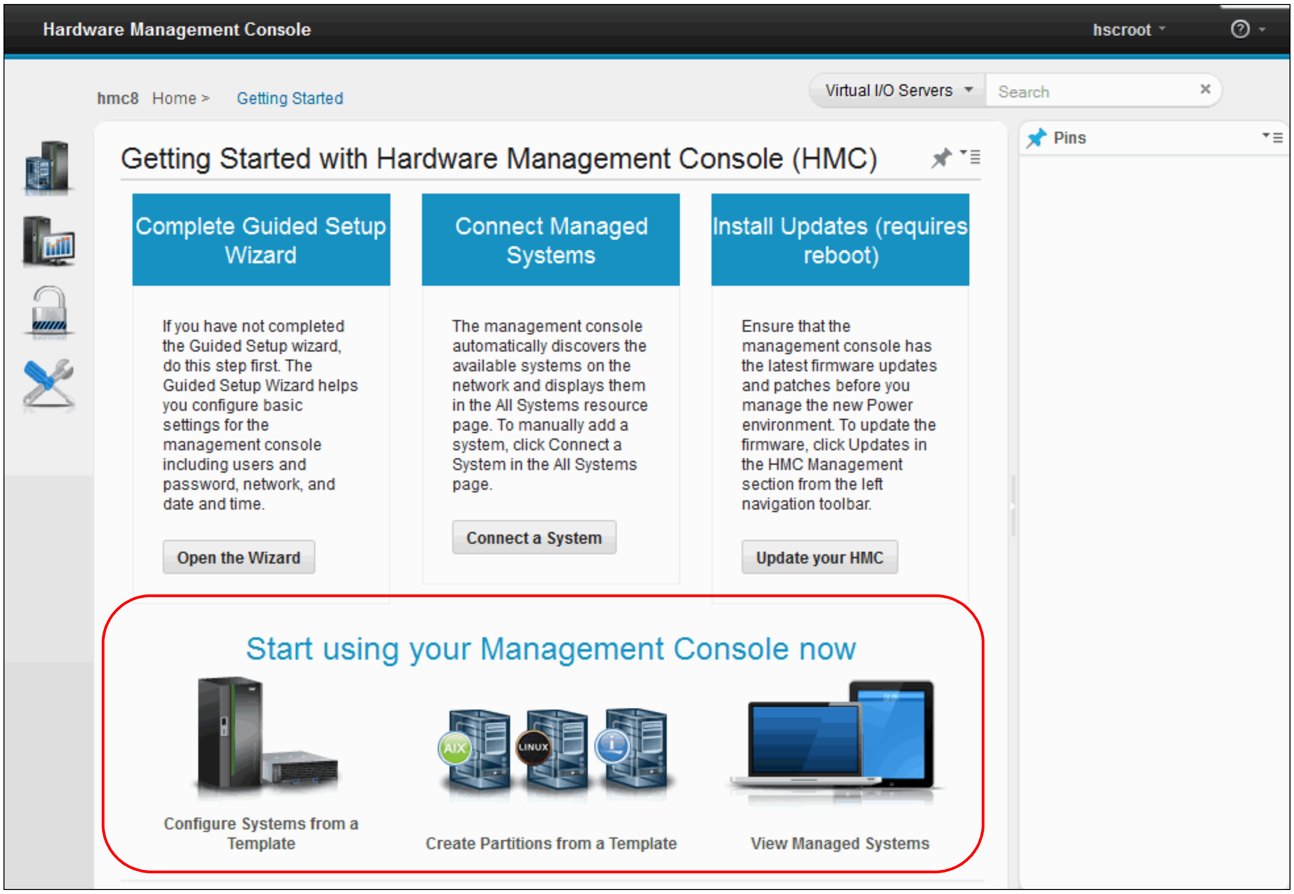
View Managed Systems

Figure 5-15 Center pane

Lower pane: Start using your Management Console now

The lower pane (highlighted in Figure 5-16) provides these tasks:

- Configure systems from templates
- Create partitions from a template
- View and operate managed systems



Hardware Management Console
hscroot
hmc8 Home > Getting Started
Virtual I/O Servers
Search
Pins
Getting Started with Hardware Management Console (HMC)
Complete Guided Setup Wizard

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

Open the Wizard
Connect Managed Systems

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

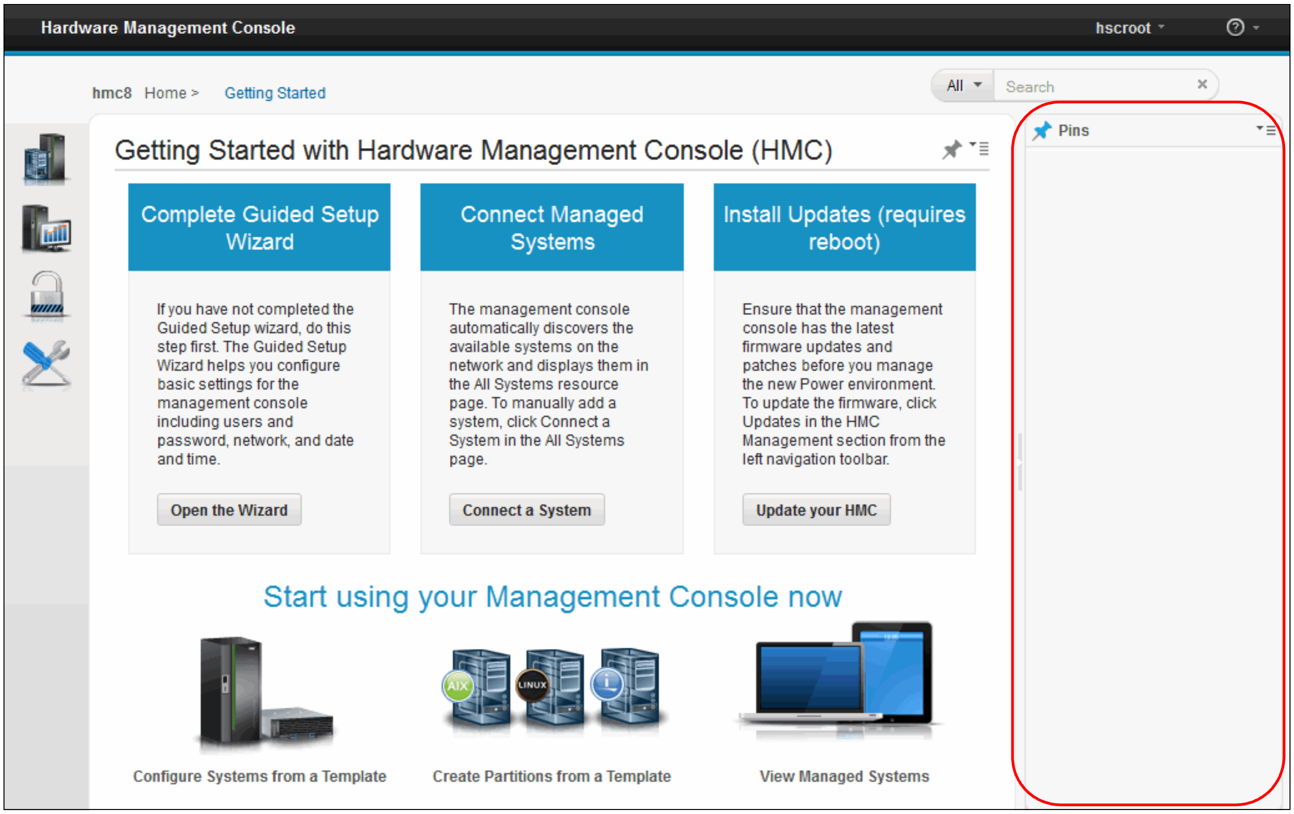
Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Update your HMC
Start using your Management Console now
AIX
LINUX
Configure Systems from a Template
Create Partitions from a Template
View Managed Systems

Figure 5-16 Lower pane

The Pins pane

Use the Pins pane (highlighted in Figure 5-17) to keep tasks or resources that you need on a regular basis easily accessible in a quick manner.


Hardware Management Console
hscroot
hmc8 Home > Getting Started
All
Search
Pins
Getting Started with Hardware Management Console (HMC)
Complete Guided Setup Wizard
Connect Managed Systems
Install Updates (requires reboot)
Open the Wizard
Connect a System
Update your HMC
Start using your Management Console now
AIX
LINUX
Configure Systems from a Template
Create Partitions from a Template
View Managed Systems

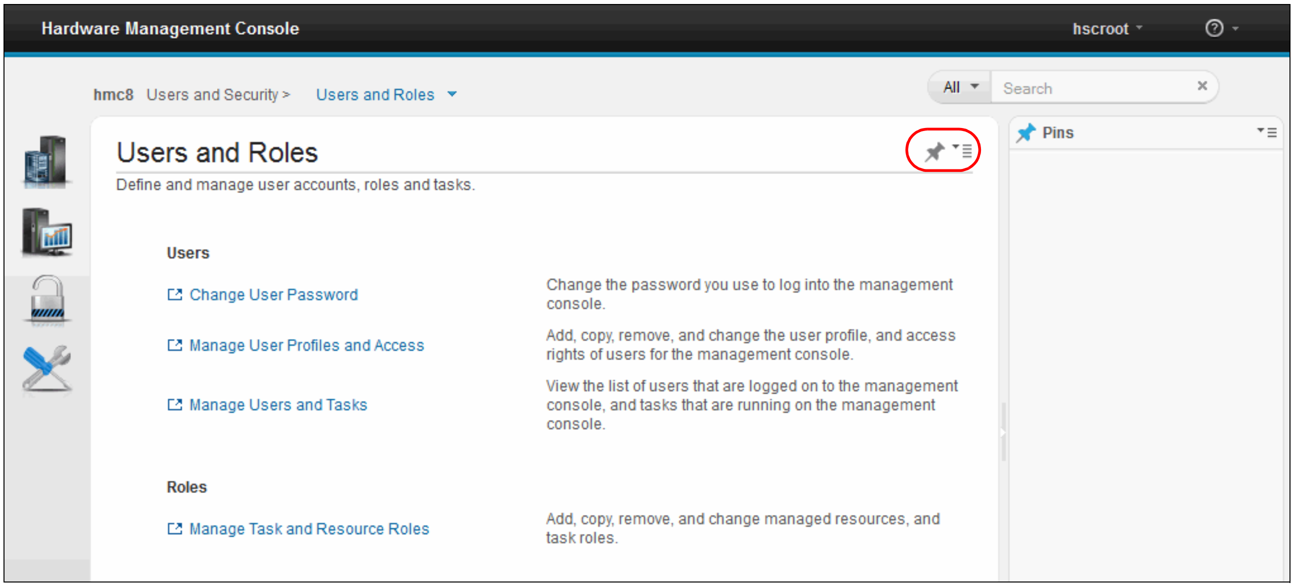
If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-17 The Pins pane

To add a resource to the Pins pane, select a task. In this example, the Users and Roles tasks is selected (Figure 5-18). Then, click the **Pin** button.


Hardware Management Console
hscroot
hmc8 Users and Security > Users and Roles
All
Search
Pins
Users and Roles
Users
Change User Password
Manage User Profiles and Access
Manage Users and Tasks
Roles
Manage Task and Resource Roles

Define and manage user accounts, roles and tasks.

Change the password you use to log into the management console.

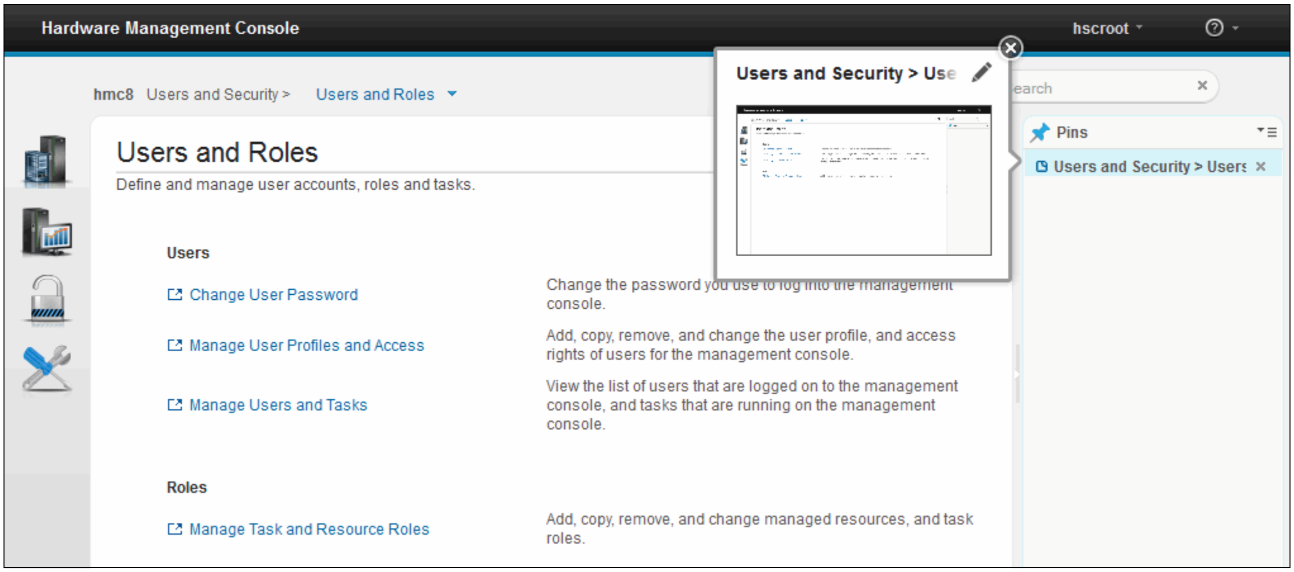
Add, copy, remove, and change the user profile, and access rights of users for the management console.

View the list of users that are logged on to the management console, and tasks that are running on the management console.

Add, copy, remove, and change managed resources, and task roles.

Figure 5-18 Pin a page

The task is now added to the Pins pane (Figure 5-19).


Hardware Management Console hscroot

hmc8 Users and Security > Users and Roles

Users and Security > Use

Search

Pins

Users and Security > Users ×

Users and Roles

Define and manage user accounts, roles and tasks.

Users

Change User Password — Change the password you use to log into the management console.

Manage User Profiles and Access — Add, copy, remove, and change the user profile, and access rights of users for the management console.

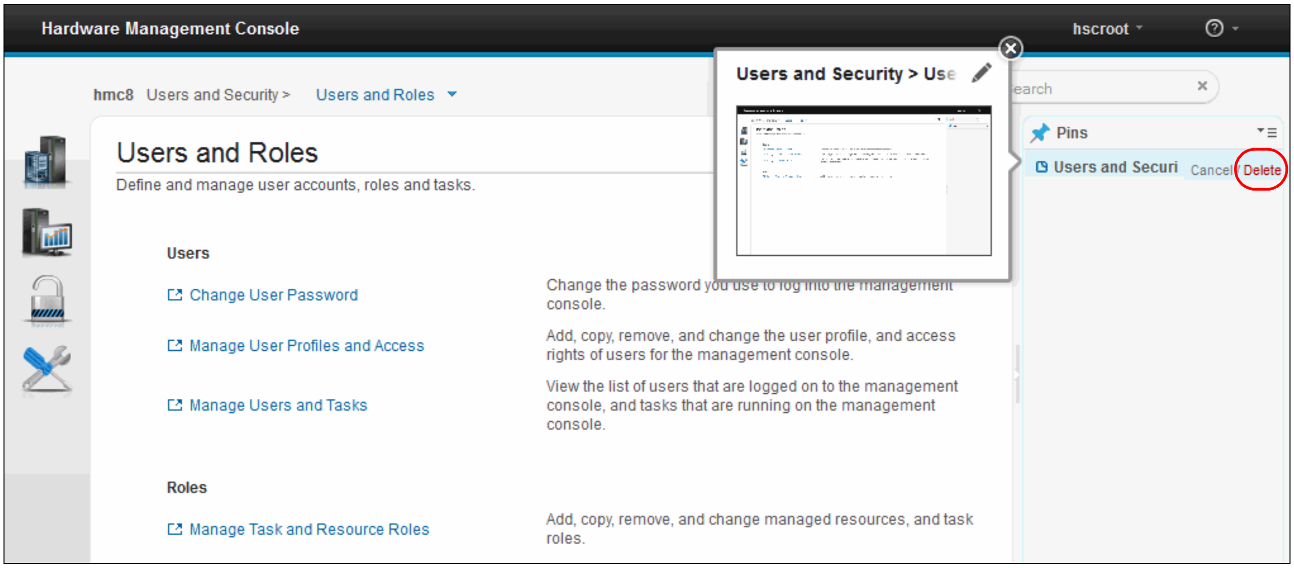
Manage Users and Tasks — View the list of users that are logged on to the management console, and tasks that are running on the management console.

Roles

Manage Task and Resource Roles — Add, copy, remove, and change managed resources, and task roles.

Figure 5-19 Pinned task

To delete this pinned task, move the cursor to the pinned task, and click delete (Figure 5-20).


Hardware Management Console hscroot

hmc8 Users and Security > Users and Roles

Users and Security > Use

Search

Pins

Users and Securi Cancel Delete

Users and Roles

Define and manage user accounts, roles and tasks.

Users

Change User Password — Change the password you use to log into the management console.

Manage User Profiles and Access — Add, copy, remove, and change the user profile, and access rights of users for the management console.

Manage Users and Tasks — View the list of users that are logged on to the management console, and tasks that are running on the management console.

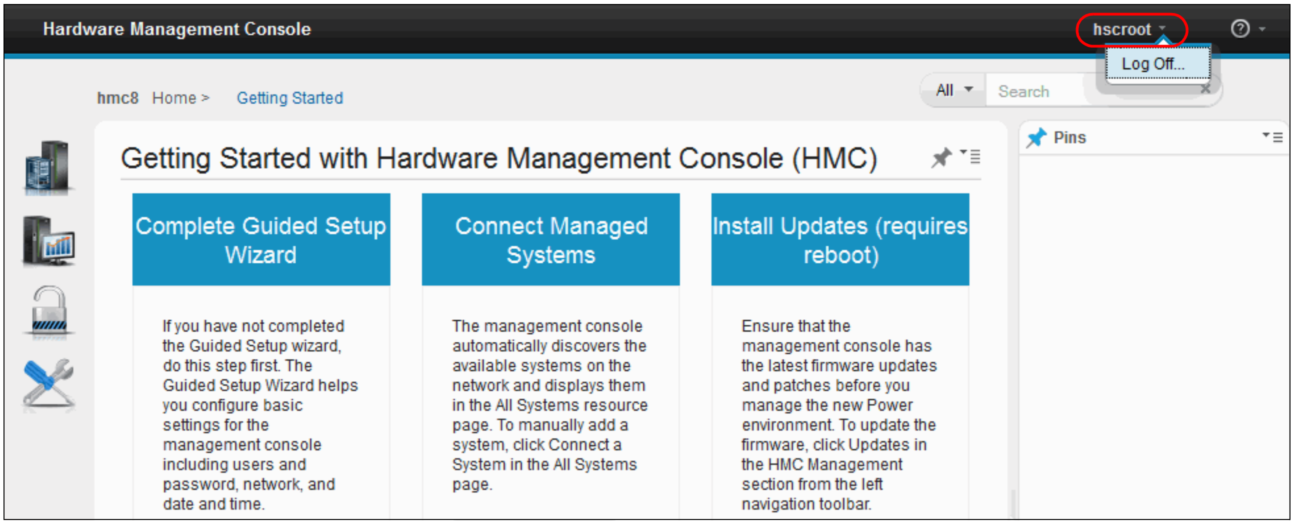
Roles

Manage Task and Resource Roles — Add, copy, remove, and change managed resources, and task roles.

Figure 5-20 Delete a pinned task

Log off from the HMC

To log off the HMC, click the user ID that you logged in with and then select **Log Off** (Figure 5-21).



Getting Started with Hardware Management Console (HMC)

Complete Guided Setup Wizard

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

Connect Managed Systems

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Install Updates (requires reboot)

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-21 Log off from HMC

5.1.2 Command-line interface (CLI)

The CLI is an alternative to the HMC graphical user interface (GUI). This section provides information about the most common command-line options and usage. You can use the CLI for the following situations:

- Consistent results are required.

  If you administer several managed systems, you can achieve consistent results by using the CLI. The command sequence can be stored in scripts and run remotely.

- Automated operations are required.

  After you develop a consistent way to administer the managed systems, you can automate the operations by starting the scripts from batch-processing applications, such as the cron daemon, from other systems.

Before using remote CLI, you must enable the access to the HMC by using the SSH facility. See 4.3.4, “Enable Remote Command Execution option” on page 287.

You can generally choose from two options to use CLI on the HMC:

- Restricted Shell Terminal task on the local HMC
- Secure Shell (SSH) client

If you use an SSH client to run scripts against the HMC, ensure that your script executions between SSH clients and the HMC are secure.

See the following sources for more information:

- General information to set up the SSH client in the IBM Knowledge Center:

  http://www.ibm.com/support/knowledgecenter/8247-22L/p8eh6/p8eh6_securescript.htm?cp=8247-22L&lang=en

- HMC commands in the IBM Knowledge Center:

  https://www.ibm.com/support/knowledgecenter/POWER8/p8edm/p8edm_kickoff.htm

- A PDF document with all the commands is available:

  http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/resources.html

- Examples of CLI commands are in Appendix B, “CLI commands examples” on page 569.

5.1.3 REST API

The HMC provides the following services to systems administrators with the Representational State Transfer (REST) application program interfaces (API):

- Power Systems server virtualization
- Performance Capacity and Monitoring
- Power Enterprise Pools (CoD)

REST defines a set of architectural principles by which you can design web services that focus on a system's resources, including how resource states are addressed and transferred over HTTP by a wide range of clients written in different languages. If measured by the number of web services that use it, REST has emerged in the last several years as a predominant web service design model. In fact, REST has had such a large impact on the web that it has mostly displaced SOAP-based and WSDL-based interface design because it is a considerably simpler style to use.

Further details are available at the following web pages:

- https://www.ibm.com/developerworks/library/ws-restful/
- https://www.ibm.com/support/knowledgecenter/POWER8/p8ehl/concepts/ApiOverview.htm

5.2 Management of the HMC

This section describes the available HMC management tasks in a categorized view. These tasks are used for setting up the HMC, maintaining its internal code, and securing the HMC.

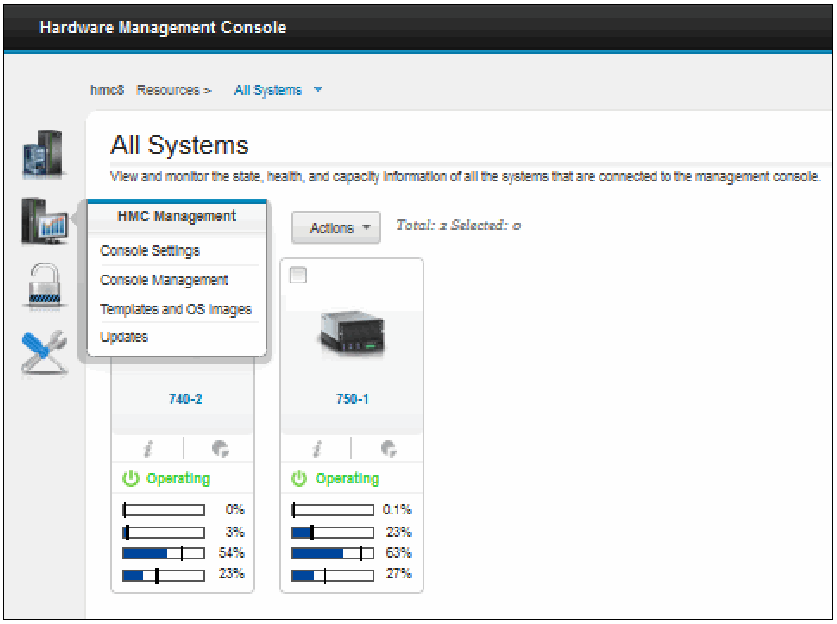
In deference to the classic GUI, management tasks in the Enhanced+ GUI are at different locations. In the main window, two icons are in the left pane:

- HMC Management
- Users and Security

When you select one of the icons, a menu opens and lists further choices.

Click the **HMC Management** icon to see the following menu choices (Figure 5-22 on page 309):

- Console Settings
- Console Management
- Templates and OS Management
- Updates

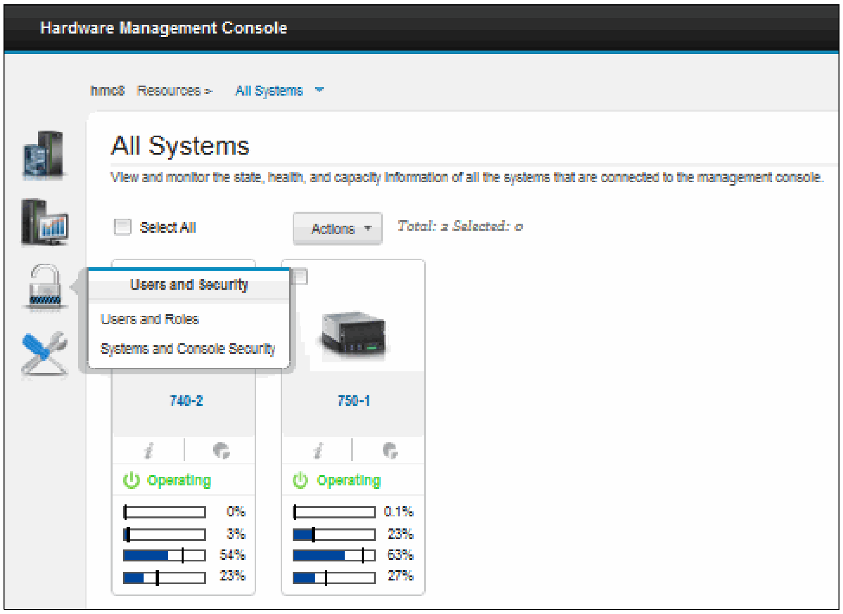


View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

Figure 5-22 HMC Management icon menu

Click the **Users and Security** icon to see the following menu choices (Figure 5-23):

- Users and Roles
- Systems and Console Security



View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

Figure 5-23 Users and Security icon menu

Each menu option has further choices. These are discussed more in the following sections.

5.2.1 Console Settings

Click **HMC Management** → **Console Settings** to see the following management tasks:

- Launch Guided Wizard

  Use this management task to set up the HMC. To set up your HMC successfully, complete all the tasks in the order that the wizard presents them. The task is further explained in 3.3, “HMC Install Wizard” on page 223.

- View Network Topology

  Use this management task to show a tree view of the network nodes that are known to this HMC. Examples of such nodes are managed systems, logical partitions, storage, and other HMCs. The task is further explained in 4.1.4, “View network topology” on page 270.

- Test Network Connectivity

  Use this management task to view and ping the connectivity between various network nodes. You can also view network diagnostic information for the TCP/IP connection. The task is further explained in 4.1.3, “Test network connectivity” on page 268.

- Change Network Settings

  Use this management task to view current network information for the HMC and change the network settings. The task is further explained in 4.1.2, “Configuring the HMC network settings” on page 260.

- Change Performance Monitoring Settings

  Use this management task to view and modify settings for the Performance and Capacity Monitor (PCM) of the HMC. The task is explained in 7.2, “Enabling Performance and Capacity Monitor data collection” on page 512.

- Change Date and Time

  Use this management task to set the date and time of the management console, and view the current time servers in use, if the Network Time Protocol (NTP) service is enabled. The task is further explained in 4.4.3, “Change Date and Time selection” on page 289.

- Change Language and Locale

  Use this management task to change the language and locale in use for the management console. The task is further explained in 4.4.4, “Change Language and Locale selection” on page 290.

5.2.2 Console Management

Click **HMC Management** → **Console Management** to see the following management tasks:

- Shut Down or Restart the Management Console

  Use this management task to shut down or restart the management console. The task is further explained in 5.3.1, “Shut Down or Restart the Management Console” on page 317.

- Schedule Operations

  Use this management task to schedule operations of the management console. The task is further explained in 5.3.2, “Schedule Operations” on page 317.

- View Licenses

  Use this management task to review third party and other licenses agreements for the HMC. The task is further explained in 5.3.3, “View Licenses” on page 319.

- Update the Hardware Management console

  Use this management task to update the internal code of the management console, view system information and readiness. You can also view the Software Code Level of the HMC. The task is further explained in 5.3.4, “Update the Hardware Management Console” on page 320.

- Format Media

  Use this management task to format a media, like a DVD-RAM or USB flash memory device. The task is further explained in 5.3.5, “Format Media” on page 321.

- Backup Management Console Data

  Use this management task to back up (or archive) the data that is stored on your HMC hard disk that is critical to support HMC operations. You can backup the data to a local system, a remote system, or a remote site. The task is further explained in 5.3.6, “Backup Management Console Data” on page 321.

- Restore Management Console Data

  Use this management task to restore backed up data for this HMC. You can restore data from a Network File System (NFS), a File Transfer Protocol (FTP) server, an SSH file Transfer Protocol (SFTP) server, or removable media. The task is further explained in 5.3.7, “Restore Management Console Data” on page 322.

- Save Upgrade Data

  Use this management task to save all of the customizable data for the HMC to the hard disk drive or to a DVD-RAM before performing a HMC software upgrade. The task is further explained in 5.3.8, “Save Upgrade Data” on page 323.

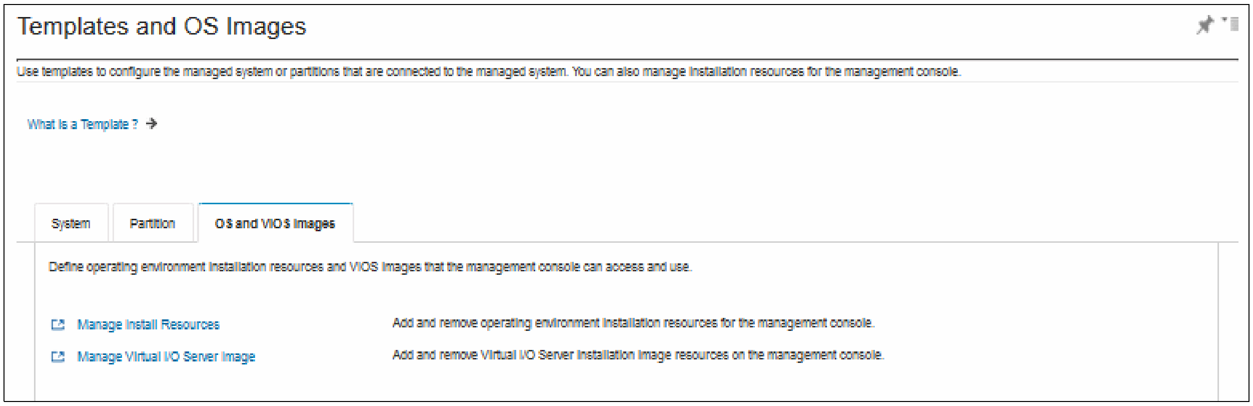
- Manage Data Replication

  Use this management task to enable customized data replication. Customized data replication allows another HMC to obtain customized data from or send data to a HMC. With this you can synchronize certain sets of configured data between HMCs without manual intervention. The task is further explained in 5.3.9, “Manage Data Replication” on page 324.

5.2.3 Templates and OS Management

This section describes the Templates and OS Management menu. You can manage templates to configure a managed system or partitions that are connected to the managed system. This task is further explained in 2.5, “System and partition templates” on page 67. You can also manage installation resources for the management console.

Click **HMC Management** → **Templates and OS Images** to manage installation resources. The Templates and OS Images view opens to the OS and VIOS images tab (Figure 5-24).



Templates and OS Images

Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

What is a Template ? →

Define operating environment installation resources and VIOS images that the management console can access and use.

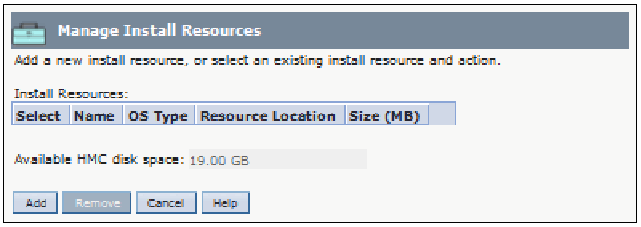
Manage Install Resources	Add and remove operating environment installation resources for the management console.
Manage Virtual I/O Server Image	Add and remove Virtual I/O Server installation image resources on the management console.

Figure 5-24 OS and VIOS Images view

From this tab, you can add and remove operating environment and Virtual I/O Server (VIOS) installation resources.

Manage Install Resources task

When you select this task, the Manage Install Resources window opens (Figure 5-25), where you can add or remove install resources.



Manage Install Resources

Add a new install resource, or select an existing install resource and action.

Install Resources:

Select	Name	OS Type	Resource Location	Size (MB)

Available HMC disk space: 19.00 GB

Figure 5-25 Manage Install Resources window

An operating environment installation resource is the necessary set of installation files for a specific version of an operating environment at a specific release and modification level. The installation resource can be on the local hard drive for the HMC or it can be on a Network Installation Management (NIM) server that the HMC can access.

The following prerequisites must be met:

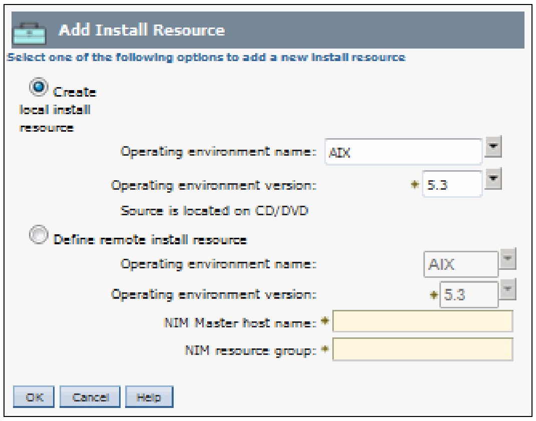
- You can define only one local installation resource for a specific operating environment and modification level. For example, you can define a local resource for AIX 6.1 and another for AIX 7.1, but you cannot define two local installation resources for the same AIX version and modification level. This restriction applies to all listed operating environments.
- The HMC must have enough free hard disk space for the necessary set of operating environment installation files. The HMC creates the installation resources in the same local hard drive location that the HMC uses for main storage dumps. Consequently, a suggestion is that you maintain a certain amount of free hard drive space to avoid potential main store dump problems because main store dumps are necessary to help resolve some types of HMC errors. The typical main store dump averages 4 - 8 GB, so consider maintaining at least 10 GB of free hard drive space for these dumps when you define and create local installation resources for the HMC.

- The HMC must have a minimum of 3 GB of free hard disk space on the local hard drive. If the amount of available space is below this minimum, the Add button is unavailable and you cannot define and add a local installation resource.

When you define a remote NIM server installation resource, several prerequisites must be met to ensure that the HMC can access and use the installation resource:

- The complete set of necessary operating environment installation files must exist on the NIM server within a uniquely named NIM resource group.
- You can define multiple remote installation resources for a specific operating environment version and modification level, as long as each installation resource is within a different NIM named resource group.
- You must know the fully qualified host name of the NIM server.
- You must know the resource group name.
- You must set up the HMC to be able to access the NIM server. The HMC must be able to run secure shell commands by means of an SSH connection to access the NIM server successfully.

If you click **Add** on the Manage Install Resources window, the Add Install Resource window opens (Figure 5-26). This window is where you can specify whether to create a local installation resource or to define a remote installation resource for the HMC.



Add Install Resource

Select one of the following options to add a new install resource

● Create local install resource

Operating environment name: AIX

Operating environment version: * 5.3

Source is located on CD/DVD

○ Define remote install resource

Operating environment name: AIX

Operating environment version: * 5.3

NIM Master host name: *

NIM resource group: *

Figure 5-26 Add Install Resource window

The following operating environments are supported for the *local* installation resources:

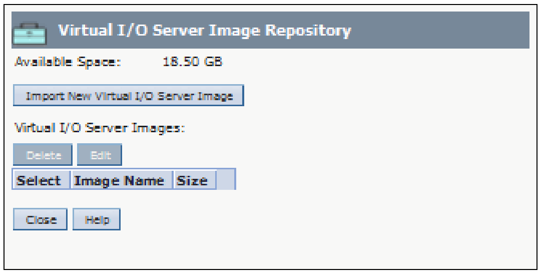
- AIX
- Red Hat Enterprise Linux Application Server
- Red Hat Enterprise Linux Server
- SUSE Linux Enterprise Server
- Virtual I/O Server

The following operating environments are supported for the *remote* installation resources:

- AIX
- Virtual I/O Server

Manage Virtual I/O Server image

If you select the **Manage Virtual I/O Server image** management task, the Virtual I/O Server Image Repository window opens (Figure 5-27). You can use this window to add or remove VIOS installation image resources on the HMC.


Virtual I/O Server Image Repository
Import New Virtual I/O Server Image
Virtual I/O Server Images:
Delete
Edit
Close
Help

Available Space: 18.50 GB

Select	Image Name	Size

Figure 5-27 Virtual I/O Server Image Repository

These prerequisites must be met before you can begin the installation of the VIOS image:

- You must have HMC super administrator privileges (`hmcsuperadmin`) to install a VIOS image.
- Ensure that a DVD that contains the VIOS image in the `.iso` format is inserted into the disk drive, if you want to get the image from a DVD.

If you click **Import New Virtual I/O Server Image** on the Virtual I/O Server Image Repository window you can select a source from which to import the image:

- DVD in the HMC disk drive
- Remote NFS-Server
- Remote FTP-Server
- Remote SFTP-Server

An HMC that has a total disk space of 80 GB can store a maximum of two VIOS images and 300 GB disk space can store a maximum of five VIOS images. When the disk space is 500 GB or more, the HMC can store a maximum of ten images.

5.2.4 Updates

Click **HMC Management** → **Updates** to see the following tasks:

- For the update of the management console task, see 5.3.4, “Update the Hardware Management Console” on page 320.
- For the update of managed systems task, see 6.9.6, “Managed system firmware updates” on page 467.

5.2.5 Users and Roles

Click **HMC Management** → **Users and Roles** to see the following management tasks:

- Change User Password

  Use this management task to change a HMC access password. The task is further explained in 4.2.1, “Change User Password option” on page 273.

- Manage User Profiles and Access

  Use this management task to add, copy, remove, and change an user profile, and modify access rights of users for the management console. The task is further explained in 4.2.2, “Manage User Profiles and Access option” on page 273.

- Manage Users and Tasks

  Use this management task to display a list of users that are currently logged on and the list of tasks that are run on the HMC. The task is further explained in 4.2.3, “Manage Users and Tasks option” on page 276.

- Manage Task and Resource Roles

  Use this management task to define and customize manage resource roles and task roles. The task is explained in 4.2.4, “Manage Task and Resource Roles option” on page 278.

5.2.6 Systems and Console Security

Click **HMC Management** → **Systems and Console Security** to see the following management tasks:

- Manage Certificates

  Use this management task to manage the certificates that are used on the HMC. You can create a new certificate for the console, change the property values of a certificate, and work with existing and archived certificates. The task is further explained in 4.3.1, “Manage Certificates option” on page 282.

- Manage LDAP

  Use this management task to configure the Lightweight Directory Access Protocol (LDAP) access options that are used by this HMC for LDAP remote authentication. The task is further explained in 4.3.2, “Manage LDAP option” on page 285.

- Manage KDC

  Use this management task to configure the key distribution center (KDC) access options that are used by this HMC for Kerberos remote authentication. The task is further explained in 4.3.3, “Manage KDC option” on page 286.

- Enable Remote command Execution

  Use this management task to enable remote command execution by using the SSH facility. The task is further explained in 4.3.4, “Enable Remote Command Execution option” on page 287.

- Enable Remote Operation

  Use this management task to control whether the HMC can be operated with a web browser from a remote workstation. The task is further explained in 4.3.5, “Enable Remote Operation option” on page 287.

- Enable Remote Virtual Terminal

  Use this management task to configure remote virtual terminal access for remote clients. The task is explained in 4.3.6, “Enable Remote Virtual Terminal option” on page 287.

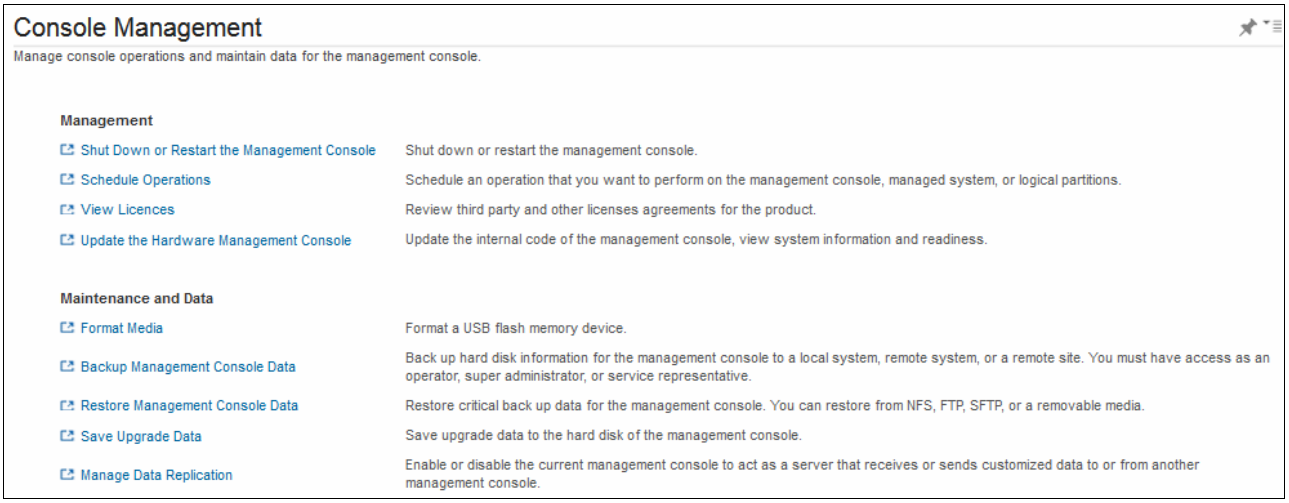
5.2.7 Deferred management tasks

In the Enhanced+ GUI, some tasks that exist in the Classic GUI are no longer supported. To use those tasks, switch to the Classic GUI. The following Classical GUI tasks are described in the *IBM Power Systems HMC Implementation and Usage Guide*, SG24-7491:

- Tip of the Day
- Change Default User Interface Settings
- Change User Interface Settings
- Manage Certificates
- Create Welcome Text

5.3 Console Management

This section describes tasks for managing the HMC and maintaining its internal code. Select **HMC Management** → **Console Management**. The Console Management menu opens (Figure 5-28). From here, you can manage console operations and maintain data for the management console. These tasks are explained in the following sections.



Console Management

Manage console operations and maintain data for the management console.

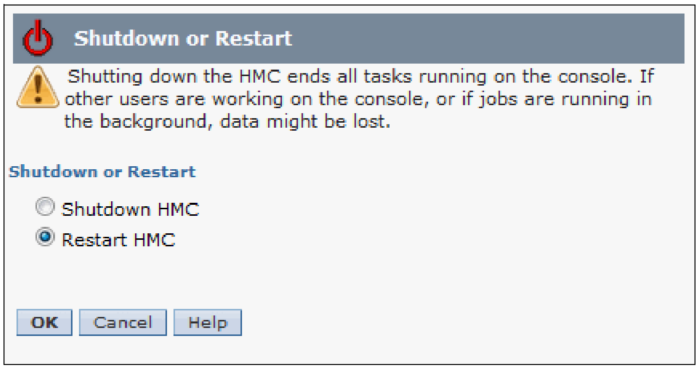
Management	
Shut Down or Restart the Management Console	Shut down or restart the management console.
Schedule Operations	Schedule an operation that you want to perform on the management console, managed system, or logical partitions.
View Licences	Review third party and other licenses agreements for the product.
Update the Hardware Management Console	Update the internal code of the management console, view system information and readiness.
Maintenance and Data	
Format Media	Format a USB flash memory device.
Backup Management Console Data	Back up hard disk information for the management console to a local system, remote system, or a remote site. You must have access as an operator, super administrator, or service representative.
Restore Management Console Data	Restore critical back up data for the management console. You can restore from NFS, FTP, SFTP, or a removable media.
Save Upgrade Data	Save upgrade data to the hard disk of the management console.
Manage Data Replication	Enable or disable the current management console to act as a server that receives or sends customized data to or from another management console.

Figure 5-28 Console Management menu

5.3.1 Shut Down or Restart the Management Console

Select **Console Management** → **Shut Down or Restart the Management Console**. The Shutdown or Restart window opens (Figure 5-29). Here you can shut down (turn off) or restart the console.

- To shut down the console, select **Shutdown HMC** and then click **OK**.
- To restart the console, select **Restart HMC** and then click **OK**.



Shutdown or Restart

Shutting down the HMC ends all tasks running on the console. If other users are working on the console, or if jobs are running in the background, data might be lost.

Shutdown or Restart

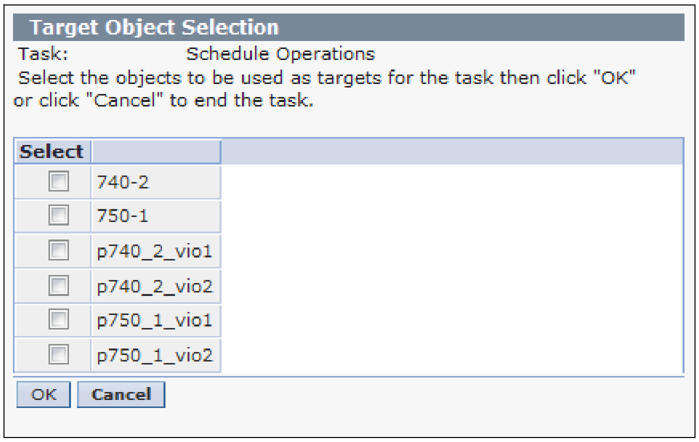
○ Shutdown HMC
● Restart HMC

Figure 5-29 Shutdown or Restart window

5.3.2 Schedule Operations

Select **Console Management** → **Schedule Operations**. The Target Object Selection window opens (Figure 5-30). Use this window to create a schedule for certain operations to be performed on the managed system without operator assistance. Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations are necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times. For example, you can schedule power on or power off operations for a managed system.

First select a managed system or a logical partition on one of the managed systems (Figure 5-30).



Target Object Selection

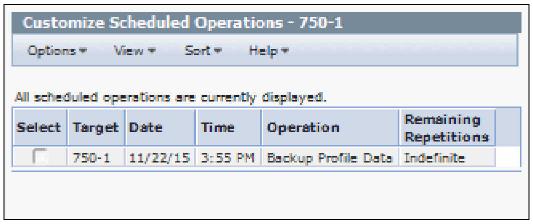
Task: Schedule Operations

Select the objects to be used as targets for the task then click "OK" or click "Cancel" to end the task.

Select	
□	740-2
□	750-1
□	p740_2_vio1
□	p740_2_vio2
□	p750_1_vio1
□	p750_1_vio2

Figure 5-30 Target Object Selection window

When you select an object to be used for a schedule, the Customize Scheduled Operations window opens (Figure 5-31). Here you see an overview of all your scheduled operations.



All scheduled operations are currently displayed.

Select	Target	Date	Time	Operation	Remaining Repetitions
□	750-1	11/22/15	3:55 PM	Backup Profile Data	Indefinite

Figure 5-31 Customize Scheduled Operations window

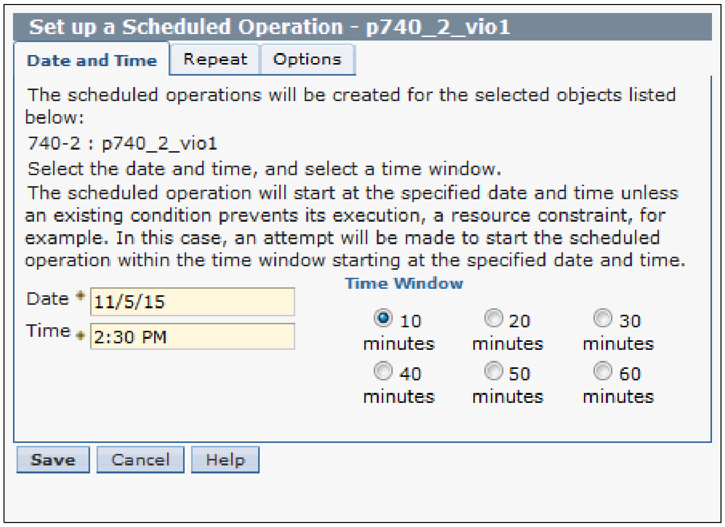
In addition to the Help menu, the following menus are available on the menu bar:

- Click **Options** to select the following items:
  - **New** to create a new scheduled operation
  - **Delete** to remove a scheduled operation
  - **Refresh** to update the current list of scheduled operations
  - **Select All** to choose all scheduled operations currently displayed
  - **Deselect All** to deselect all scheduled operations that were currently selected
  - **Exit** to exit this task
- Click **View** to select the following items:
  - **Scheduled Details** to display schedule information for the selected operation
  - **New Time Range** to specify a definite time range for the selected operation
- Click **Sort** to select how you want to view the list of scheduled operations:
  - **By Date and Time**
  - **By Object**
  - **By Operation**

If you create a new scheduled operation on an object, you must provide an operation you want to schedule on this object:

- For managed systems, you can choose one of the following scheduled operations:
  - Activate on a System Profile
  - Back up Profile Data
  - Power Off Managed System
  - Power on Managed System
  - Manage Utility CoD processors
  - Manage Utility CoD processor minute usage limit
  - Modify a Shared Processor Pool
  - Move a partition to a different pool
  - Change power saver mode on a managed system
- For logical partitions (including Virtual I/O Servers) you could choose one of the following scheduled operations:
  - Activate on an LPAR
  - Dynamic Reconfiguration
  - Operating System Shutdown (on a partition)

When you select an operation, the Set up a Schedule Operation window opens (Figure 5-32). From here, you can set up the date and time for the scheduled operation, the repeat options for the scheduled operation, and further options depending on the operation you select. After you select, click **Save** to activate the schedule.



Set up a Scheduled Operation - p740_2_vio1

The scheduled operations will be created for the selected objects listed below:

740-2 : p740_2_vio1

Select the date and time, and select a time window.

The scheduled operation will start at the specified date and time unless an existing condition prevents its execution, a resource constraint, for example. In this case, an attempt will be made to start the scheduled operation within the time window starting at the specified date and time.

Date * 11/5/15

Time * 2:30 PM

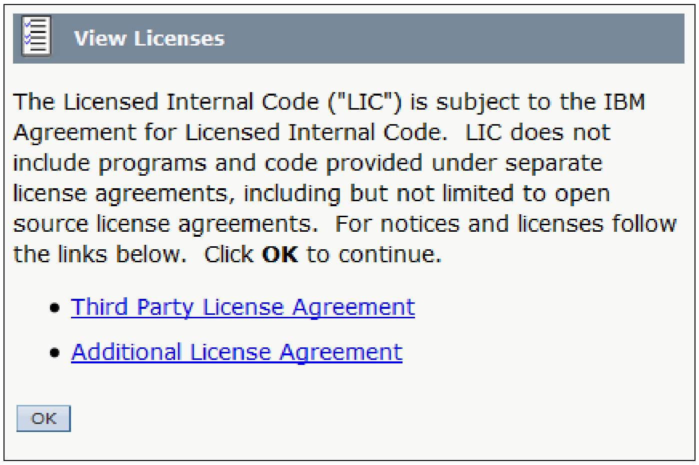
Time Window

● 10 minutes ○ 20 minutes ○ 30 minutes
○ 40 minutes ○ 50 minutes ○ 60 minutes

Figure 5-32 Set up a Scheduled Operation window

5.3.3 View Licenses

Select **Console Management** → **View Licenses**. The View Licenses window opens (Figure 5-33). You can view the *Third Party License Agreement* and the *Additional License Agreement* that you agreed to for this HMC.



View Licenses

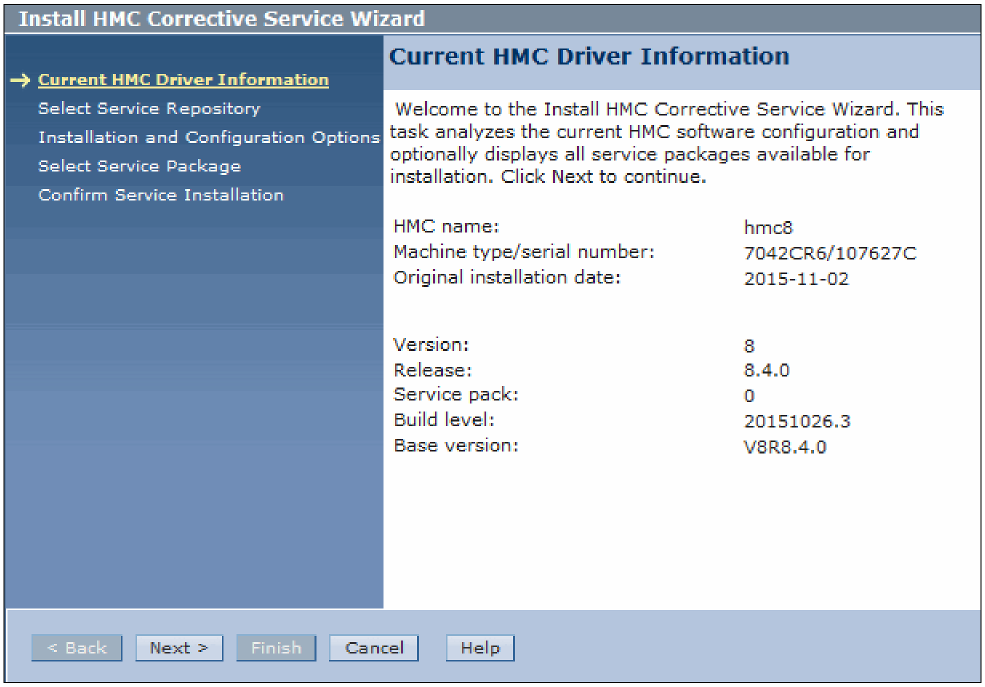
The Licensed Internal Code ("LIC") is subject to the IBM Agreement for Licensed Internal Code. LIC does not include programs and code provided under separate license agreements, including but not limited to open source license agreements. For notices and licenses follow the links below. Click **OK** to continue.

- Third Party License Agreement
- Additional License Agreement

Figure 5-33 View Licenses window

5.3.4 Update the Hardware Management Console

Select **Console Management** → **Update the Hardware Management Console**. The Install HMC Corrective Service Wizard opens (Figure 5-34).


Install HMC Corrective Service Wizard
→ Current HMC Driver Information
Select Service Repository
Installation and Configuration Options
Select Service Package
Confirm Service Installation
< Back
Next >
Finish
Cancel
Help

Current HMC Driver Information

Welcome to the Install HMC Corrective Service Wizard. This task analyzes the current HMC software configuration and optionally displays all service packages available for installation. Click Next to continue.

HMC name:	hmc8
Machine type/serial number:	7042CR6/107627C
Original installation date:	2015-11-02
Version:	8
Release:	8.4.0
Service pack:	0
Build level:	20151026.3
Base version:	V8R8.4.0

Figure 5-34 Install HMC Corrective Service Wizard

The Wizard guides you through five steps:

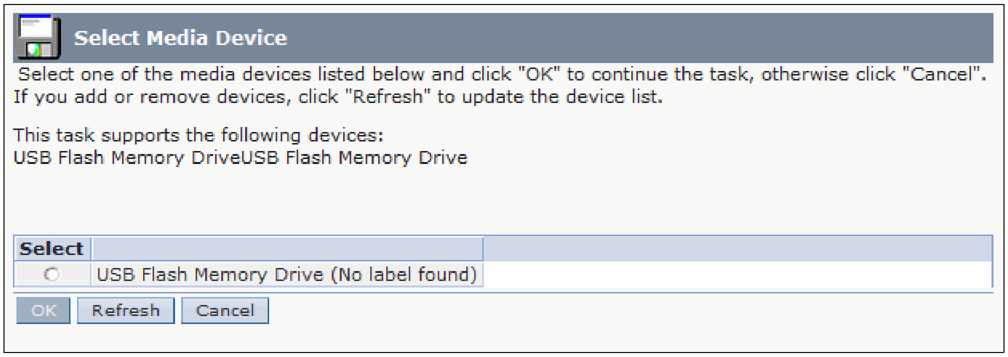
1. The first window shows the HMC Release Level with some further information. Click **Next**.
2. In the next window, select the location of where the new software for the HMC can be found: on **Removable media** or on a **Remote Server**. Then, click **Next**.
3. Depending on which on you selected in the previous step, do one of these steps and then click **Next**:
   - If you selected Removable media, select the source of where it is located:
     - CD-ROM or DVD-RAM
     - USB Flash Memory Device
     - Diskette
   - If you selected Remote Server, specify the type of remote server:
     - FTP
     - NFS
     - SFTP

     Then specify the connection parameters (Remote Server, User ID, Password, Remote directory).
4. The HMC then checks the specified repository whether a service package is available on the specified resource. If so, it will be displayed on the next window, where you select the service package that you want to install (more than one might be available). After you select a service package, click **Next**.
5. On the final window, confirm your selection before the installation begins and click **Finish**.

The HMC now downloads the service pack to local disk and then installs the service pack. This process can take a while. After, you must reboot the HMC to activate the new code level.

5.3.5 Format Media

Select **Console Management** → **Format Media**. The Select Media Device window opens (Figure 5-35). Here you can select a media device to format (for example a USB Flash Memory Drive or a DVD-RAM) and after clicking **OK** the media will be formatted. You cannot do this task remotely unless you already placed the media in the system.


Select Media Device

Select one of the media devices listed below and click "OK" to continue the task, otherwise click "Cancel". If you add or remove devices, click "Refresh" to update the device list.

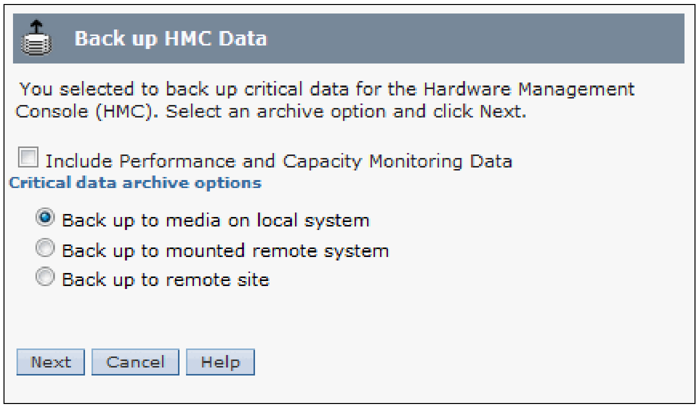
This task supports the following devices:
USB Flash Memory DriveUSB Flash Memory Drive

Select	
○	USB Flash Memory Drive (No label found)

Figure 5-35 Select Media Device window

5.3.6 Backup Management Console Data

Select **Console Management** → **Backup Management Console Data**. The Backup HMC Data window opens (Figure 5-36).


Back up HMC Data

You selected to back up critical data for the Hardware Management Console (HMC). Select an archive option and click Next.

□ Include Performance and Capacity Monitoring Data

Critical data archive options

● Back up to media on local system
○ Back up to mounted remote system
○ Back up to remote site

Figure 5-36 Back up HMC Data window

It has three options of where to back up the critical data of the HMC:

- Back up to media on local system. This backs up to DVD-RAM or USB Flash Memory Drive.
- Back up to mounted remote system. This backs up is through NFS.
- Back up to remote site. This backs up through FTP or SFTP.

You can further choose whether to include the Performance and Capacity Monitoring Data in the backup.

For the backup to a mounted remote system or to a remote site, specify the connection details. For the backup to media on local system, ensure that the media is formatted (see 5.3.5, “Format Media” on page 321).

To back up the HMC, you must be a member of one of the following roles:

- Super administrator
- Operator
- Service representative

After you select a backup option, click **Next** and follow the instructions to back up the data. The backup can take a considerable amount of time.

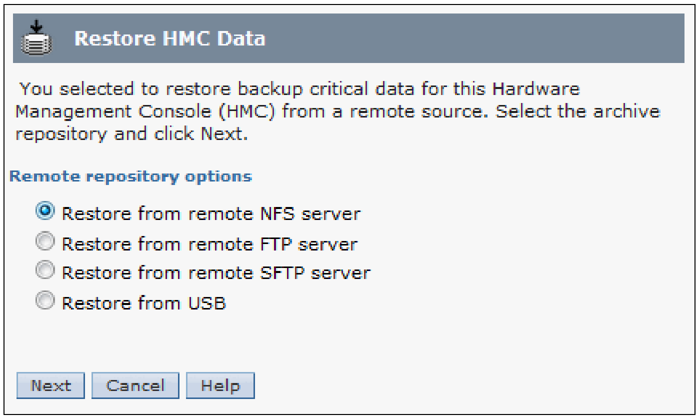
> **Notes:**
>
> - If any HMC corrective services to the HMC have been installed, the resulting backup archive size can grow considerably, generally greater than 1 GB.
> - Do not power off the HMC while a backup task is running.
> - You cannot have more than one instance of the backup task running. This includes any scheduled HMC backup operations.

Scheduled HMC Data backup

Back up the HMC Data at least once a week. Also keep two copies of the HMC Data backup: one copy from the upgrade or any changes to the HMC, and one HMC Data backup to store in a safe place.

5.3.7 Restore Management Console Data

Select **Console Management** → **Restore Management Console Data**. The Restore HMC Data window opens (Figure 5-37).



You selected to restore backup critical data for this Hardware Management Console (HMC) from a remote source. Select the archive repository and click Next.

Remote repository options

- ● Restore from remote NFS server
- ○ Restore from remote FTP server
- ○ Restore from remote SFTP server
- ○ Restore from USB

Figure 5-37 Restore HMC data window

Select one of the options and click **Next**:

- Restore from remote NFS server
- Restore from remote FTP server
- Restore from remote SFTP server
- Restore from USB

Restoring data

If the critical console data was archived remotely, follow these steps to restore:

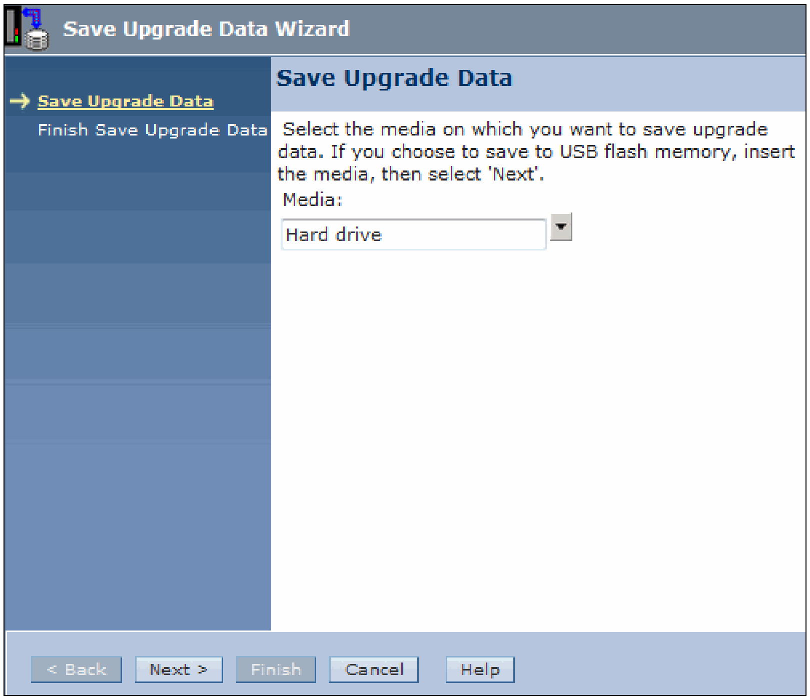
1. Manually reconfigure network settings to enable access to the remote server after the HMC is installed. For information about configuring network settings, see 4.1.2, “Configuring the HMC network settings” on page 260.
2. In the HMC Main window, select **HMC Managemen**t → **Console Management** → **Restore Management Console Data**. Then select the type of restoration and click **Next**.
3. Follow the directions to restore the HMC data. The data restores automatically from the remote server when the HMC restarts.

5.3.8 Save Upgrade Data

Select **Console Management** → **Save Upgrade Data**. The Save Upgrade Data Wizard opens (Figure 5-38). This wizard saves upgrade data to the selected media. The data consists of files that were created or customized while running the current software level. Saving this data to selected media is performed prior to a HMC software upgrade. These are the two location options to save the data:

- Hard Drive
- USB flash memory device

Select one of them from the Media drop-down and click **Next**. On the next panel, click **Finish**, and the data will be saved to the selected location. If you selected USB flash memory device, remember to format the device before you save the upgrade data onto this device, see 5.3.5, “Format Media” on page 321.



Save Upgrade Data

Select the media on which you want to save upgrade data. If you choose to save to USB flash memory, insert the media, then select 'Next'.

Media: Hard drive

Figure 5-38 Save Upgrade Data Wizard

Note: Do this task prior to an HMC software upgrade. Any configuration changes made after performing this task will not be included with the new HMC software release.

If the save upgrade data task fails, do not continue with the upgrade process.

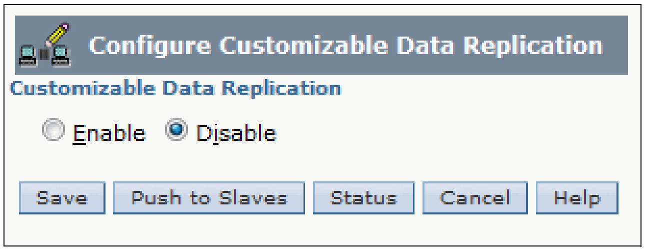
5.3.9 Manage Data Replication

Select **Console Management** → **Manage Data Replication**. The Configure Customizable Data Replication window opens (Figure 5-39). Use this window to enable or disable the ability of this HMC to act as a server of customizable console data and to indicate whether this HMC can accept customizable console data sent by another HMC.

After you enable or disable this service and save the settings, this settings become effective immediately.

If you enable Data Replication, this HMC is completely configured to act as a server of customized data, but you need to perform further configuration steps (select data sources, data types) to control whether this HMC will accept customizable console data from other consoles.

Note: Before you enable this replication service, save your original data settings in case you need to restore these settings in the future.



Configure Customizable Data Replication

Customizable Data Replication

○ Enable ● Disable

Figure 5-39 Configure Customizable Data Replication window

You can configure the following types of data:

- User Profiles data

  User identifications, methods of authentication, user managed resource roles and task roles, logon session properties, and remote access settings

- Kerberos Configuration Data

  Key Distribution Center (KDC), realm, and host name that is used by the HMC for Kerberos authentication

- LDAP Configuration Data

  LDAP server name and distinguished name tree that is used by the HMC for LDAP authentication

- Password Policy Configuration Data

  The information required to ensure passwords meet the password strength required by your IT policies

- Customer Information Data

  Customer information for a server or group or servers that includes administrator, system, and account information about the system that is being installed

- Group data

  All user-defined groups that are defined to the HMC

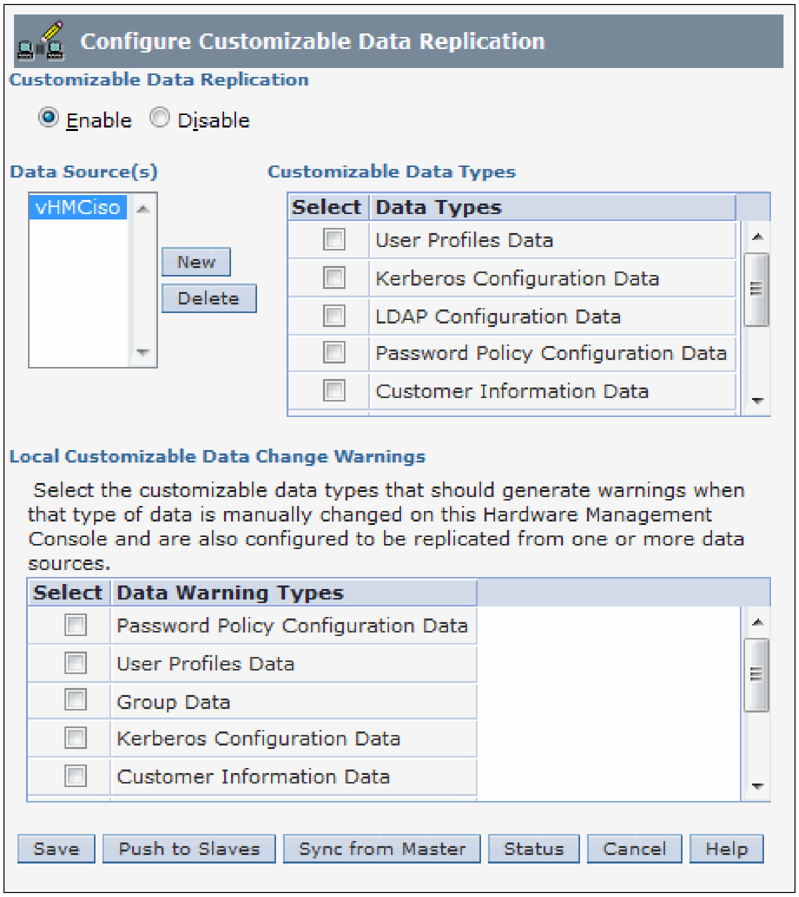
- Modem Configuration Data

  Dial type (tone or pulse) and other settings such as whether to wait for a dial tone

- Outbound Connectivity Data

  Information for dialing out, such as whether to enable the local system as a call-home server, or whether to allow dialing to use the local modem, the dial prefix, and phone numbers

Figure 5-40 shows the types of customizable console data that can be replicated.



Configure Customizable Data Replication

Customizable Data Replication

● Enable ○ Disable

Data Source(s)

vHMCiso

Customizable Data Types

Select	Data Types
□	User Profiles Data
□	Kerberos Configuration Data
□	LDAP Configuration Data
□	Password Policy Configuration Data
□	Customer Information Data

Local Customizable Data Change Warnings

Select the customizable data types that should generate warnings when that type of data is manually changed on this Hardware Management Console and are also configured to be replicated from one or more data sources.

Select	Data Warning Types
□	Password Policy Configuration Data
□	User Profiles Data
□	Group Data
□	Kerberos Configuration Data
□	Customer Information Data

Figure 5-40 Manage Data Replication Task

You can enable the Customizable Data Replication service for the following types of operations:

- Peer-to-Peer replication

  Provides automatic replication of the selected customized data type between peer HMCs. Changes that are made on any of these consoles are replicated to the other consoles.

- Master-to-subordinated replication

  Provides automatic replication of the selected customized data types from one or more designated master HMCs to one or more designated subordinates HMCs. Changes that are made on a master console are automatically replicated to the subordinate console.

Configuring Peer-to-Peer replication

To configure Peer-to-Peer replication, follow these steps:

1. Select **Console Management** → **Manage Data Replication**.
2. Select **Enable** in the Configure Customizable Data Replication window.
3. Click **New** under Data Source. The configure New Replication Source window opens.
4. Select an HMC to be used as data source from the Discovered Console Information list, and click **Add**.

   Alternatively, you can enter the TCP/IP address of the HMC that you want to use as a data source in the TCP/IP Address Information field, and then click **Find**.
5. The Customizable Data Replication window opens again.
6. Select the types of data that you want to replicate from the Customizable Data Types list, from a peer HMC that is selected currently under Data Source.
7. Click **Save** to close the Customizable Data Replication window.
8. Repeat steps 1 through 7 on each of the HMCs that you want to act as peers with one another.

Note: When communication is established between the HMCs, the requested types of customizable data are replicated automatically from one HMC to the other immediately following the change in the data itself.

Configuring master-to-subordinate replication

To configure master-to-subordinate replication involves two steps:

1. Setting up a master console.
2. Setting up the subordinate console.

Setting up a master console

Complete these steps:

1. Select **Console Management** → **Manage Data Replication**.
2. Select **Enable** in the Configure Data Replication window.
3. Click **Save** to close the Customizable Data Replication window.

Setting up the subordinate console

Complete these steps:

1. Select **Console Management** → **Manage Data Replication**.
2. Select **Enable** in the Configure Data Replication window.
3. Click **New** under Data Source. The configure New Replication Source window opens.

4. Select the master HMC to be used as a data source from the Discovered console Information list, and click **Add**.

   Alternatively, you can enter the TCP/IP address of the master HMC in the TCP/IP Address Information field, and then click **Find**.

5. The Customizable Data Replication window opens again.
6. Select the types of data that you want to replicate from the Customizable Data Types list, from the master HMC selected currently under Data Source.
7. Click **Save** to close the Customizable Data Replication window.
8. Repeat steps 1 through 7 on each HMC that you want to be a subordinate HMC.

> **Note:** When communication is established between the master HMC and the subordinate HMC, the requested types of customizable data are replicated automatically from the master HMC to the subordinate HMC immediately following the change in the data itself.

5.4 Resource management

This section describes resource management. Resources can be managed systems, partitions, Virtual I/O Servers, frames, shared storage pool clusters, Power Enterprise pools and groups.

Click the **Resources** icon in the left pane. The Resources menu opens (Figure 5-41).

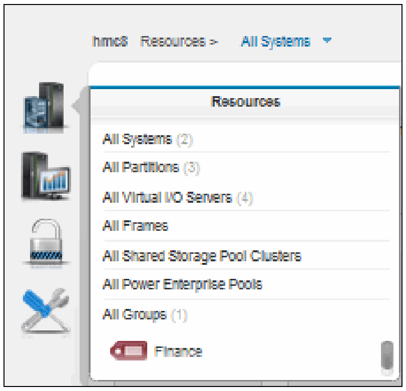

hmc8 Resources > All Systems
Resources
All Systems (2)
All Partitions (3)
All Virtual I/O Servers (4)
All Frames
All Shared Storage Pool Clusters
All Power Enterprise Pools
All Groups (1)
Finance

Figure 5-41 Resource management menu

The menu also shows the number of each resource managed by the HMC. For the Group resource, a list of the groups are listed in the menu.

In the following sections each resource task is explained in more detail.

5.4.1 All Systems

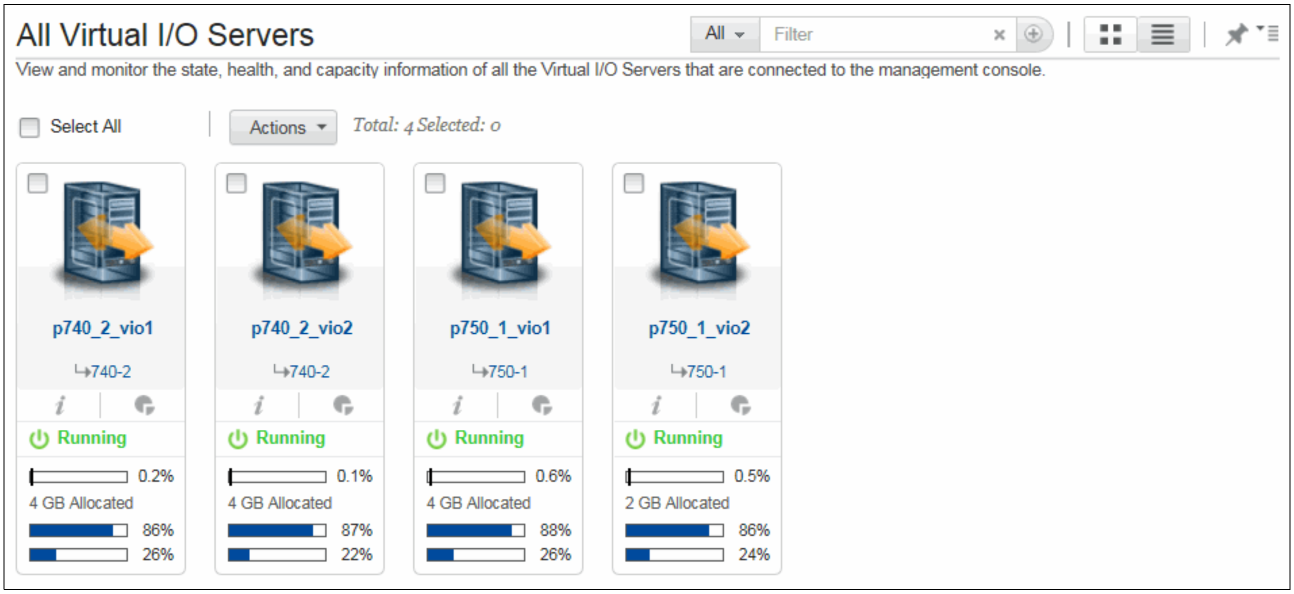
Use the **All Systems** resource management task to manage your managed systems. This task is explained in 5.5, “Systems Management for Servers” on page 340.

5.4.2 All Partitions

Use the **All Partitions** resource management task to manage your partitions (AIX, IBM i, or Linux). This task is explained in 5.6, “Partition management” on page 370.

5.4.3 All Virtual I/O Servers

Use the **All Virtual I/O Servers** resource management task to manage your Virtual I/O Servers. When you select the task an overview of your Virtual I/O Servers is displayed (Figure 5-42).



All Virtual I/O Servers

View and monitor the state, health, and capacity information of all the Virtual I/O Servers that are connected to the management console.

Total: 4 Selected: 0

Figure 5-42 Virtual I/O Servers overview

You can list the Virtual I/O Servers (VIOS) in a table view by clicking the **Display Table View** button in the upper right corner.

You can select a Virtual I/O Server and perform different actions on it on a specific Virtual I/O Server. Use either of the following methods to access the actions you can use:

- Select a VIOS and click **Actions**.
- Double-click a VIOS name.

The General Properties pane opens with the menu on the left (Figure 5-43). The upper part shows status information about the selected Virtual I/O Server. The menu structure is explained in the following sections.

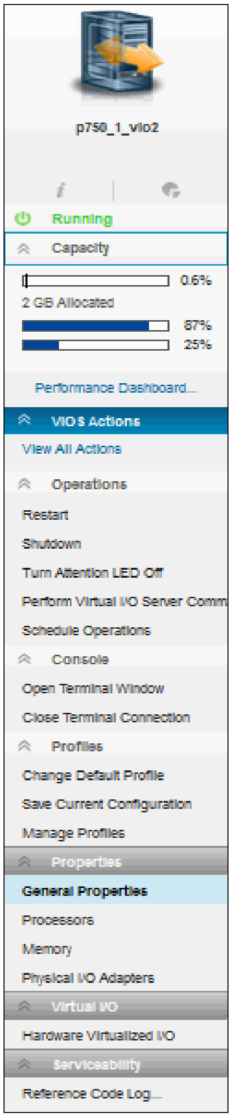


Figure 5-43 Virtual I/O Server menu

Capacity

The Capacity area shows an overview of some performance data. For details, click the **Performance Dashboard** link in the menu. The Performance and Capacity (PCM) page opens. For more information, see Chapter 7, “Performance and capacity monitoring” on page 511.

Operations

Use the Operations area for doing basic management operations with the selected VIOS. Select any of the following options:

- Restart

  Click **Restart** to start the reboot of the Virtual I/O Server. You can then select any of the following options:

  - Dump

    Initiates a system memory dump on the VIOS and restarts the VIOS when complete.

  - Operating System

    Issues the operating system command to restart the VIOS normally.

  - Immediate

    Restarts the VIOS as quickly as possible, without notifying it. This option might cause undesirable results if data was partially updated.

  - Operating System Immediate

    Issues the operating system command to restart the VIOS immediately.

  - Dump Retry

    Retries a system memory dump for the VIOS and restarts the VIOS when complete.

- Shutdown

  Click **Shutdown** to start the shut down process of the selected VIOS. You can select any of the following options:

  - Delayed

    Shut down the VIOS by starting the delayed power-off sequence.

  - Immediate

    Shuts down the VIOS as quickly as possible, without notifying it. This option might cause undesirable results if data has been partially updated.

  - Operating System

    Issues the operating system command to shut down the VIOS normally.

  - Operating System Immediate

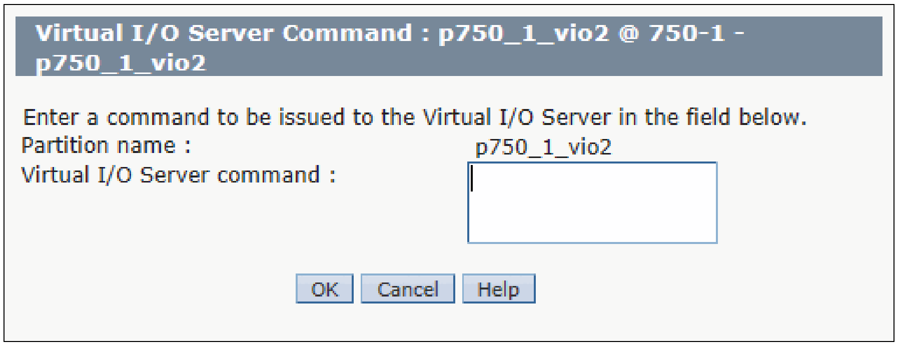
    Issues the operating system command to shut down the VIOS immediately.

  - Turn Attention LED Off

  Click T**urn Attention LED Off** task to turn off an active Attention LED on the selected VIOS.

- Perform Virtual I/O Server Command

  If you select the **Perform Virtual I/O Server Command** task, the window shown in Figure 5-44 on page 331 opens. Enter a command in this window, the command is then executed on the VIOS and the output of the command is displayed.



Virtual I/O Server Command : p750_1_vio2 @ 750-1 - p750_1_vio2

Enter a command to be issued to the Virtual I/O Server in the field below.

Partition name : p750_1_vio2

Virtual I/O Server command :

Figure 5-44 Virtual I/O Server command window

The commands will be passed to the VIOS through a Resource Monitoring and Control (RMC) session. Therefore the VIOS must have an external Ethernet connection to support the RMC session. You can send only `ioscli` commands (no AIX operating systems commands), and the field does not allow the use of the semicolon (`;`) or the greater than (>) character.

- Schedule Operations

  Click **Schedule Operations** task to schedule an operation for the selected VIOS. The task is further explained in 5.3.2, "Schedule Operations" on page 317.

Console

Use the Console area to manage terminals for the selected VIOS. Select any of the following options:

- Open Terminal Window

  Click **Open Terminal Window** to open a terminal window to the selected VIOS. You can have only one open terminal window for a VIOS at a time, independent how many HMCs you have.

- Close Terminal Connection

  Click **Close Terminal Connection** to close an open terminal window. Be aware that another administrator might be using this window and therefore might lose work.

Profiles

Use the Profiles area to manage the profiles of the selected VIOS. Select any of the following options:

- Change Default Profile

  Click **Change Default Profile** to make another profile the default profile.

- Save Current Configuration

  Click **Save Current Configuration** to save the state of a running partition to a new profile, or overwrite an existing profile, which you can select. This is useful if you made changes to a VIOS using DLPAR (CPU, memory, I/O), and now want make theses changes to be permanent.

- Manage Profiles

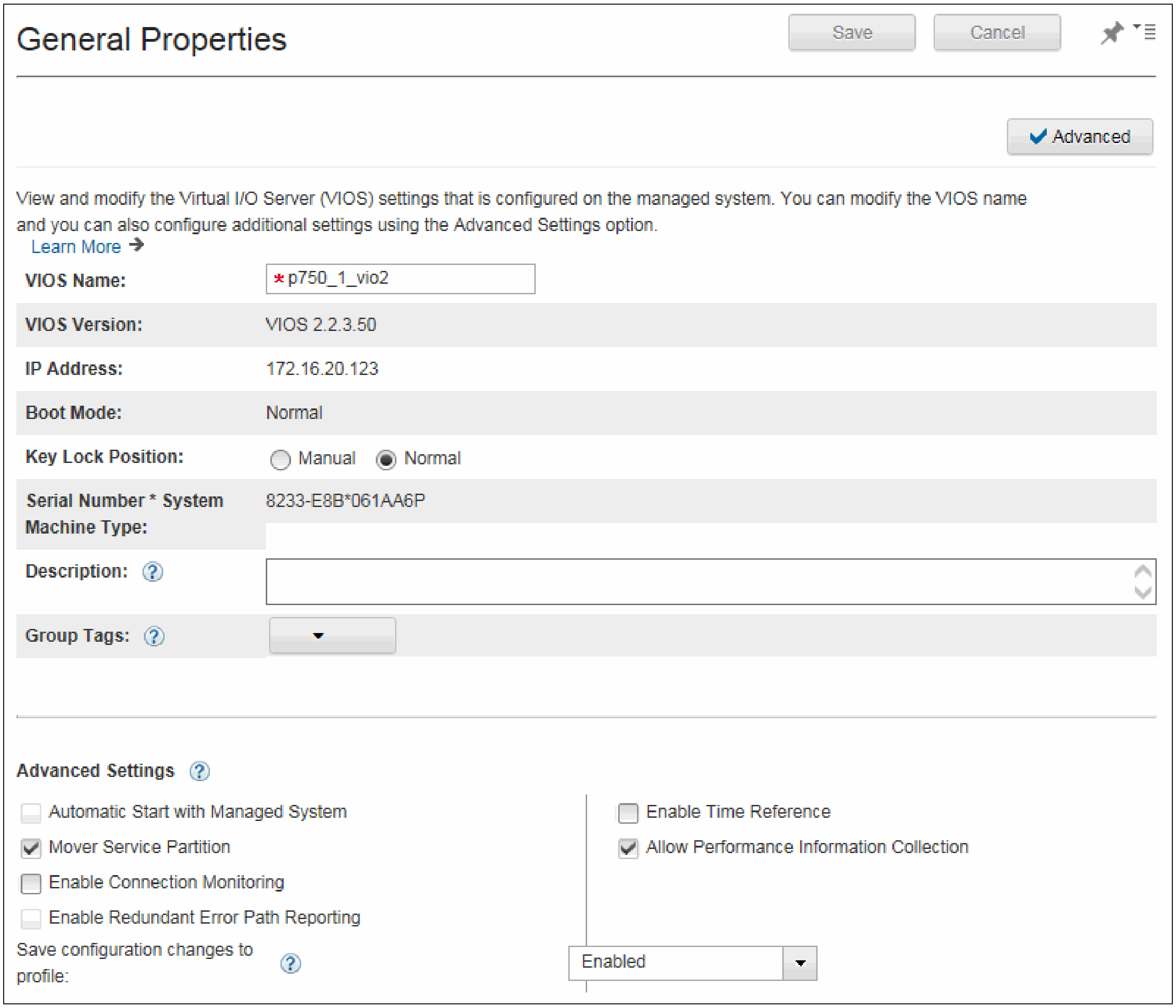
  Click **Manage Profiles** to edit every aspect of an existing profile. Also you can create a new profile, copy a profile, delete a profile, or activate a profile.

Properties

Use the Properties area to view and edit the properties of a selected VIOS. Select any of the following options:

- General Properties

  Click **General Properties** to open a view (Figure 5-45), which shows information such as name, version, or IP address of the selected VIOS. You also can change properties, such as the name of the selected VIOS, the description, or the Key Lock Position. If you click **Advanced**, more options for the VIOS become available, as Figure 5-45 shows.



General Properties

View and modify the Virtual I/O Server (VIOS) settings that is configured on the managed system. You can modify the VIOS name and you can also configure additional settings using the Advanced Settings option.
Learn More →

VIOS Name:	* p750_1_vio2
VIOS Version:	VIOS 2.2.3.50
IP Address:	172.16.20.123
Boot Mode:	Normal
Key Lock Position:	○ Manual ● Normal
Serial Number * System Machine Type:	8233-E8B*061AA6P
Description: ?	
Group Tags: ?	

Advanced Settings ?

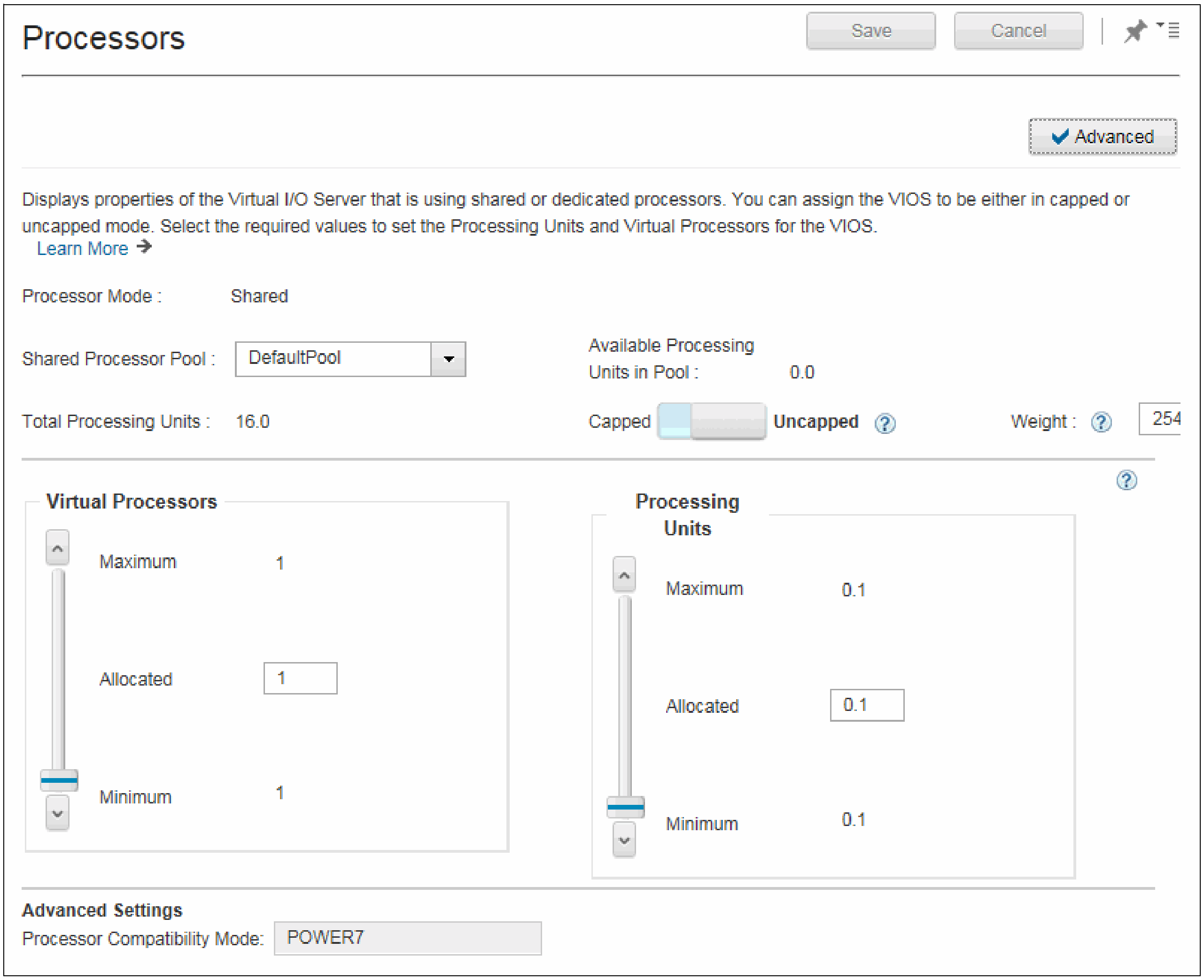
□ Automatic Start with Managed System
☑ Mover Service Partition
□ Enable Connection Monitoring
□ Enable Redundant Error Path Reporting
□ Enable Time Reference
☑ Allow Performance Information Collection

Save configuration changes to profile: ? Enabled

Figure 5-45 General Properties view with Advanced Options

- Processors

  Click **Processors** to view and edit the CPU settings for the selected VIOS (Figure 5-46). To edit the CPU settings, move the slider of the resource (Processing Units or Virtual Processors) to another value. You can also type in the exact values. If you click **Save**, a DLPAR operation initiates the changes.



Processors

Displays properties of the Virtual I/O Server that is using shared or dedicated processors. You can assign the VIOS to be either in capped or uncapped mode. Select the required values to set the Processing Units and Virtual Processors for the VIOS.

Processor Mode : Shared

Shared Processor Pool : DefaultPool

Available Processing Units in Pool : 0.0

Total Processing Units : 16.0

Capped **Uncapped**

Weight : 254

Virtual Processors

Maximum 1

Allocated 1

Minimum 1

Processing Units

Maximum 0.1

Allocated 0.1

Minimum 0.1

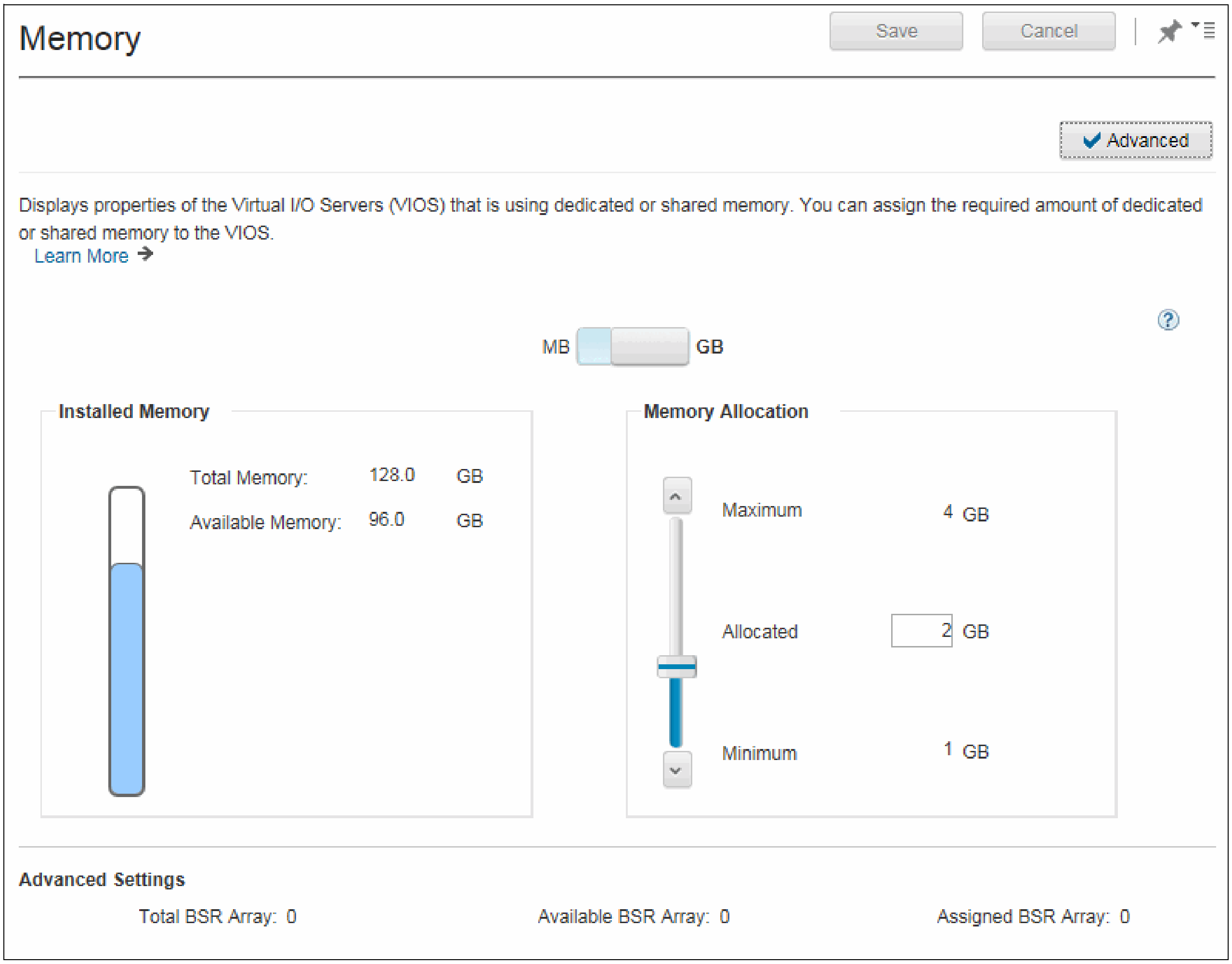
Advanced Settings

Processor Compatibility Mode: POWER7

Figure 5-46 Processor view

- Memory

  Click **Memory** to view and edit the Memory settings for the selected VIOS (Figure 5-47). To edit the memory settings, move the slider of the Memory Allocation resource to the required value. You can also type in the exact value. If you click **Save**, a DLPAR operation starts to change the value.



Displays properties of the Virtual I/O Servers (VIOS) that is using dedicated or shared memory. You can assign the required amount of dedicated or shared memory to the VIOS.

Installed Memory

Total Memory: 128.0 GB

Available Memory: 96.0 GB

Memory Allocation

Maximum 4 GB

Allocated 2 GB

Minimum 1 GB

Advanced Settings

Total BSR Array: 0

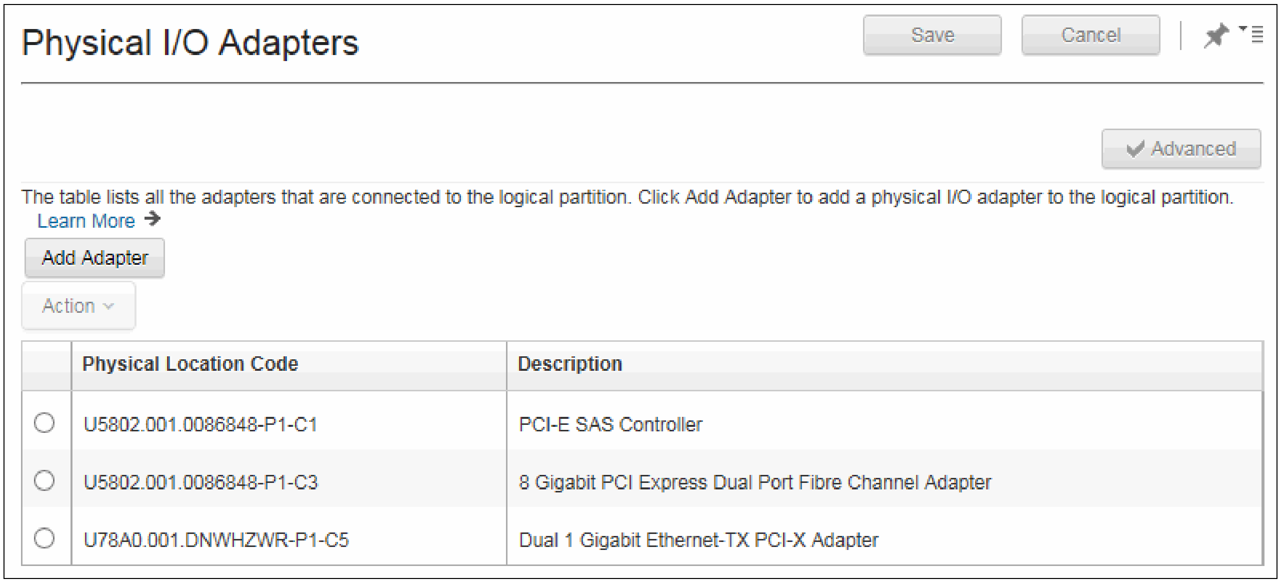
Available BSR Array: 0

Assigned BSR Array: 0

Figure 5-47 Memory view

- Physical I/O Adapters

  Click **Physical I/O Adapters** to open a panel (Figure 5-48) where you can view, add, or remove physical adapters of the selected VIOS.



The table lists all the adapters that are connected to the logical partition. Click Add Adapter to add a physical I/O adapter to the logical partition. Learn More →

	Physical Location Code	Description
○	U5802.001.0086848-P1-C1	PCI-E SAS Controller
○	U5802.001.0086848-P1-C3	8 Gigabit PCI Express Dual Port Fibre Channel Adapter
○	U78A0.001.DNWHZWR-P1-C5	Dual 1 Gigabit Ethernet-TX PCI-X Adapter

Figure 5-48 Physical I/O Adapters view

To add a physical adapter, click **Add Adapter**. A window with the available adapters in the system opens. The default filter shows all the available adapters in the system. On systems with multiple I/O drawers, you can filter by I/O drawer by selecting the I/O drawer from the View drop-down menu. A filter also can be applied to show only a specific slot in each I/O drawer, for example, slot C1, by entering the filter parameter in the Filter by Physical Location text box.

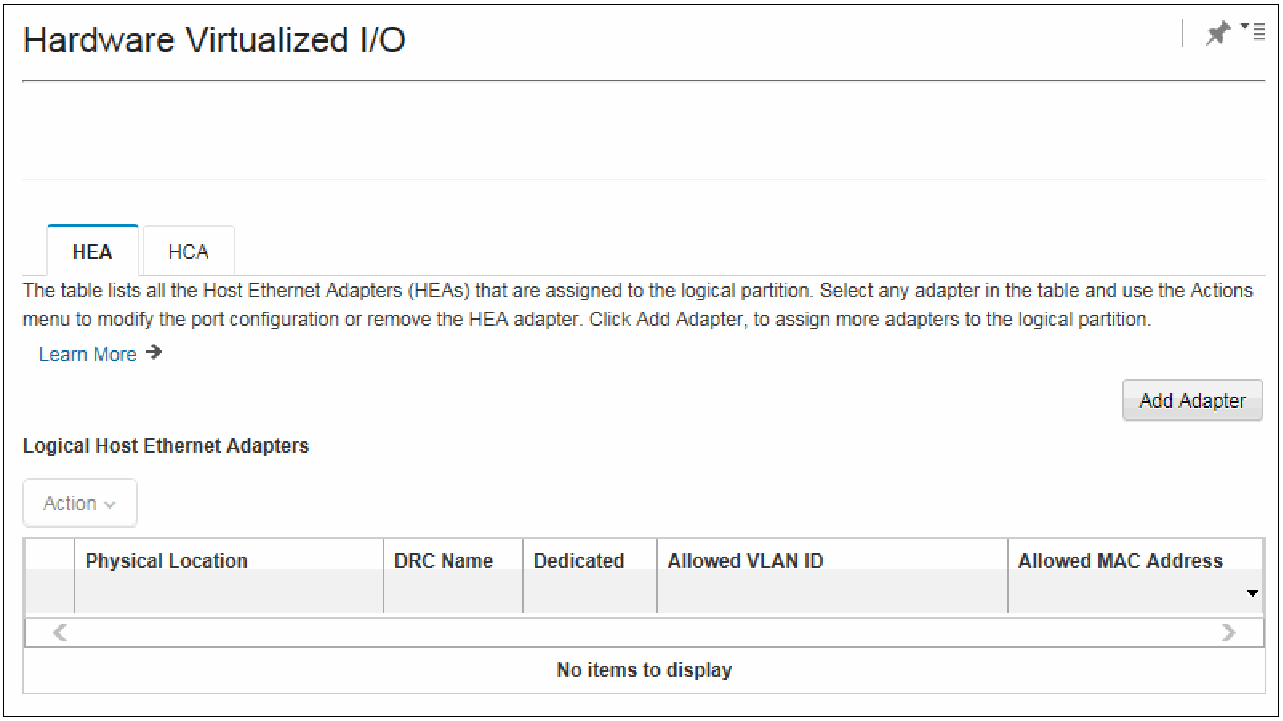
To remove a physical adapter, select the adapter to be removed and click **Action** → **Remove Adapter**.

Virtual I/O

Use the Virtual I/O area to view and edit Hardware Virtualized I/O adapters, such as Host Ethernet Adapters (HEA) and Host Channel Adapters (HCA), of a selected VIOS. Select the following option:

- Hardware Virtualized I/O

  Click **Hardware Virtualized I/O** to open a panel (Figure 5-49) where you can view, add, edit, or delete HEAs and HCAs of the selected VIOS.



The table lists all the Host Ethernet Adapters (HEAs) that are assigned to the logical partition. Select any adapter in the table and use the Actions menu to modify the port configuration or remove the HEA adapter. Click Add Adapter, to assign more adapters to the logical partition.

Logical Host Ethernet Adapters

	Physical Location	DRC Name	Dedicated	Allowed VLAN ID	Allowed MAC Address

No items to display

Figure 5-49 Hardware Virtualized I/O view

Serviceability

Use the Serviceability area to view the Reference Code Log of a selected VIOS. You can select the following option:

- Reference Code Log

  Click **Reference Code Log** to view a list of the most recent reference codes. Reference codes provide general diagnostic, troubleshooting, and debugging information. To view the details of a specific reference code, select the reference code.

5.4.4 All Frames

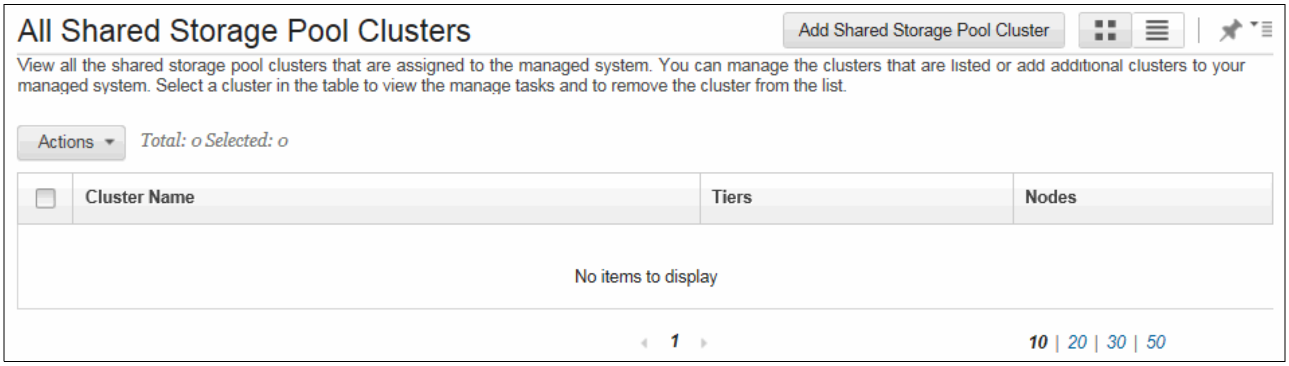
At the time of writing this task is not available in the Enhanced+ GUI. You are referred to the Classic GUI. This task is further explained in *IBM Power Systems HMC Implementation and Usage Guide*, SG24-7491.

5.4.5 All Shared Storage Pool Clusters

Use the **All Shared Storage Pool Clusters** resource management task to manage shared storage pools. Shared storage pools are a feature in PowerVM Standard and Enterprise Editions that was introduced in Virtual I/O Server 2.2.0.11 Fix Pack 11 Service Pack 1. It is a server-based storage virtualization that provides distributed storage access to Virtual I/O Server partitions for their client partitions.

For more information about shared storage pools, see *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940 and *IBM PowerVM Virtualization Managing and Monitoring*, SG24-7590.

Click **All Shared Storage Pool Clusters** to open a panel (Figure 5-50) that shows an overview of your shared storage pools.



All Shared Storage Pool Clusters

View all the shared storage pool clusters that are assigned to the managed system. You can manage the clusters that are listed or add additional clusters to your managed system. Select a cluster in the table to view the manage tasks and to remove the cluster from the list.

Total: 0 Selected: 0

□	Cluster Name	Tiers	Nodes
	No items to display		

Figure 5-50 Shared storage pool overview

Click **Add Shared Storage Pool Cluster** to add a shared storage pool cluster. You can also select a cluster in the table to view the available manage tasks and to remove the cluster from the list.

The following minimum requirements must be met before adding a shared storage pool:

- Managed system:
  - POWER6 processor-based or later
- Per Node:
  - Processor: One core
  - Memory: 4 GB
  - Adapters: One Fibre Channel
  - Disks:
    - Storage are network (SAN) disks
    - RAID protected
    - One 10 GB repository disk
    - One 10 GB pool disk
  - Network:
    - The VIOS partition must have uninterrupted network connectivity for shared storage pool operations.
    - The forward and reverse DNS lookups for a VIOS partition host name must resolve to the same IP address.

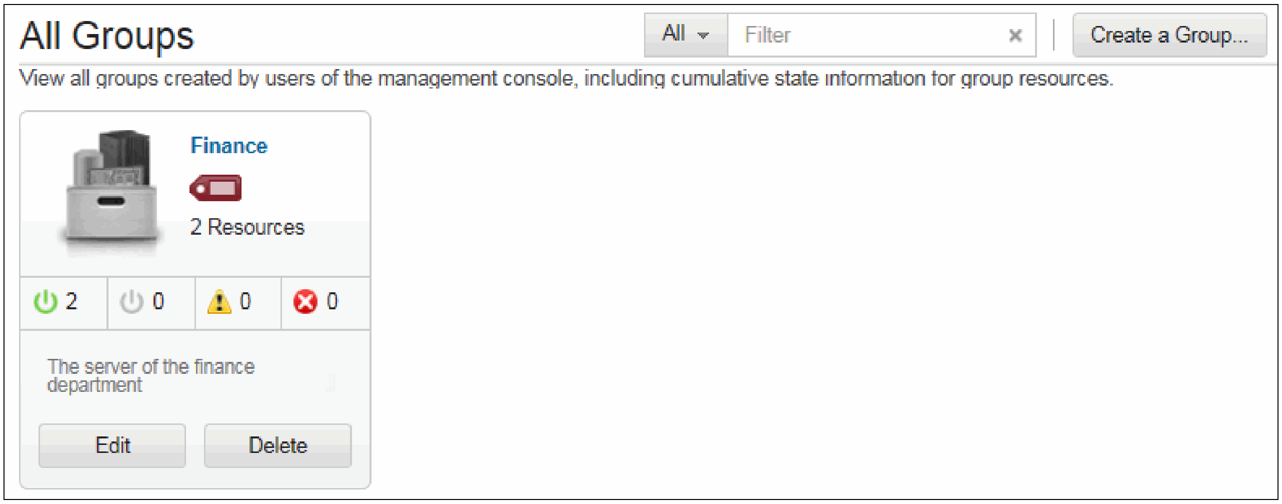
5.4.6 All Power Enterprise Pools

Use the **All Power Enterprise Pools** resource management task to manage your Power Enterprise Pools. This task is explained in 5.11.5, “Managing Power Enterprise Pools” on page 418.

5.4.7 All Groups

Use the **All Groups** resource management task to manage a group of resources in a common view. This task becomes handy if some administrators are responsible for only a group of servers on a managed system for example.

When you select the task, an overview of your groups is displayed (Figure 5-51).



View all groups created by users of the management console, including cumulative state information for group resources.

The server of the finance department

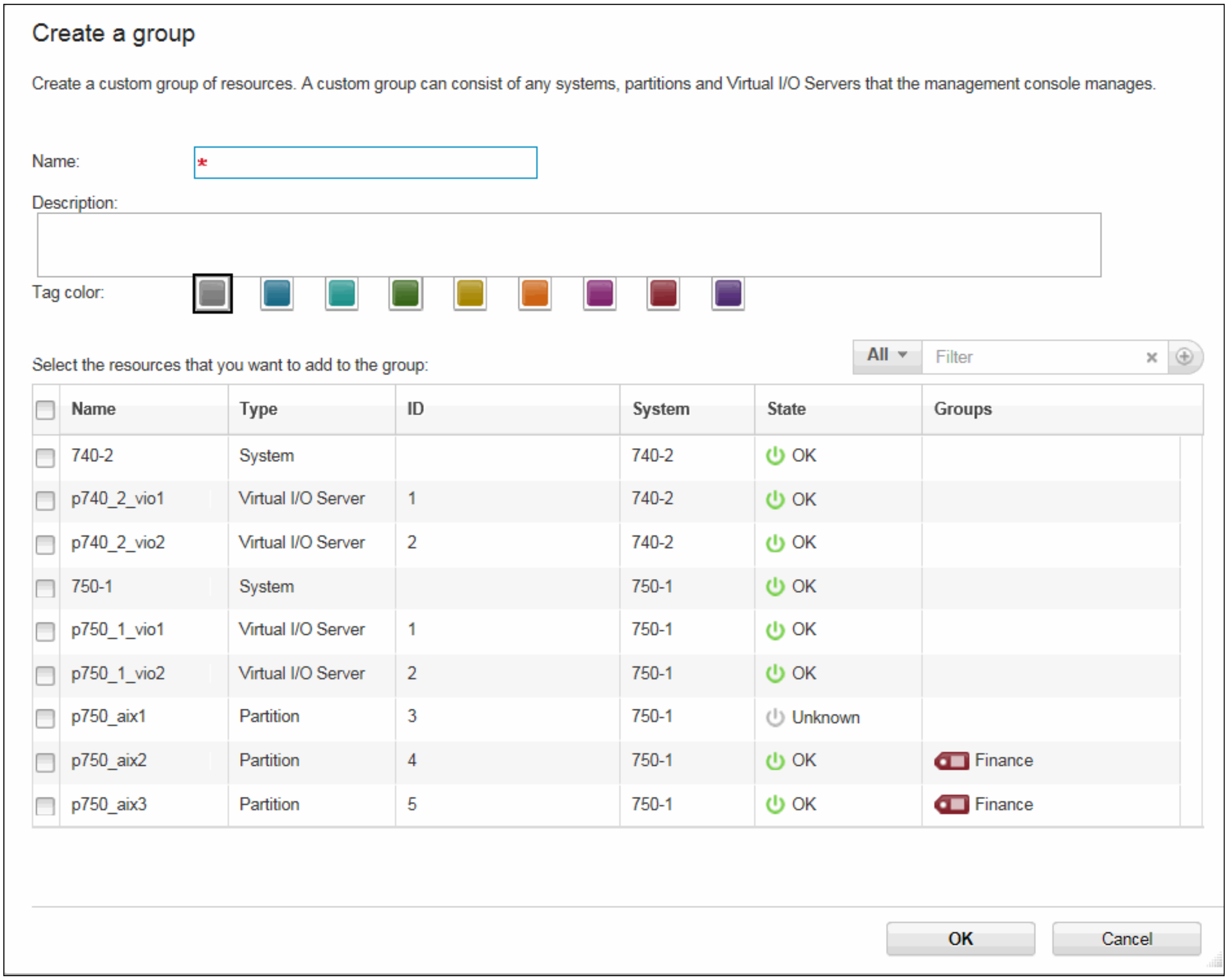
Figure 5-51 All Groups overview

From here you can create, edit, or delete a group:

- Click **Create a Group** to open the Create a group window (Figure 5-52 on page 339).

  Here you can specify a name and meaningful description for the new group, select a color for and the resources for the new group. After making your selections, click **OK**. The group will be created and you see an overview with your new group appended.

- If you click **Edit**, a similar window opens where you can change the name, the description, the color, and the selection of resources.
- If you click **Delete**, the group will be deleted.



Create a group

Create a custom group of resources. A custom group can consist of any systems, partitions and Virtual I/O Servers that the management console manages.

Name: *

Description:

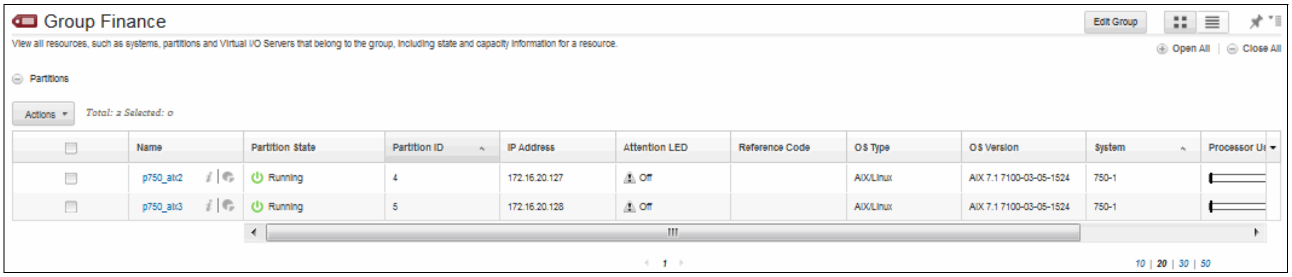
Tag color:

Select the resources that you want to add to the group:

□	Name	Type	ID	System	State	Groups
□	740-2	System		740-2	OK	
□	p740_2_vio1	Virtual I/O Server	1	740-2	OK	
□	p740_2_vio2	Virtual I/O Server	2	740-2	OK	
□	750-1	System		750-1	OK	
□	p750_1_vio1	Virtual I/O Server	1	750-1	OK	
□	p750_1_vio2	Virtual I/O Server	2	750-1	OK	
□	p750_aix1	Partition	3	750-1	Unknown	
□	p750_aix2	Partition	4	750-1	OK	Finance
□	p750_aix3	Partition	5	750-1	OK	Finance

Figure 5-52 Create a group window

If you select the name of your group, for example the Finance group as shown in Figure 5-51 on page 338, a list of all resources belonging to the group is displayed (Figure 5-53). You can also see the status, and some configuration and performance details of the resource group members.



Group Finance

View all resources, such as systems, partitions and Virtual I/O Servers that belong to the group, including state and capacity information for a resource.

Total: 2 Selected: 0

□	Name	Partition State	Partition ID	IP Address	Attention LED	Reference Code	OS Type	OS Version	System	Processor U
□	p750_aix2	Running	4	172.16.20.127	Off		AIX/Linux	AIX 7.1 7100-03-05-1524	750-1	
□	p750_aix3	Running	5	172.16.20.128	Off		AIX/Linux	AIX 7.1 7100-03-05-1524	750-1	

Figure 5-53 Resource overview of the Finance group example

From here, you can manage the members of the resource group by selecting a resource group member, and then clicking **Actions** and selecting an actions task.

5.5 Systems Management for Servers

Systems Management displays tasks to manage servers, logical partitions, and frames. Use these tasks to set up, configure, view current status, troubleshoot, and apply solutions for servers.

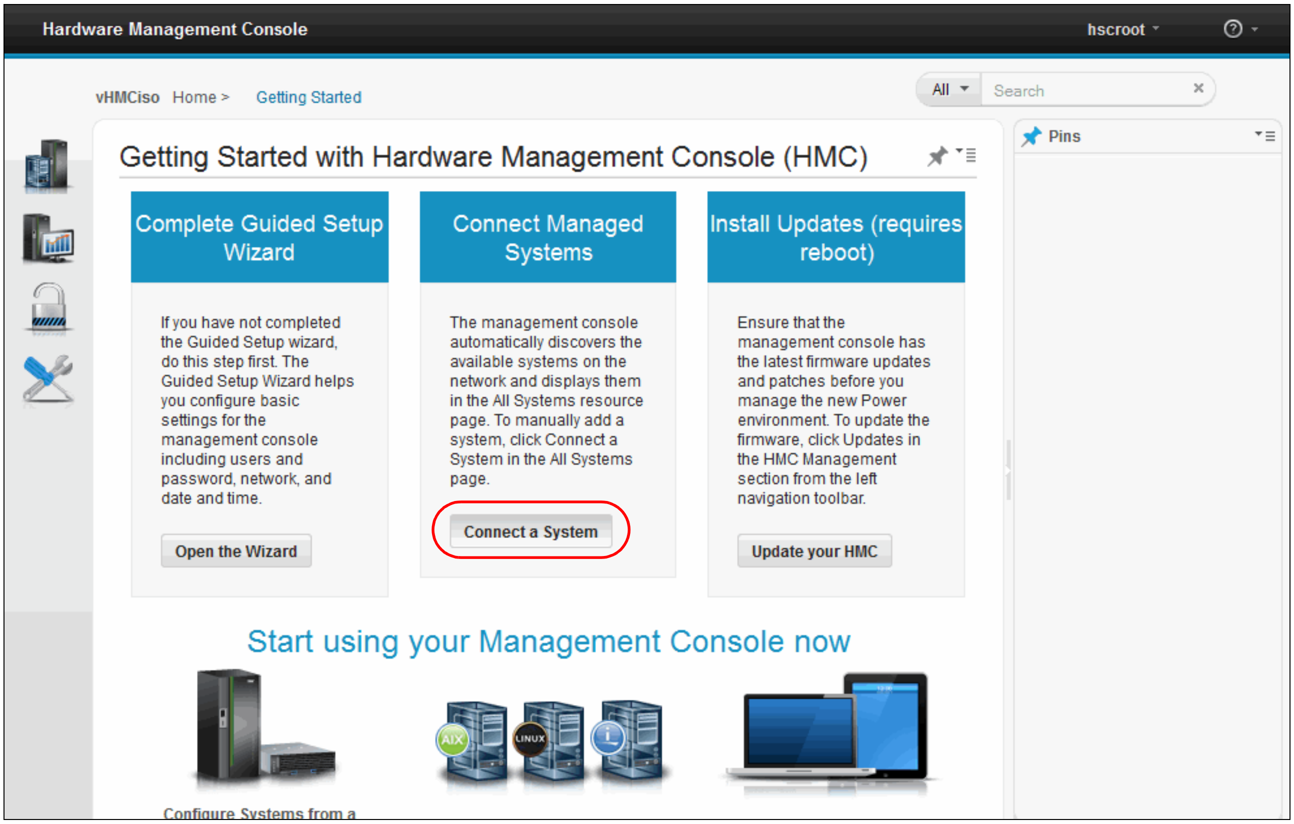
These tasks are listed when a managed system is selected. The tasks listed in the menu pod change as selections are made in the work area.

5.5.1 Add a server

To add servers, complete the following steps:

> **Before you begin:** You must get the IP address or host name of the service processor on the managed system. The task of connecting managed systems is explained in 3.3, “HMC Install Wizard” on page 223.

1. You have two options to add a new managed system to the HMC:
   – From the initial Getting Started panel (Figure 5-54), click **Connect a System**.


Hardware Management Console
hscroot
vHMCiso Home > Getting Started
All
Search
Pins
Getting Started with Hardware Management Console (HMC)
Complete Guided Setup Wizard
Connect Managed Systems
Install Updates (requires reboot)
Open the Wizard
Connect a System
Update your HMC
Start using your Management Console now
AIX
LINUX
Configure Systems from a

If you have not completed the Guided Setup wizard, do this step first. The Guided Setup Wizard helps you configure basic settings for the management console including users and password, network, and date and time.

The management console automatically discovers the available systems on the network and displays them in the All Systems resource page. To manually add a system, click Connect a System in the All Systems page.

Ensure that the management console has the latest firmware updates and patches before you manage the new Power environment. To update the firmware, click Updates in the HMC Management section from the left navigation toolbar.

Figure 5-54 Connect a System

– From the Resources/All Systems view (Figure 5-55), select **Resources** → **Servers**, and then click **Connect Systems**.

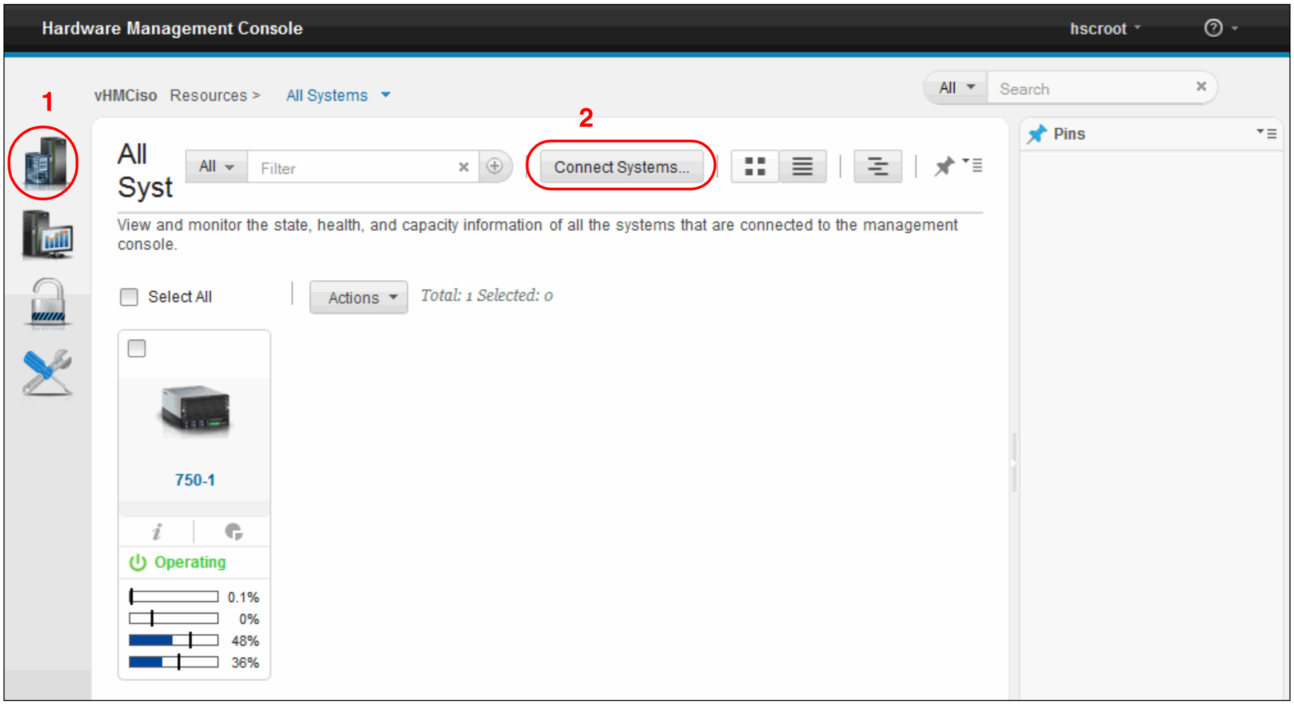
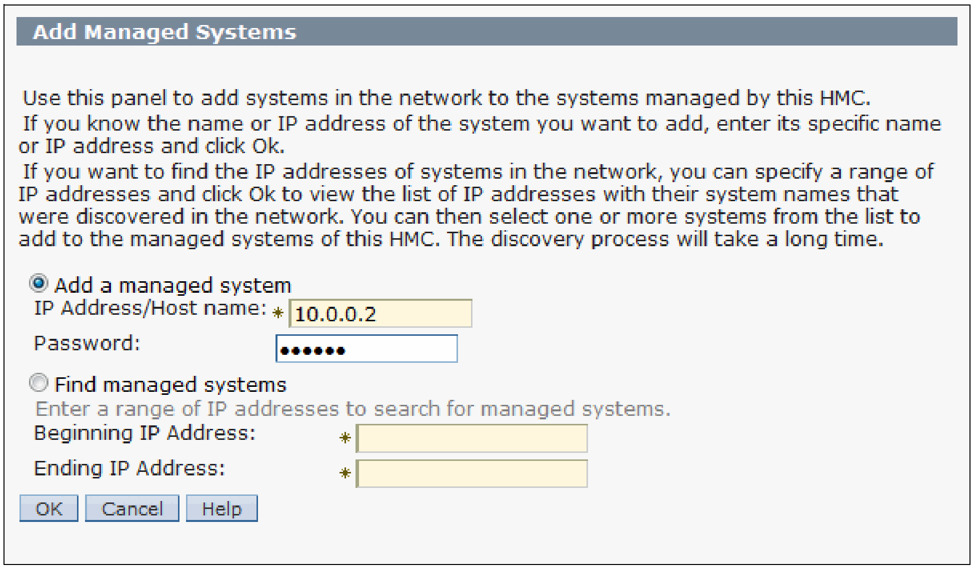

Hardware Management Console
hscroot
1
2
vHMCiso Resources > All Systems
All
Search
Pins
All Syst
All
Filter
Connect Systems...
View and monitor the state, health, and capacity information of all the systems that are connected to the management console.
Select All
Actions
Total: 1 Selected: 0
750-1
Operating
0.1%
0%
48%
36%

Figure 5-55 Selecting Connect Systems

The Add Managed System panel opens (Figure 5-56). Specify the IP address of the target managed system, and its HMC password, and then click **OK**.


Add Managed Systems

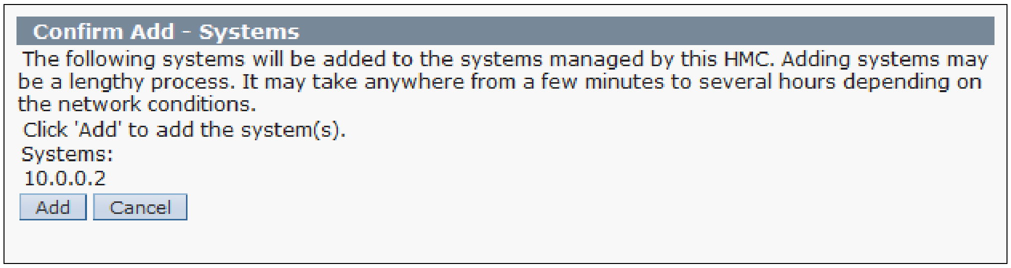
Use this panel to add systems in the network to the systems managed by this HMC.
If you know the name or IP address of the system you want to add, enter its specific name or IP address and click Ok.
If you want to find the IP addresses of systems in the network, you can specify a range of IP addresses and click Ok to view the list of IP addresses with their system names that were discovered in the network. You can then select one or more systems from the list to add to the managed systems of this HMC. The discovery process will take a long time.

● Add a managed system
IP Address/Host name: * 10.0.0.2
Password: ••••••

○ Find managed systems
Enter a range of IP addresses to search for managed systems.
Beginning IP Address: *
Ending IP Address: *

Figure 5-56 Add systems

2. In the Confirm Add panel (Figure 5-57), click **Add**.



Confirm Add - Systems

The following systems will be added to the systems managed by this HMC. Adding systems may be a lengthy process. It may take anywhere from a few minutes to several hours depending on the network conditions.

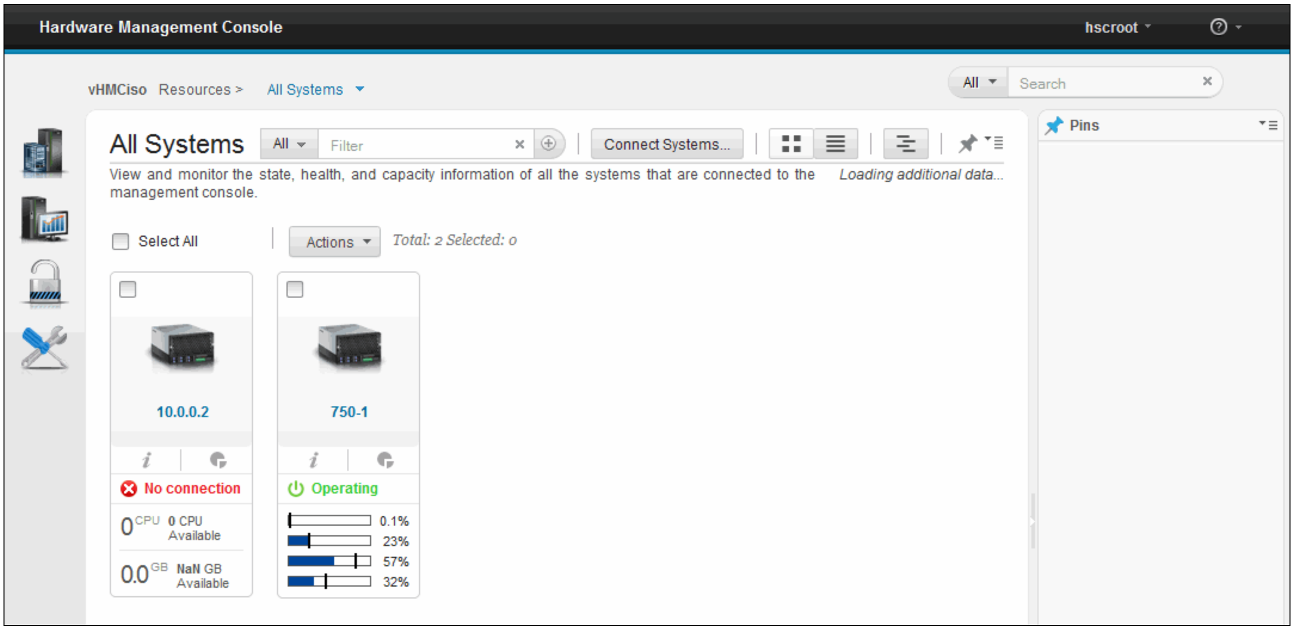
Click 'Add' to add the system(s).

Systems:

10.0.0.2

Figure 5-57 Confirm add systems

After several seconds, the selected system shows a status of `No connection` (Figure 5-58).



All Systems

View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

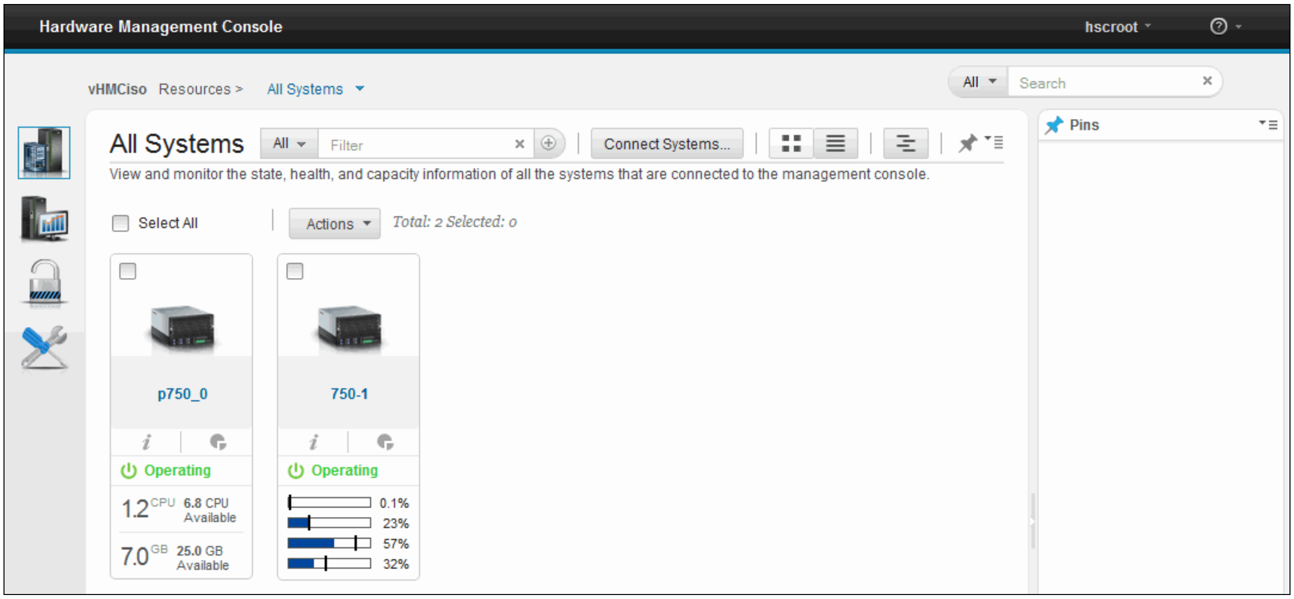
Loading additional data...

Total: 2 Selected: 0

10.0.0.2	750-1
No connection	Operating
0 CPU 0 CPU Available	0.1%
0.0 GB NaN GB Available	23%
	57%
	32%

Figure 5-58 Showing the No connection state

Finally, the status changes to `Operating` (Figure 5-59).



View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

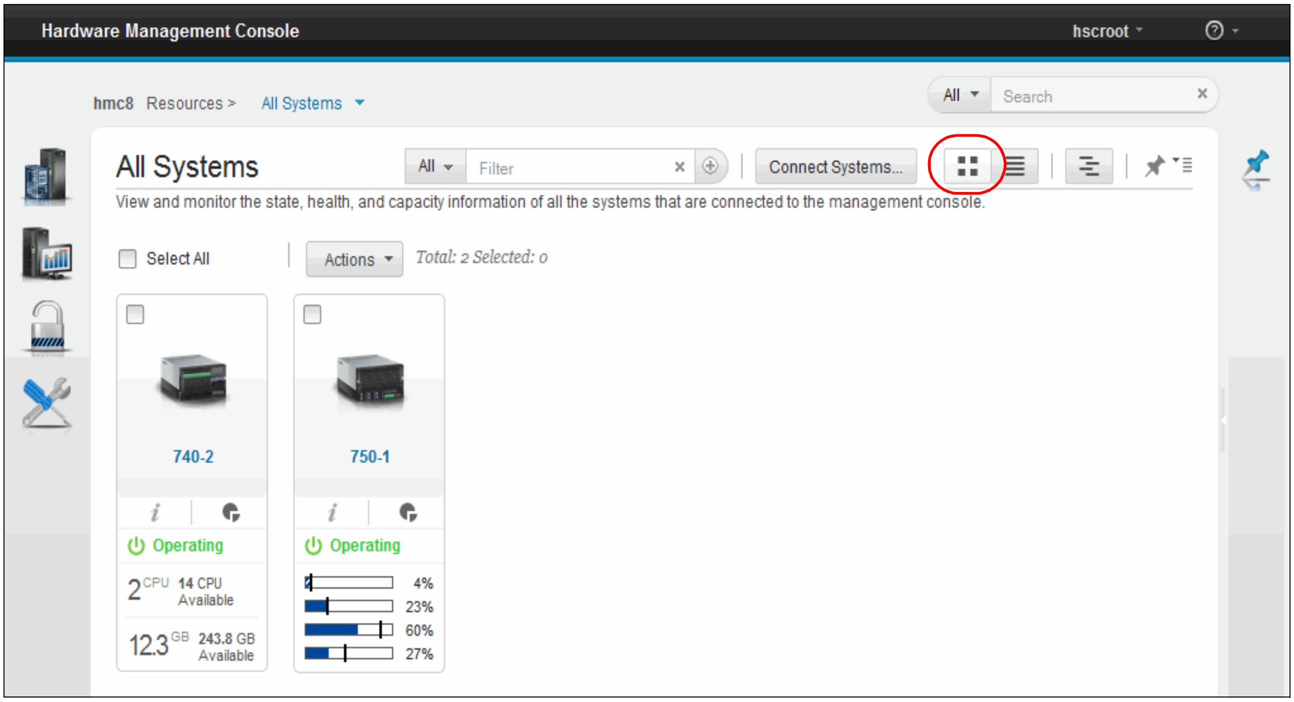
Figure 5-59 New system added

5.5.2 The server management panel

After the initial setup and configuration steps, when you log in to the HMC, the server management panel (Resources/All Systems) opens (Figure 5-60).

The server management panel offers various views: Gallery, Table, and Relational.

- The default *Gallery* view is shown in Figure 5-60.



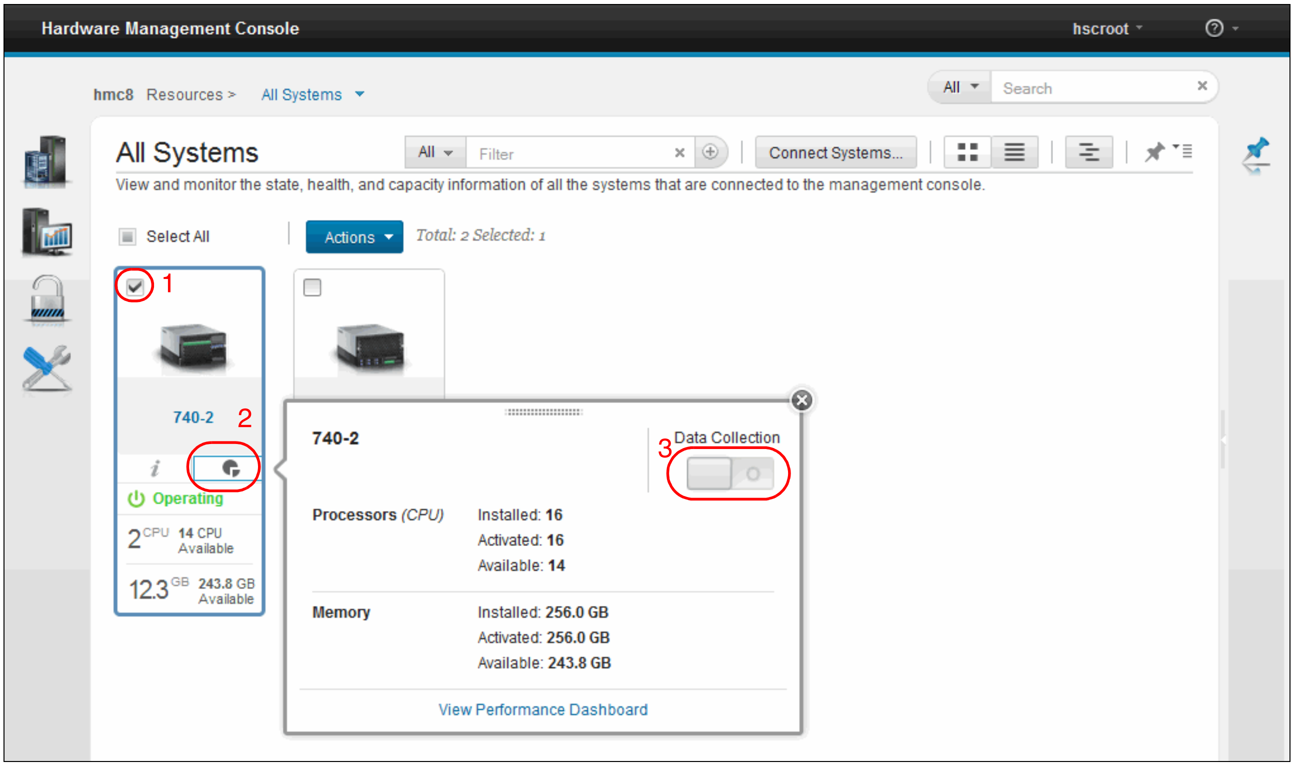
View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

Figure 5-60 Gallery view

The Gallery view shows the servers with information, such as these examples:

– Server *740-2* with the number of CPUs and the amount of memory used and available.
– Server *750-1* with:
  - Processor usage and peaks
  - Memory allocated
  - Network I/O usage
  - Storage I/O usage

To view the performance information, activate the data collection (Figure 5-61) by clicking the server, the **pie chart** icon, and finally slide the **Data Collection** button.



Hardware Management Console hscroot

hmc8 Resources > All Systems

All Systems

View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

☐ Select All | Actions | *Total: 2 Selected: 1*

☑ 1

740-2 2

Operating

2 CPU 14 CPU Available

12.3 GB 243.8 GB Available

740-2

3 Data Collection

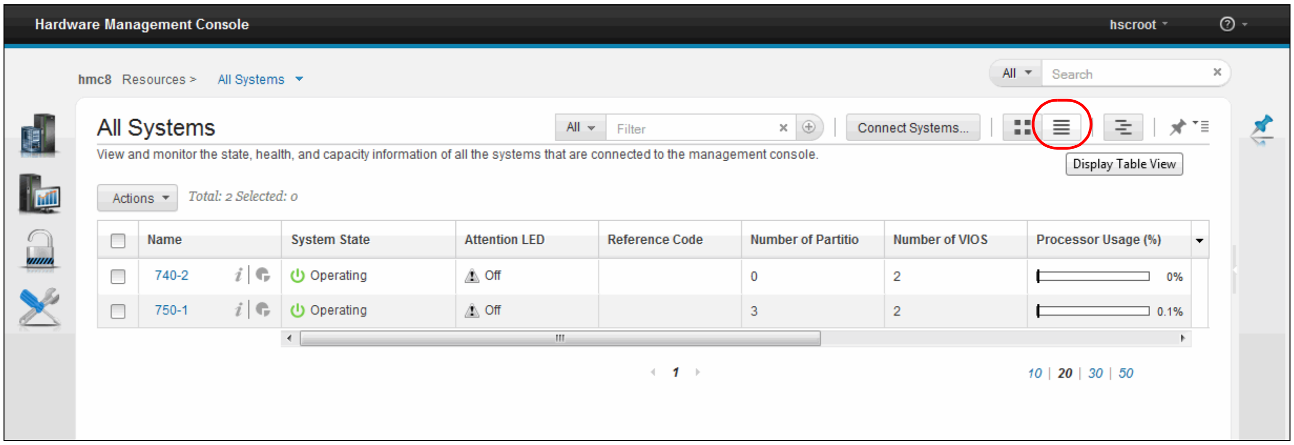
Processors *(CPU)* Installed: **16**
Activated: **16**
Available: **14**

Memory Installed: **256.0 GB**
Activated: **256.0 GB**
Available: **243.8 GB**

View Performance Dashboard

Figure 5-61 Data collection

► The *Table* view is shown in Figure 5-62.



Hardware Management Console hscroot

hmc8 Resources > All Systems

All Systems

View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

Display Table View

Actions | *Total: 2 Selected: 0*

☐	Name	System State	Attention LED	Reference Code	Number of Partitio	Number of VIOS	Processor Usage (%)
☐	740-2	Operating	Off		0	2	0%
☐	750-1	Operating	Off		3	2	0.1%

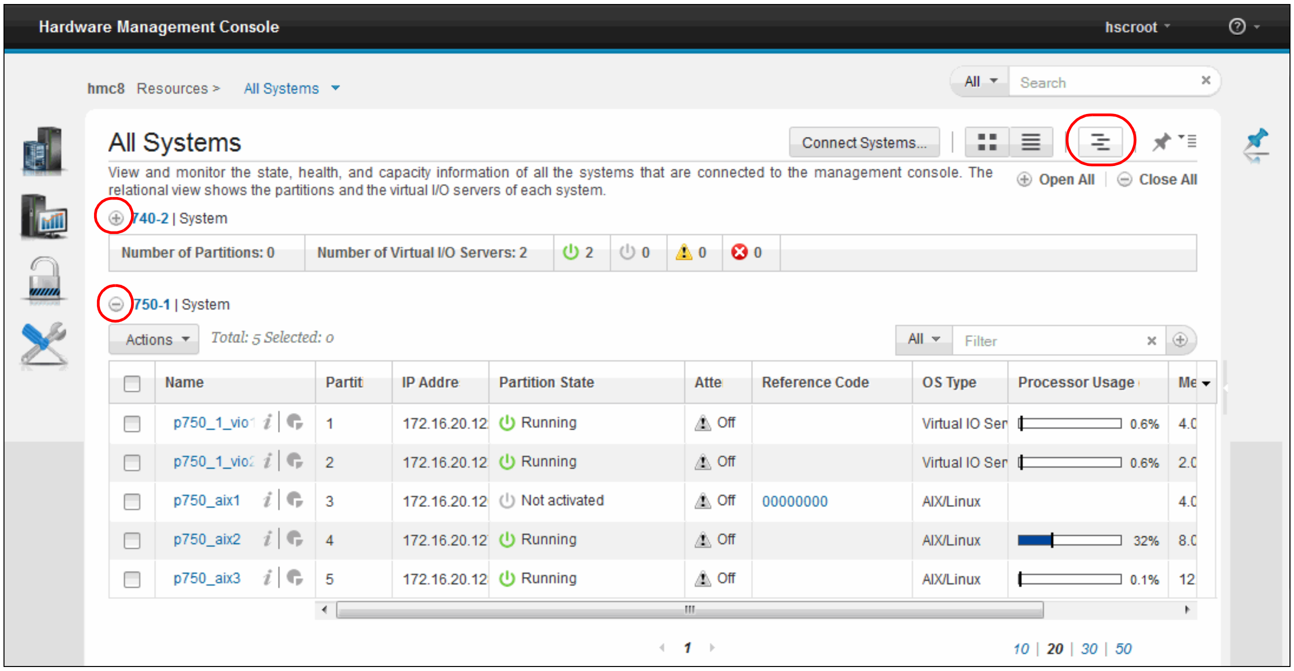
‹ 1 › 10 | 20 | 30 | 50

Figure 5-62 Table view

Move the bar to the right to see more of the view. The Table view provides the following information for each server:

- System name
- System State
- Attention LED
- Reference code
- Number of partitions
- Number of VIOS
- Processor Usage
- Memory Usage
- Network I/O Usage
- Storage I/O Usage

- The *Relational* view is shown in Figure 5-63.



All Systems

View and monitor the state, health, and capacity information of all the systems that are connected to the management console. The relational view shows the partitions and the virtual I/O servers of each system.

740-2 | System

Number of Partitions: 0	Number of Virtual I/O Servers: 2	2	0	⚠ 0	✖ 0

750-1 | System

Total: 5 Selected: 0

□	Name	Partit	IP Addre	Partition State	Atte	Reference Code	OS Type	Processor Usage	Me
□	p750_1_vio1	1	172.16.20.12	Running	⚠ Off		Virtual IO Ser	0.6%	4.0
□	p750_1_vio2	2	172.16.20.12	Running	⚠ Off		Virtual IO Ser	0.6%	2.0
□	p750_aix1	3	172.16.20.12	Not activated	⚠ Off	00000000	AIX/Linux		4.0
□	p750_aix2	4	172.16.20.12	Running	⚠ Off		AIX/Linux	32%	8.0
□	p750_aix3	5	172.16.20.12	Running	⚠ Off		AIX/Linux	0.1%	12

1

10 | 20 | 30 | 50

Figure 5-63 Relational View

The Relational view presents one pane for each server. In this example, server *740-2* is collapsed, showing only basic server status. Server *750-1* is expanded to show more information. The detailed view is scaled and provides the following information for each partition:

- Name
- ID
- IP address
- State
- Reference code
- Operating System type (VIOS, AIX or Linux, and IBM i)
- Processor Usage
- Memory Allocated

5.5.3 Server management

To find the management server tasks, click one of the servers in the All Systems panel (Figure 5-64). This example uses **750-1**.

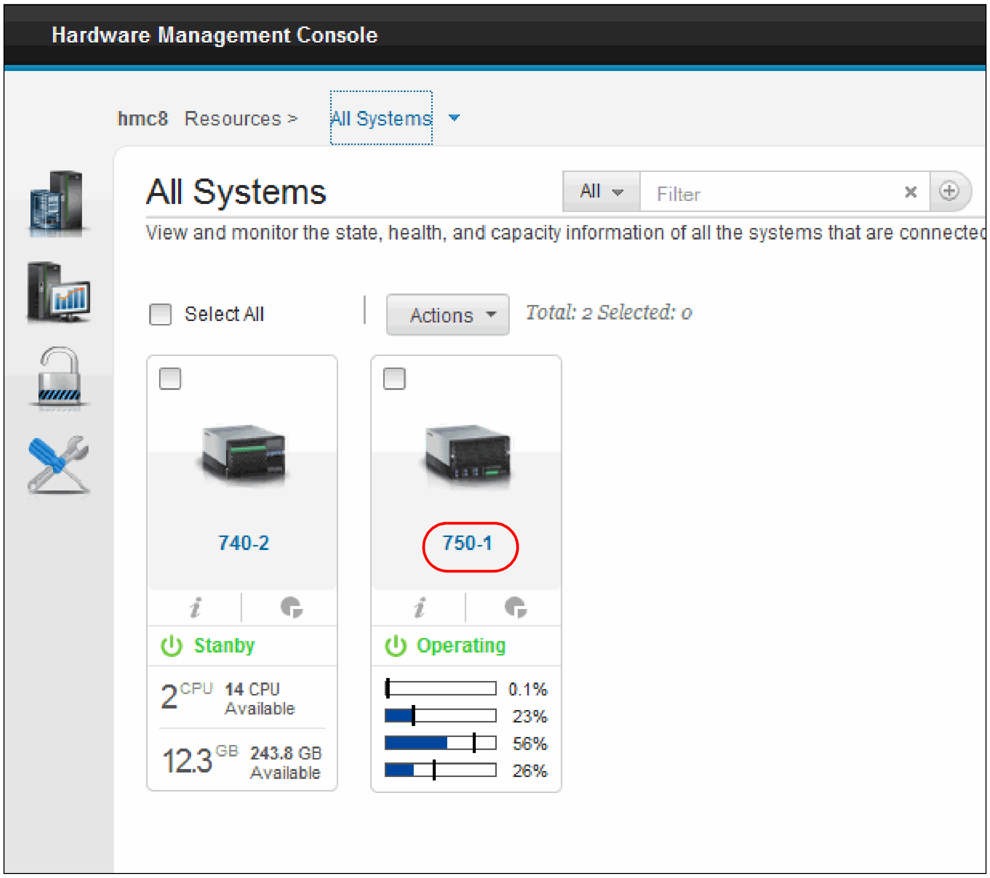
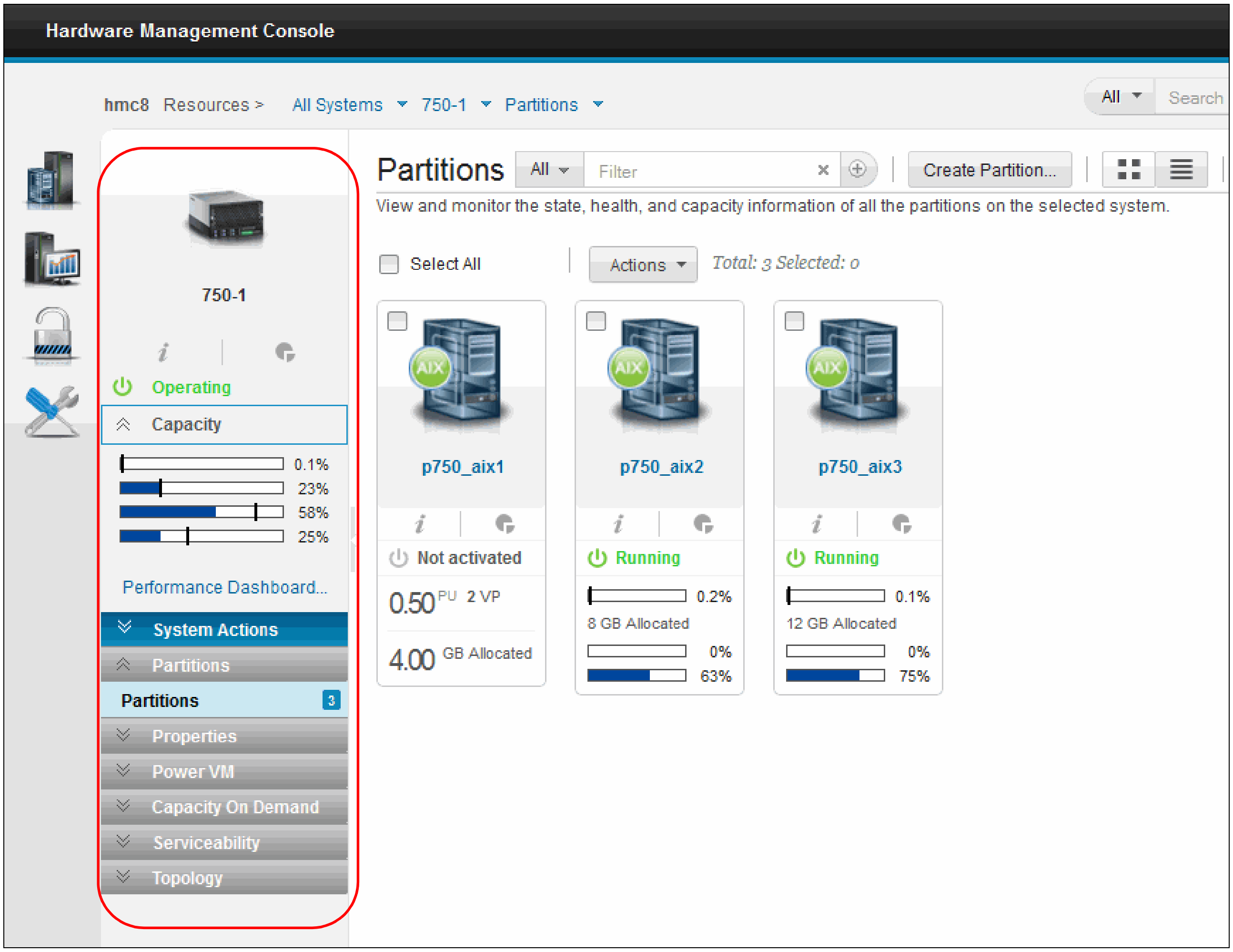

Hardware Management Console
hmc8 Resources > All Systems
All Systems
All
Filter
View and monitor the state, health, and capacity information of all the systems that are connected
Select All
Actions
Total: 2 Selected: 0
740-2
Stanby
2 CPU 14 CPU Available
12.3 GB 243.8 GB Available
750-1
Operating
0.1%
23%
56%
26%

Figure 5-64 Choose a server to manage

The server management panel opens (Figure 5-65). The center area is dedicated to the partitions, which are further described in 5.6, “Partition management” on page 370. This view also shows a new pane, highlighted in the figure, for server management tasks.



View and monitor the state, health, and capacity information of all the partitions on the selected system.

Figure 5-65 Management tasks

The server pane offers the following management tasks, which are described in the next sections:

- Capacity
- System Actions
- Partitions
- Properties
- Power VM
- Capacity On Demand
- Serviceability
- Topology

Capacity

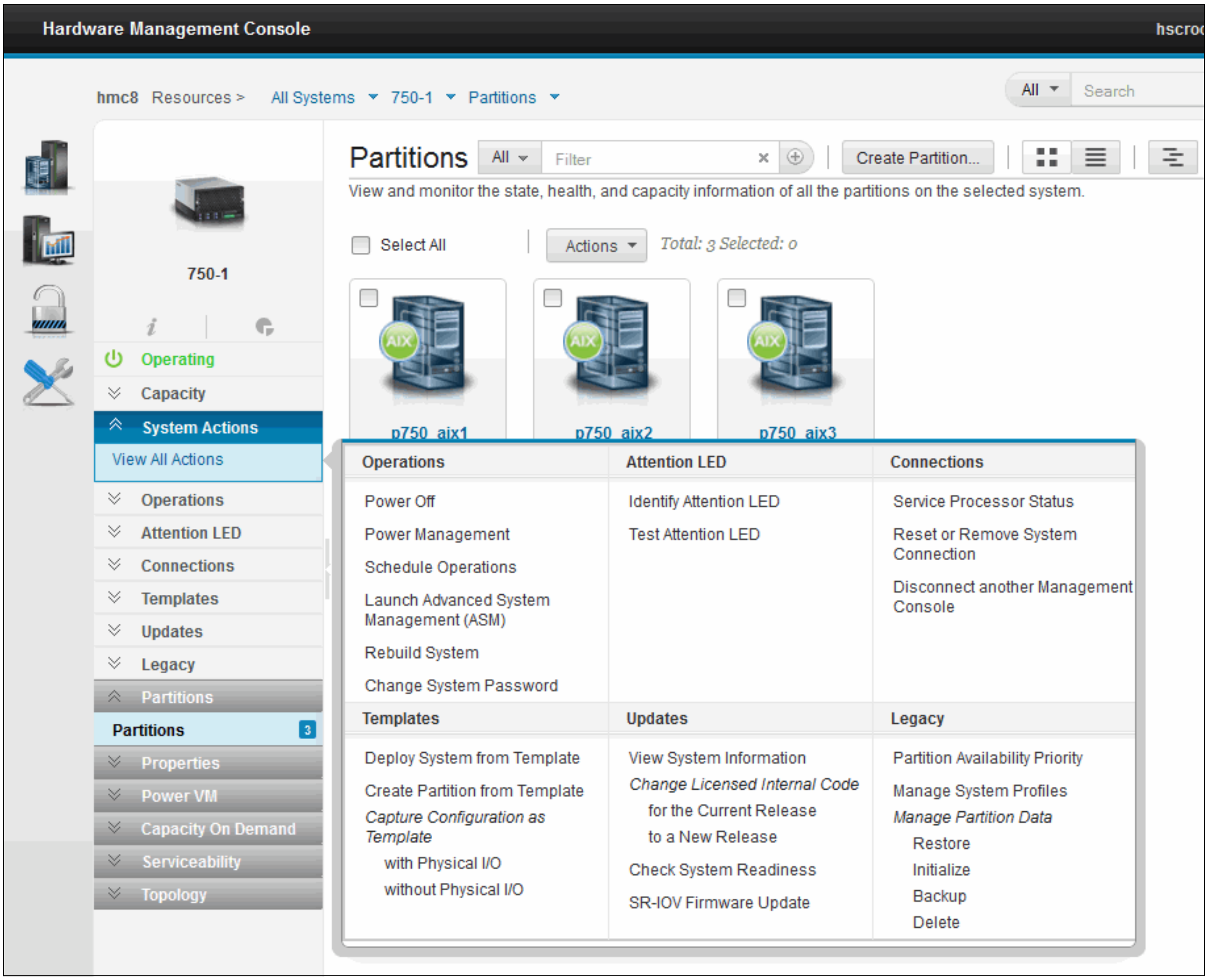
The Capacity task, expanded as in Figure 5-65, indicates the server load. For more information about performance details, click **Performance Dashboard**. This task is further detailed in Chapter 7, “Performance and capacity monitoring” on page 511.

System Actions

Click the **System Actions** task to reveal the following task tabs:

- View All Actions
- Operations
- Attention LED
- Connections
- Templates
- Updates
- Legacy

Click **View All Actions** to see a list of available tasks (Figure 5-66).



Operations
- Power Off
- Power Management
- Schedule Operations
- Launch Advanced System Management (ASM)
- Rebuild System
- Change System Password

Attention LED
- Identify Attention LED
- Test Attention LED

Connections
- Service Processor Status
- Reset or Remove System Connection
- Disconnect another Management Console

Templates
- Deploy System from Template
- Create Partition from Template
- *Capture Configuration as Template*
  - with Physical I/O
  - without Physical I/O

Updates
- View System Information
- *Change Licensed Internal Code*
  - for the Current Release
  - to a New Release
- Check System Readiness
- SR-IOV Firmware Update

Legacy
- Partition Availability Priority
- Manage System Profiles
- *Manage Partition Data*
  - Restore
  - Initialize
  - Backup
  - Delete

Figure 5-66 System actions

Operations

Operations tasks are for server operations, such as these tasks:

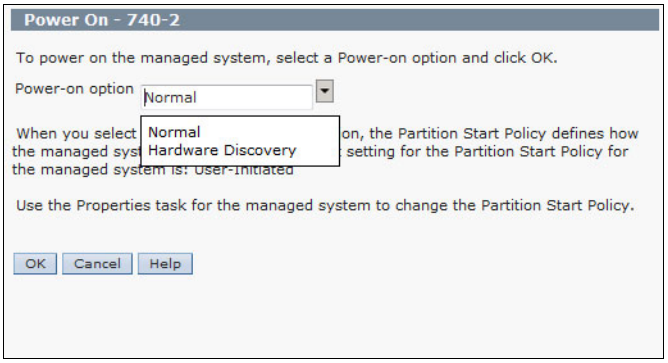
- Power on
- Power off
- Power management
- Schedule operations
- Launch Advanced System Management (ASM)
- Rebuild System
- Change System Password

These tasks are described as follows:

- Power On task

  Powers on the managed system.

  Figure 5-67 shows the Power On window.



Power On - 740-2

To power on the managed system, select a Power-on option and click OK.

Power-on option: Normal

When you select … on, the Partition Start Policy defines how the managed syst… setting for the Partition Start Policy for the managed system is: User-Initiated

Use the Properties task for the managed system to change the Partition Start Policy.

Figure 5-67 Power On task

Available options in this window are as follows:

– Normal

  Turns on the managed system with the current setting for the partition start policy to determine how to power on the managed system. You can change the partition start policy from the **Power On Parameters** tab of the **Properties** task for the managed system. The current setting can be one of the following values:

  - Auto-Start Always
  - Stop at Partition Standby
  - Auto-Start for Auto-Recovery
  - User-Initiated

– Hardware Discovery

  Turns on the managed system in a special mode, which performs the hardware discovery. After the hardware discovery process is complete, the system is in an `Operating` state with any partitions in the `power-off` state.The hardware discovery process records the hardware inventory in cache on the managed system. The collected information is then available for use when displaying data for I/O devices or when creating a system plan based on the managed system. This option is available only if the system can use the hardware discovery process to capture I/O hardware inventory for the managed system.

– System Profile

Turns on the managed system and its logical partitions based on a predefined system profile. When you select this option, you must select the partition profile that you want the HMC to use to activate logical partitions on the managed system.

> **System profiles:** If the HMC does not have any system profiles, the **System Profile** option is not shown. System profiles are explained in "Legacy" on page 356.

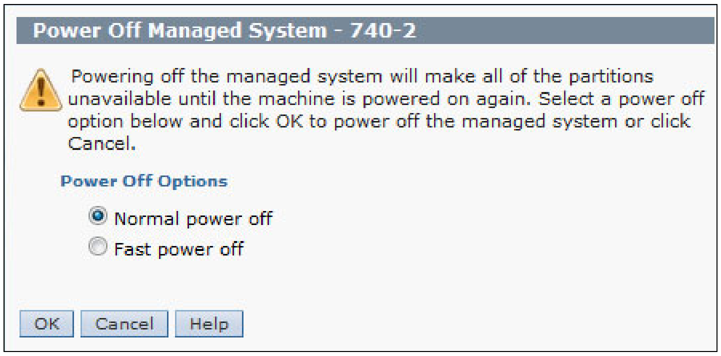
- Power Off task

  Shuts down the managed system. Turning off the managed system makes all partitions unavailable until the system is turned on again.

  Before you turn off the managed system, ensure that all logical partitions are shut down and that their states have changed from `Running` to `Not Activated`.

  If you do not shut down all logical partitions on the managed system before you turn off the managed system, the managed system shuts down each logical partition before the managed system itself turns off. This process can cause a substantial delay in turning off the managed system, particularly if the logical partitions are not responsive. Further, the logical partitions might shut down abnormally, which can result in data loss and further delays when you activate the logical partitions again.

  Figure 5-68 shows the Power Off Managed System window.



Power Off Managed System - 740-2

Powering off the managed system will make all of the partitions unavailable until the machine is powered on again. Select a power off option below and click OK to power off the managed system or click Cancel.

Power Off Options

● Normal power off
○ Fast power off

Figure 5-68 Power OFF task

  Available options in this window are as follows:

  – Normal power off

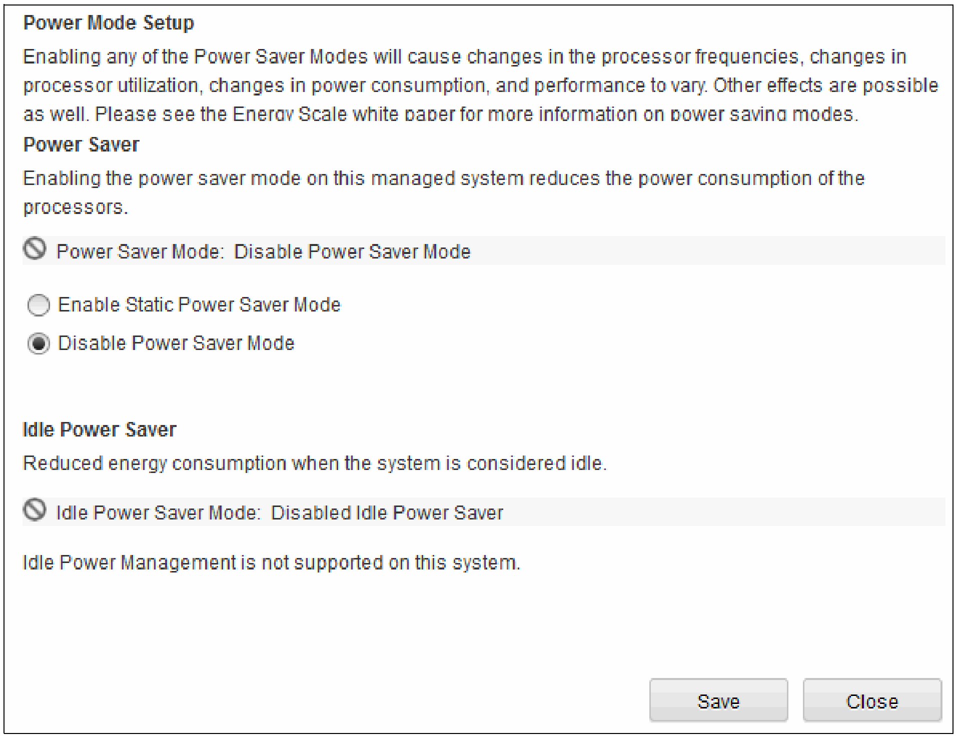
  The system ends all active jobs in a controlled manner. During that time, programs running in those jobs are allowed to do cleanup (end-of-job processing).

  – Fast power off

  The system ends all active jobs immediately. The programs running in those jobs are not allowed to do any cleanup. Some applications, such as web servers that are providing information, might not have a problem with fast power off. Other applications, such as databases with cached information, might lose data if the application cannot do cleanup before the application ends.

- Power Management task

  Use this task to change the power saver mode of the managed system. You can reduce power consumption by enabling the power saver mode. You can check the current power saver mode and change it. Figure 5-69 shows the Power Mode Setup panel.



Power Mode Setup

Enabling any of the Power Saver Modes will cause changes in the processor frequencies, changes in processor utilization, changes in power consumption, and performance to vary. Other effects are possible as well. Please see the Energy Scale white paper for more information on power saving modes.

Power Saver

Enabling the power saver mode on this managed system reduces the power consumption of the processors.

Power Saver Mode: Disable Power Saver Mode

○ Enable Static Power Saver Mode
● Disable Power Saver Mode

Idle Power Saver

Reduced energy consumption when the system is considered idle.

Idle Power Saver Mode: Disabled Idle Power Saver

Idle Power Management is not supported on this system.

Figure 5-69 Power Mode Setup

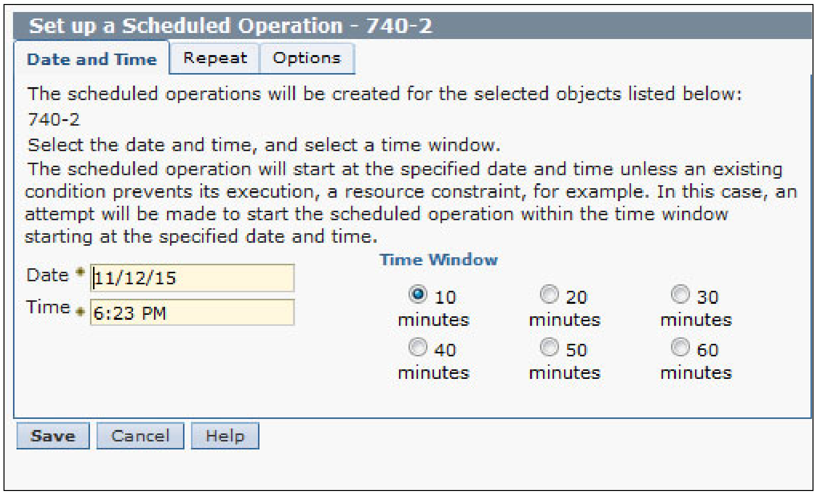
- Schedule Operations task

  Use this task to create a schedule for certain operations to be performed on the managed system without operator assistance. Scheduled operations are helpful when automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times. For example, you can schedule power on or off operations for a managed system.

  You can choose the following tasks:

  - Activate on a System Profile
  - Backup Profile Data
  - Power Off Managed System
  - Power On Managed System
  - Manage Utility CoD processors
  - Manage Utility CoD processor minute usage limit
  - Modify a Shared Processor Pool
  - Move a partition to a different pool
  - Change the power saver mode on a managed system

Figure 5-70 shows the Set up a Scheduled Operation window, where you set up the task.



The scheduled operations will be created for the selected objects listed below:
740-2
Select the date and time, and select a time window.
The scheduled operation will start at the specified date and time unless an existing condition prevents its execution, a resource constraint, for example. In this case, an attempt will be made to start the scheduled operation within the time window starting at the specified date and time.

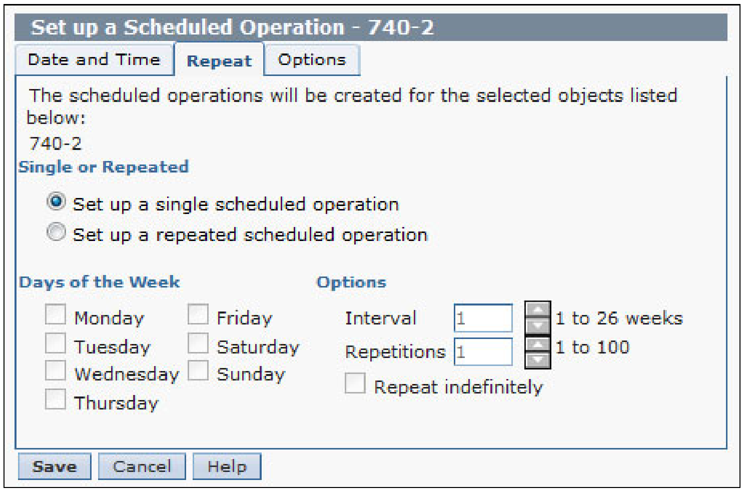
Date * 11/12/15
Time * 6:23 PM

Time Window

● 10 minutes ○ 20 minutes ○ 30 minutes
○ 40 minutes ○ 50 minutes ○ 60 minutes

Figure 5-70 Set up a Scheduled Operation task: Date and TIme

Figure 5-71 shows how to set up a scheduled operation to repeat.



The scheduled operations will be created for the selected objects listed below:
740-2

Single or Repeated

● Set up a single scheduled operation
○ Set up a repeated scheduled operation

Days of the Week

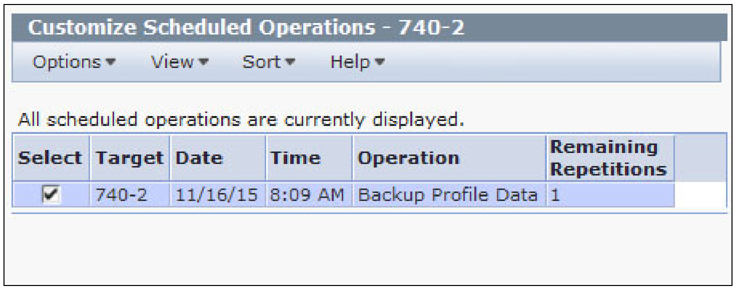
□ Monday □ Friday
□ Tuesday □ Saturday
□ Wednesday □ Sunday
□ Thursday

Options

Interval 1 1 to 26 weeks
Repetitions 1 1 to 100
□ Repeat indefinitely

Figure 5-71 Set up a Scheduled Operation task: Repeat

Figure 5-72 shows the Customize Scheduled Operations window, which displays the defined tasks.



All scheduled operations are currently displayed.

Select	Target	Date	Time	Operation	Remaining Repetitions
☑	740-2	11/16/15	8:09 AM	Backup Profile Data	1

Figure 5-72 Customize Scheduled Operations task

Power saver mode: Enabling the power saver mode on a managed system might affect the accuracy of any performance monitoring tools that are running on the managed system.

- Launch Advanced System Management (ASM) task

  If configured to do so, the HMC connects directly to the Advanced System Management (ASM) interface for a selected system from this task. This task is explained in 6.10, “Advanced System Management Interface” on page 471.

- Rebuild System task

  Use this task to extract the configuration information from the managed system and to rebuild the information about the HMC. Rebuilding the managed system means that you update, or refresh, the information about the HMC, about the managed system. Rebuilding the managed system can be helpful when the state of the managed system is `Incomplete`. The Incomplete state means that the HMC lost communication with the managed server and no longer has complete information. Rebuilding the managed system differs from simply refreshing the HMC window. When the managed system is rebuilt, the HMC extracts the information from the managed system.

  Rebuild can take several minutes: You cannot start other tasks while the HMC rebuilds the managed system. This process can take several minutes.

- Change System Password task

  Use this task to change the HMC access password on the selected managed system. After the password is changed, you must update the HMC access password for all other HMCs from which you want to access this managed system.

Attention LED

Use this task to view Attention LED information for the system, light-specific LEDs to identify a system component, and test all LEDs on a managed system.

The following options are available:

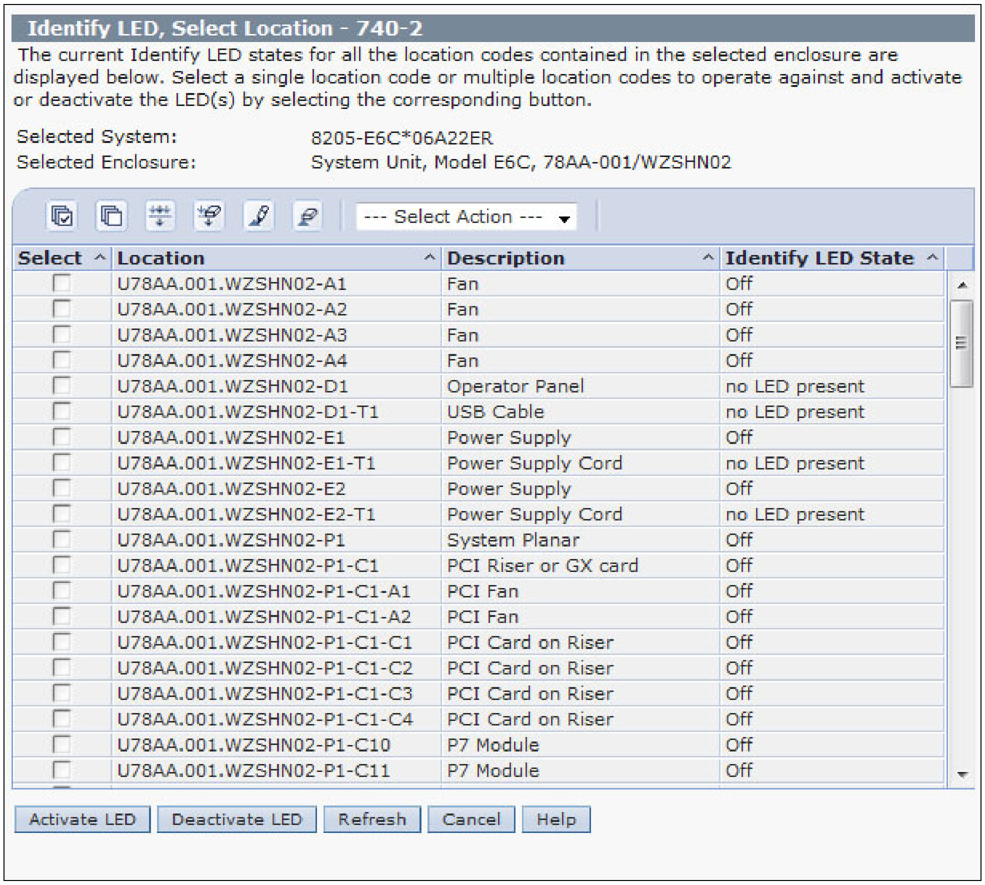
- Deactivate Attention LED

  Deactivates all system Attention LEDs and logical partition LEDs.

- Identify LED

  Displays the current Identify LED states for all the location codes that are contained in the selected enclosure.

Figure 5-73 shows the Identify LED window. From this task, you can select a single location code or multiple location codes to operate against and activate or deactivate the LEDs by selecting the corresponding box.



Identify LED, Select Location - 740-2

The current Identify LED states for all the location codes contained in the selected enclosure are displayed below. Select a single location code or multiple location codes to operate against and activate or deactivate the LED(s) by selecting the corresponding button.

Selected System: 8205-E6C*06A22ER
Selected Enclosure: System Unit, Model E6C, 78AA-001/WZSHN02

Select	Location	Description	Identify LED State
□	U78AA.001.WZSHN02-A1	Fan	Off
□	U78AA.001.WZSHN02-A2	Fan	Off
□	U78AA.001.WZSHN02-A3	Fan	Off
□	U78AA.001.WZSHN02-A4	Fan	Off
□	U78AA.001.WZSHN02-D1	Operator Panel	no LED present
□	U78AA.001.WZSHN02-D1-T1	USB Cable	no LED present
□	U78AA.001.WZSHN02-E1	Power Supply	Off
□	U78AA.001.WZSHN02-E1-T1	Power Supply Cord	no LED present
□	U78AA.001.WZSHN02-E2	Power Supply	Off
□	U78AA.001.WZSHN02-E2-T1	Power Supply Cord	no LED present
□	U78AA.001.WZSHN02-P1	System Planar	Off
□	U78AA.001.WZSHN02-P1-C1	PCI Riser or GX card	Off
□	U78AA.001.WZSHN02-P1-C1-A1	PCI Fan	Off
□	U78AA.001.WZSHN02-P1-C1-A2	PCI Fan	Off
□	U78AA.001.WZSHN02-P1-C1-C1	PCI Card on Riser	Off
□	U78AA.001.WZSHN02-P1-C1-C2	PCI Card on Riser	Off
□	U78AA.001.WZSHN02-P1-C1-C3	PCI Card on Riser	Off
□	U78AA.001.WZSHN02-P1-C1-C4	PCI Card on Riser	Off
□	U78AA.001.WZSHN02-P1-C10	P7 Module	Off
□	U78AA.001.WZSHN02-P1-C11	P7 Module	Off

Figure 5-73 Identify LED task

- Test Attention LED

  Initiates an LED Lamp Test against the selected system. All LEDs are activated for several minutes.

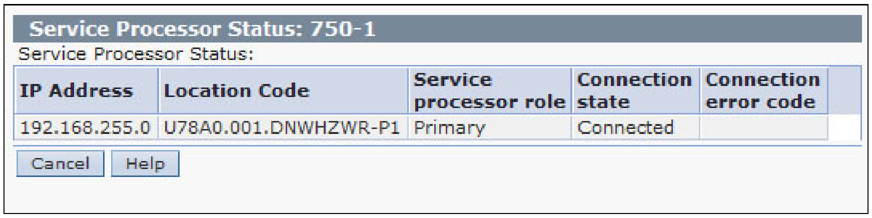
Connections

Use Connections tasks to view the HMC connection status to service processors or frames, reset those connections, connect another HMC to the selected managed system, or disconnect another managed system to the HMC.

The Connections tasks are as follows:

- Service Processor Status task

  Use this task to display the HMC connection status to the service processor of a selected managed system (Figure 5-74). If you select a frame, Service Processor Status displays the state of the connection from the HMC to side A and side B of the bulk power assembly.



Service Processor Status: 750-1

Service Processor Status:

IP Address	Location Code	Service processor role	Connection state	Connection error code
192.168.255.0	U78A0.001.DNWHZWR-P1	Primary	Connected	

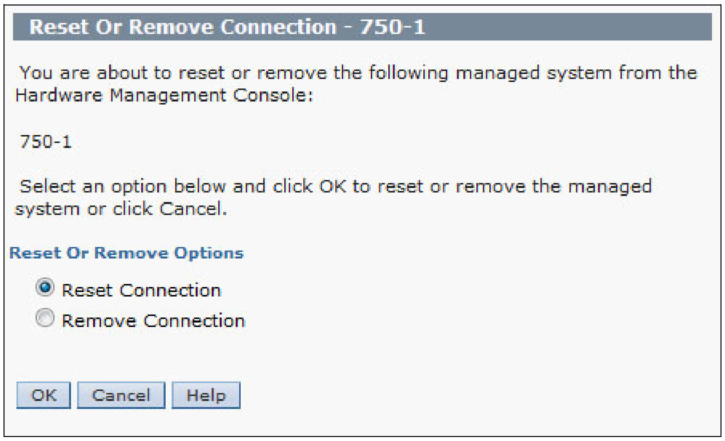
Figure 5-74 Service Processor Status task

- Reset or Remove Connections task

  Use this task to remove or reset a managed system from the contents area of the HMC, as shown in Figure 5-75.

  When you remove the connection with a managed system, the connection is broken between the HMC and the managed system. Remove the connection with the managed system if you no longer want to manage the managed system by using this HMC. Use this window to remove the connection before you physically disconnect the HMC from the managed system (or from the network).

  When you reset the connection with a managed system, the connection is broken and then reconnected. Reset the connection with the managed system if the managed system is in a `No Connection` state and you verified that the network settings are correct on both the HMC and the managed system.



Reset Or Remove Connection - 750-1

You are about to reset or remove the following managed system from the Hardware Management Console:

750-1

Select an option below and click OK to reset or remove the managed system or click Cancel.

Reset Or Remove Options

● Reset Connection

○ Remove Connection

Figure 5-75 Reset Or Remove Connection task

- Disconnect Another HMC task

  Use this task to disconnect another HMC from the selected managed system. Also, you can find which HMC locked the selected managed system. This task releases any lock that the other HMC might have on the selected managed system. After the disconnection is complete, the other HMC automatically attempts to reconnect to the managed system.

  When you use an HMC to change a managed system, the HMC locks the managed system so that no other HMC can make conflicting changes at the same time. Normally, the HMC unlocks the managed system after the change is complete. If there is an error, and the managed system remains locked, you must disconnect the HMC from the managed system to reset the lock before other HMCs can change the managed system.

Templates

Use this task to manage the system from the following templates:

- Deploy System from Template
- Create Partition from Template
- Capture Configuration as Template

This topic is described in 2.5, “System and partition templates” on page 67.

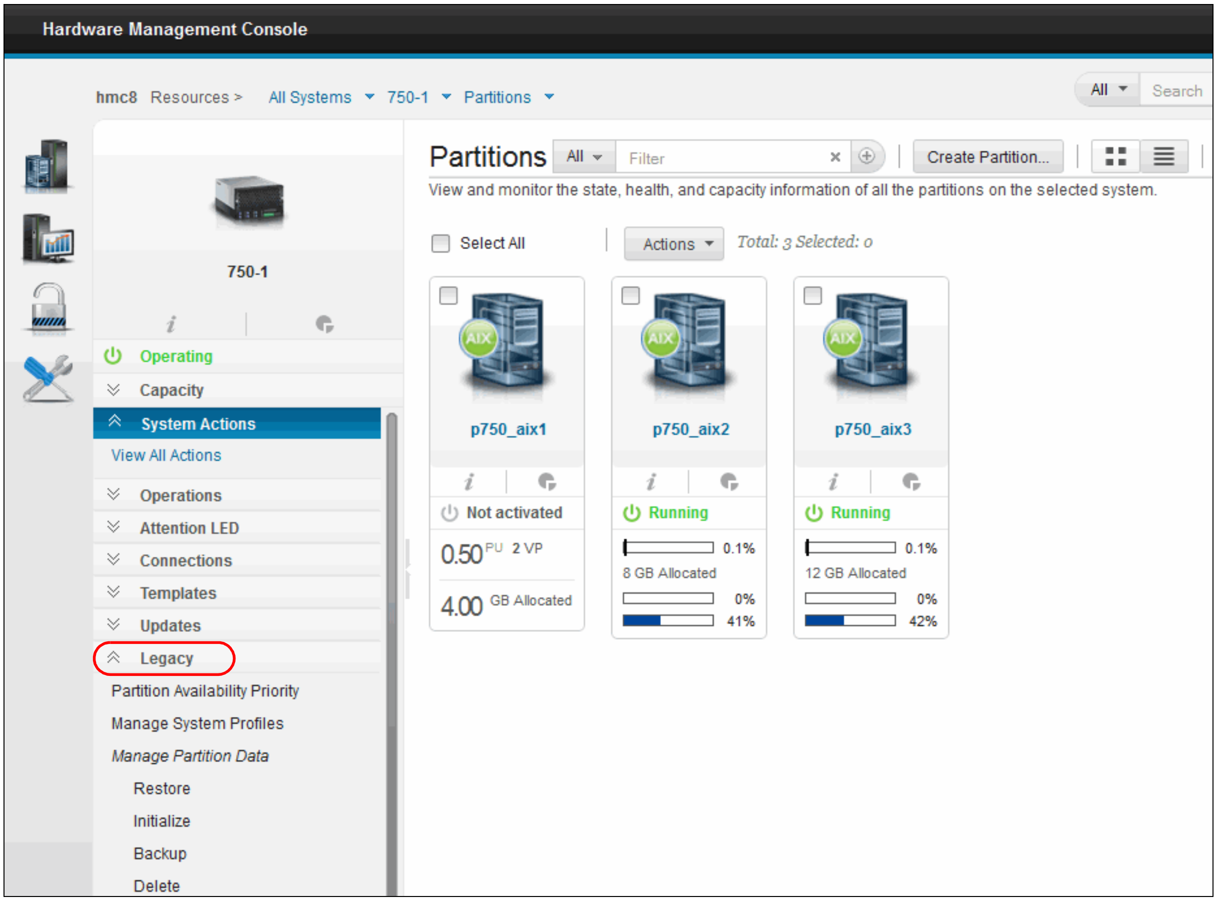
Updates

Use these tasks to do a guided update of managed system, power, or I/O Licensed Internal Code. Updates are described in 6.9.6, “Managed system firmware updates” on page 467.

Legacy

The Legacy task has the following options, which are shown in Figure 5-76 on page 357:

- Partition Availability Priority
- Manage System Profiles
- Manage Partition Data



View and monitor the state, health, and capacity information of all the partitions on the selected system.

Figure 5-76 Legacy tasks

The Legacy tasks are described in the following list:

- Partition Availability Priority task

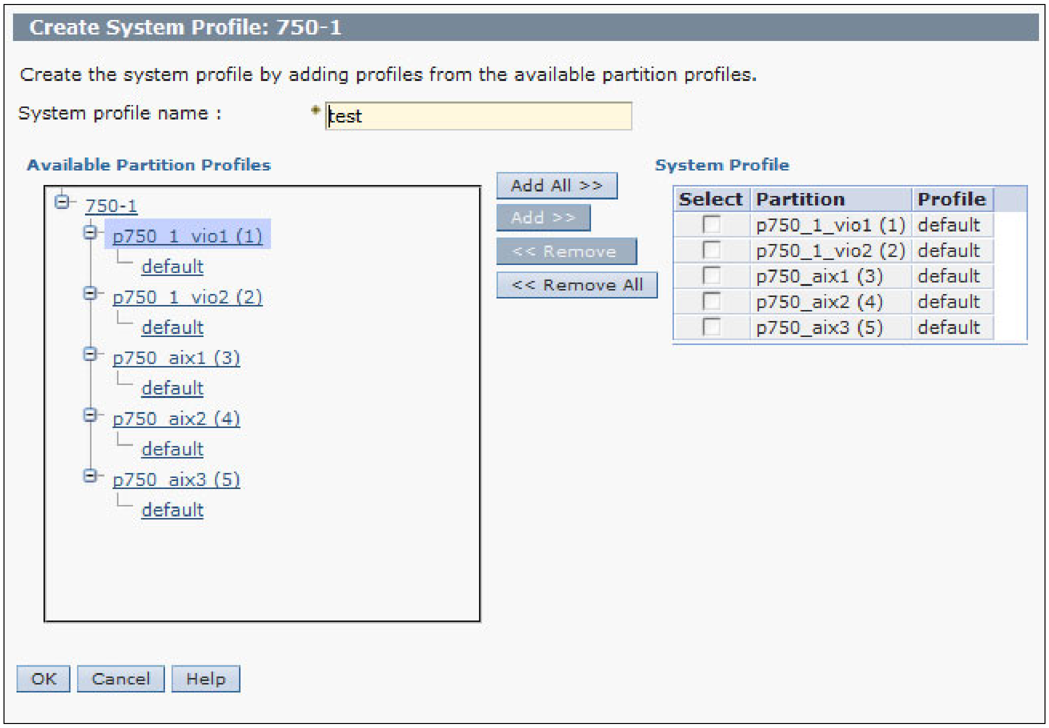
  Use this task to specify the partition availability priority of each logical partition on a managed system. The managed system uses partition availability priorities in the case of processor failure.

  If a processor fails on a logical partition, and no unassigned processors are available on the managed system, the logical partition can acquire a replacement processor from logical partitions with a lower partition-availability priority. In this way, the logical partition with the higher partition-availability priority to continue running after a processor failure.

- Manage System Profiles task

  A system profile is an ordered list of partition profiles that is used by the HMC to start the logical partitions on a managed system in a specific configuration.

  When you activate the system profile, the managed system attempts to activate each partition profile in the system profile in the order specified. A system profile helps you activate or change the managed system from one complete set of logical partition configurations to another. It can also be used to validate the resource configuration of multiple partitions to ensure that resource conflicts do not exist between partitions. You can create system profiles, as shown in Figure 5-77 on page 358.



Create System Profile: 750-1

Create the system profile by adding profiles from the available partition profiles.

System profile name : * test

Available Partition Profiles

- 750-1
  - p750_1_vio1 (1)
    - default
  - p750_1_vio2 (2)
    - default
  - p750_aix1 (3)
    - default
  - p750_aix2 (4)
    - default
  - p750_aix3 (5)
    - default

System Profile

Select	Partition	Profile
□	p750_1_vio1 (1)	default
□	p750_1_vio2 (2)	default
□	p750_aix1 (3)	default
□	p750_aix2 (4)	default
□	p750_aix3 (5)	default

Figure 5-77 Manage System Profile task

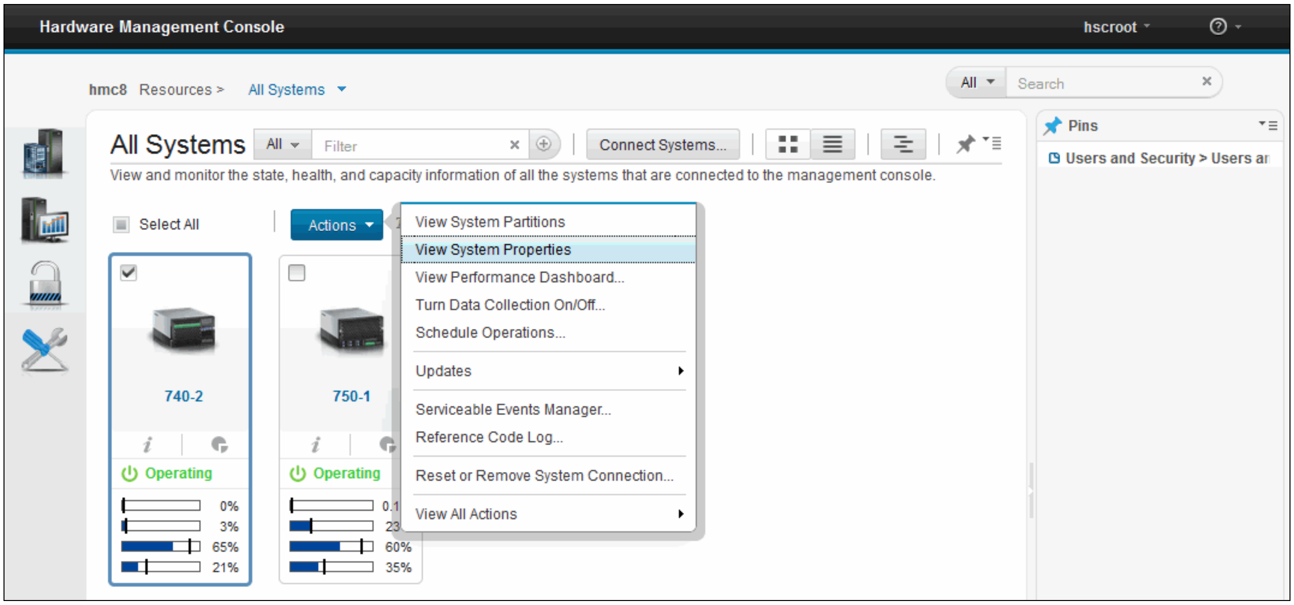
- Manage Partition Data task

  Use this task to provide four operations to manage profile data: restore, initialize, backup, and delete. This task is described in 5.6, “Partition management” on page 370.

Properties

Click the **Properties** task to displays the selected managed system’s properties. This information is useful in system and partition planning and resource allocation.

Click **Resources** → **Servers** to see a listing of the servers in the Table view, and select the server that you want to manage. Click **Actions** → **View System Properties** (Figure 5-78).

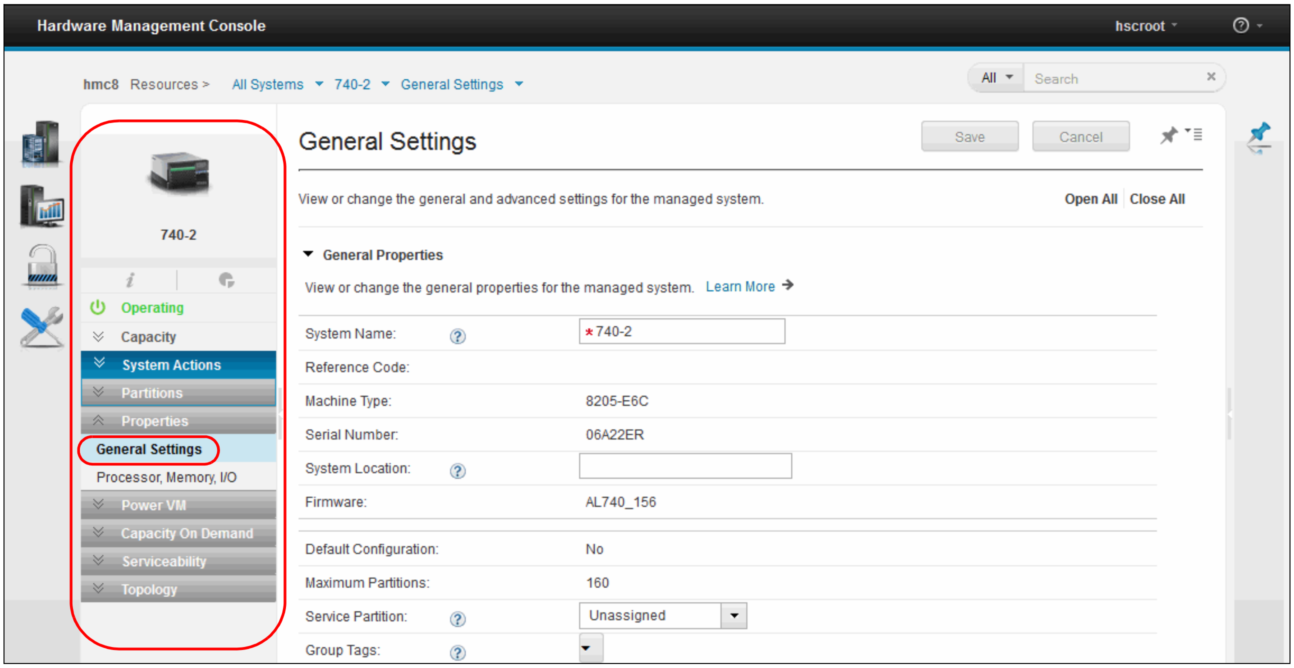


View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

Figure 5-78 Manage a server

The system properties panel opens, with a new system pane (Figure 5-79). This pane has the following tabs to help you manage the system:

- General Settings
- Processor, Memory, I/O



General Settings

View or change the general and advanced settings for the managed system.

General Properties

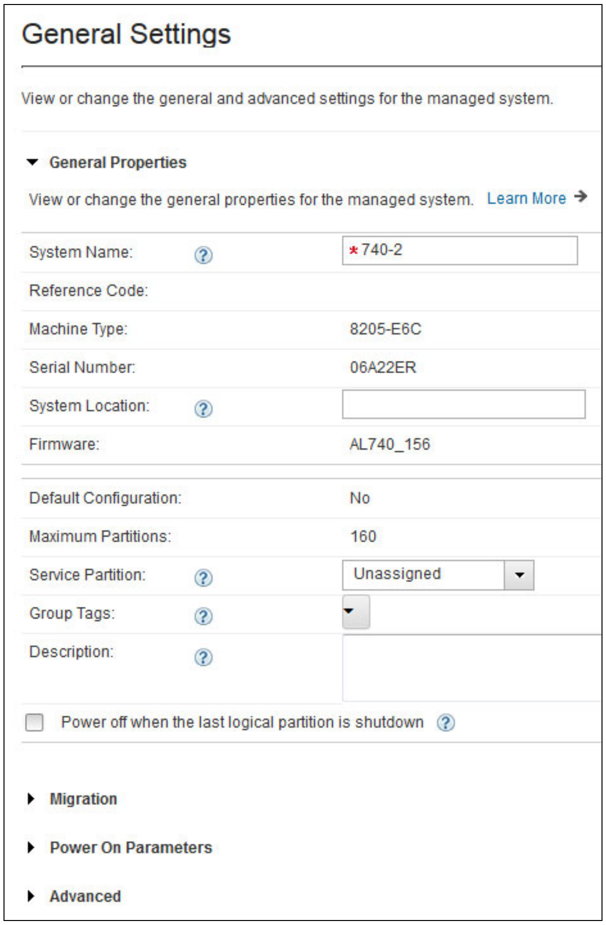
View or change the general properties for the managed system.

System Name:	* 740-2
Reference Code:	
Machine Type:	8205-E6C
Serial Number:	06A22ER
System Location:	
Firmware:	AL740_156
Default Configuration:	No
Maximum Partitions:	160
Service Partition:	Unassigned
Group Tags:	

Figure 5-79 System pane

General Settings

Click **General Settings** to open the General Settings panel (Figure 5-80). This panel lists the system name, serial number, model and type, state, attention LED state, service processor version, maximum number of partitions, assigned service partition (if designated), and power-off policy information.



General Settings

View or change the general and advanced settings for the managed system.

General Properties

View or change the general properties for the managed system. Learn More

System Name:	*740-2
Reference Code:	
Machine Type:	8205-E6C
Serial Number:	06A22ER
System Location:	
Firmware:	AL740_156
Default Configuration:	No
Maximum Partitions:	160
Service Partition:	Unassigned
Group Tags:	
Description:	

□ Power off when the last logical partition is shutdown

Migration

Power On Parameters

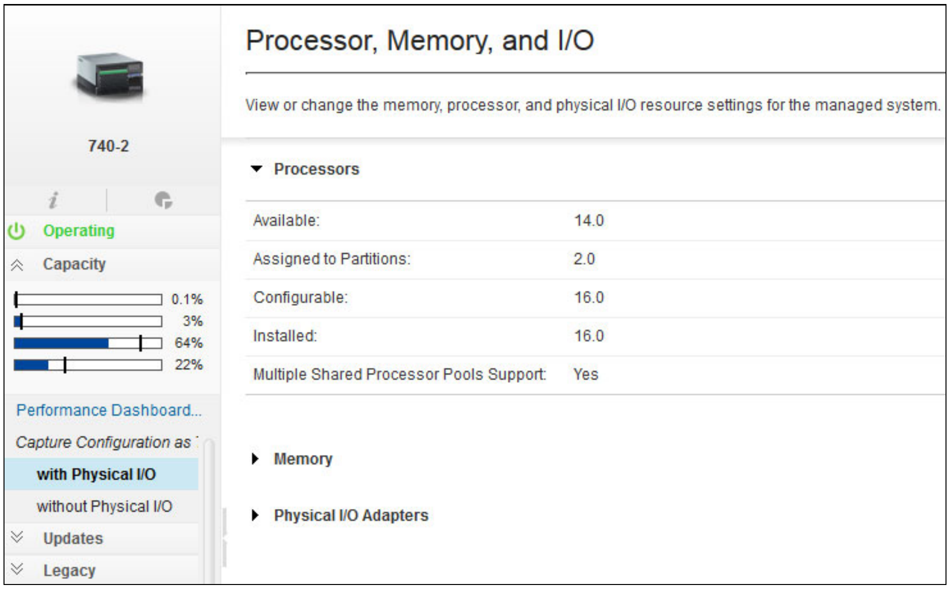
Advanced

Figure 5-80 General Settings

Processor, Memory, I/O

Click **Processor, Memory, I/O** to open the panel shown in Figure 5-81. It lists information about the processors, memory, and I/O of the managed system.

- The Processors area provides information regarding processors, including installed processing units, deconfigured processing units, available processing units, configurable processing units, minimum number of processing units per virtual processor and maximum number of shared processor pools.



Processor, Memory, and I/O

View or change the memory, processor, and physical I/O resource settings for the managed system.

▼ Processors

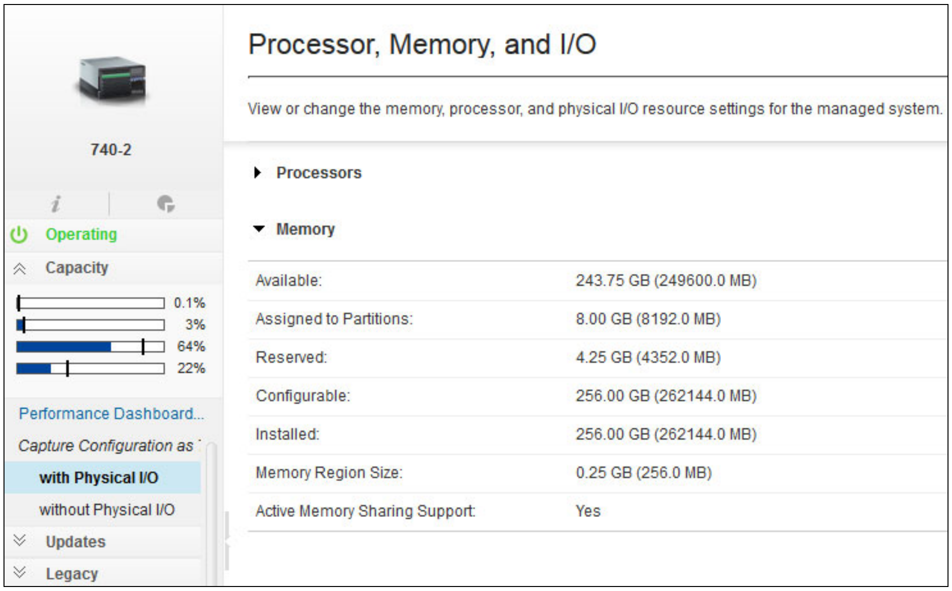
Available:	14.0
Assigned to Partitions:	2.0
Configurable:	16.0
Installed:	16.0
Multiple Shared Processor Pools Support:	Yes

▶ Memory

▶ Physical I/O Adapters

Figure 5-81 Processor tab

- The Memory area (Figure 5-82) displays information about the managed system's memory including installed memory, deconfigured memory, available memory, configurable memory, memory region size, current memory available for partition usage, system firmware current memory, and maximum number of memory pools.



Processor, Memory, and I/O

View or change the memory, processor, and physical I/O resource settings for the managed system.

▶ Processors

▼ Memory

Available:	243.75 GB (249600.0 MB)
Assigned to Partitions:	8.00 GB (8192.0 MB)
Reserved:	4.25 GB (4352.0 MB)
Configurable:	256.00 GB (262144.0 MB)
Installed:	256.00 GB (262144.0 MB)
Memory Region Size:	0.25 GB (256.0 MB)
Active Memory Sharing Support:	Yes

Figure 5-82 Memory tab

- I/O

  The I/O area (Figure 5-83) displays the physical I/O resources for the managed system. The assignment of I/O slots and partition, the adaptor, and the slot LP (Logical Partition) limit information are displayed. The physical I/O resources information is grouped by units:

  – The *slot* column lists the physical I/O properties of each resource.

  – The *I/O Pool* column lists all of the I/O pools found in the system and the partitions that are participating in the pools.

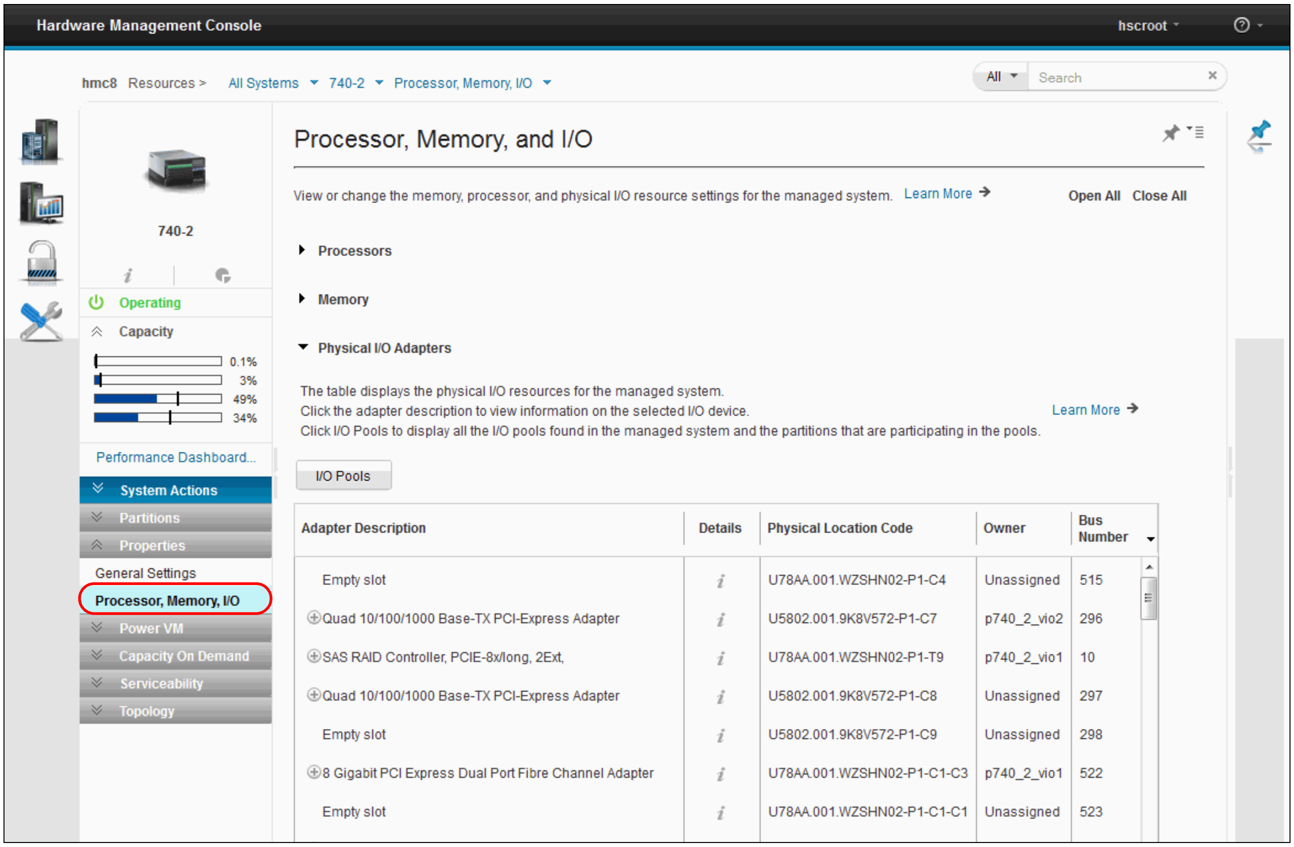
  – The *Owner* column lists who currently owns the physical I/O. The value of this column can be any of the following values:

    • When a single root I/O virtualization (SR-IOV) adapter is in the shared mode, Hypervisor is displayed in this column.

    • When an SR-IOV adapter is in the dedicated mode, Unassigned is displayed when the adapter is not assigned to any partition as a dedicated physical I/O.

    • When an SR-IOV adapter is in the dedicated mode, the logical partition name is displayed when the adapter is assigned to any logical partition as a dedicated physical I/O.

  – The *Slot LP Limit* column lists the number of logical ports supported by slot or adapter in SR-IOV shared mode.



Processor, Memory, and I/O

View or change the memory, processor, and physical I/O resource settings for the managed system. Learn More → Open All Close All

▸ Processors

▸ Memory

▾ Physical I/O Adapters

The table displays the physical I/O resources for the managed system.
Click the adapter description to view information on the selected I/O device.
Click I/O Pools to display all the I/O pools found in the managed system and the partitions that are participating in the pools.
Learn More →

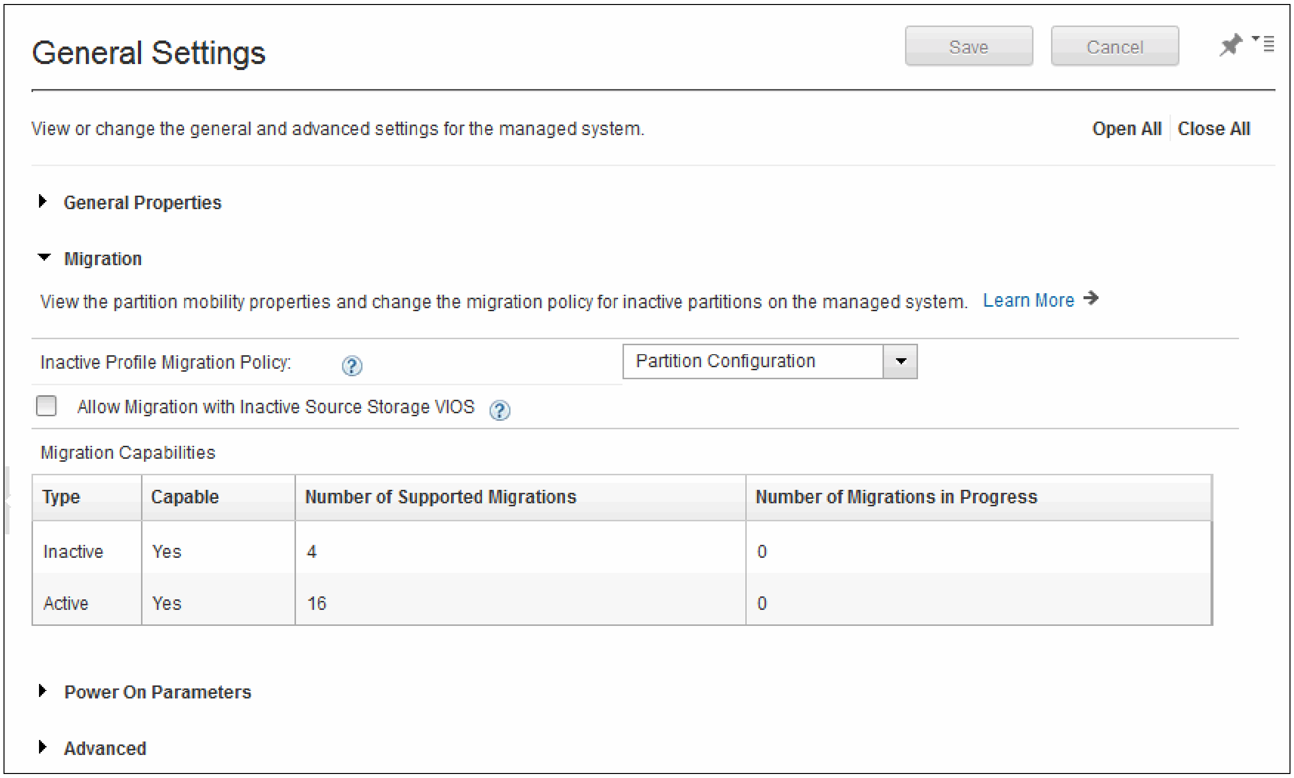
I/O Pools

Adapter Description	Details	Physical Location Code	Owner	Bus Number
Empty slot	i	U78AA.001.WZSHN02-P1-C4	Unassigned	515
⊕Quad 10/100/1000 Base-TX PCI-Express Adapter	i	U5802.001.9K8V572-P1-C7	p740_2_vio2	296
⊕SAS RAID Controller, PCIE-8x/long, 2Ext,	i	U78AA.001.WZSHN02-P1-T9	p740_2_vio1	10
⊕Quad 10/100/1000 Base-TX PCI-Express Adapter	i	U5802.001.9K8V572-P1-C8	Unassigned	297
Empty slot	i	U5802.001.9K8V572-P1-C9	Unassigned	298
⊕8 Gigabit PCI Express Dual Port Fibre Channel Adapter	i	U78AA.001.WZSHN02-P1-C1-C3	p740_2_vio1	522
Empty slot	i	U78AA.001.WZSHN02-P1-C1-C1	Unassigned	523

Figure 5-83 I/O area view

Migration

If your managed system is capable of partition migration, the Migration area (Figure 5-84) displays partition migration information.



View or change the general and advanced settings for the managed system.

View the partition mobility properties and change the migration policy for inactive partitions on the managed system.

Inactive Profile Migration Policy: Partition Configuration

□ Allow Migration with Inactive Source Storage VIOS

Migration Capabilities

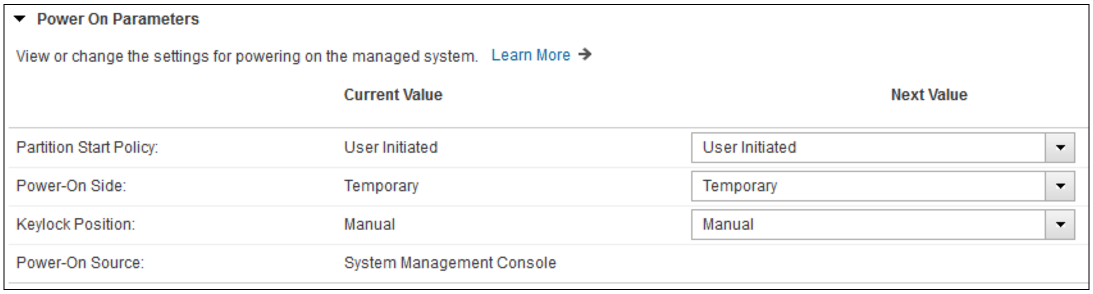
Type	Capable	Number of Supported Migrations	Number of Migrations in Progress
Inactive	Yes	4	0
Active	Yes	16	0

Figure 5-84 Migration

> **Migration tab:** If your managed system is not partition-migration capable, the **Migration** tab is not shown.

Power On Parameters

Use the Power On Parameters area (Figure 5-85) to change the power-on parameters for the next restart by changing the values in the Next fields. These changes will be valid for only the next managed system restart.



View or change the settings for powering on the managed system.

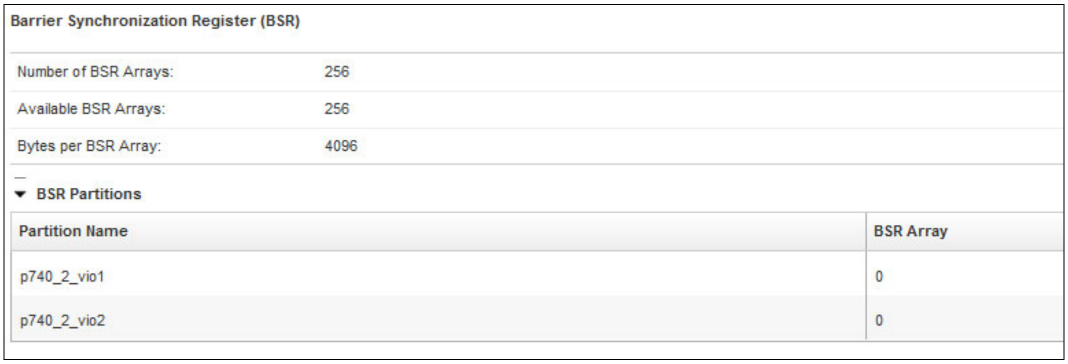
	Current Value	Next Value
Partition Start Policy:	User Initiated	User Initiated
Power-On Side:	Temporary	Temporary
Keylock Position:	Manual	Manual
Power-On Source:	System Management Console	

Figure 5-85 Power On Parameters

Advanced

The Advanced area displays huge page memory capabilities on the managed system, including available huge page memory, configurable huge page memory, current page size, and current maximum huge page memory. To change memory allocation on systems with huge page table support, set the Requested huge page memory (in pages) field to the desired memory. To change the requested value for huge page memory, the system must be powered off.

The Barrier Synchronization Register (BSR) option displays array information (Figure 5-86).



Barrier Synchronization Register (BSR)

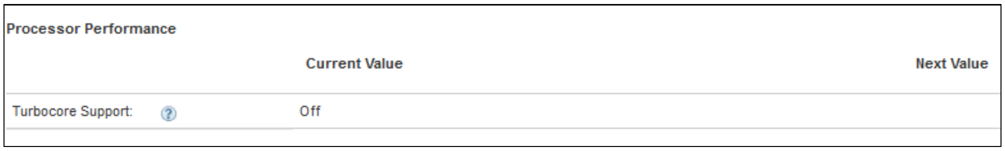
Number of BSR Arrays:	256
Available BSR Arrays:	256
Bytes per BSR Array:	4096

▼ BSR Partitions

Partition Name	BSR Array
p740_2_vio1	0
p740_2_vio2	0

Figure 5-86 Barrier Synchronization Register (BSR) view

The Processor Performance option displays the Turbocore mode (Figure 5-87) and the System Partition Processor Limit (SPPL).



Processor Performance

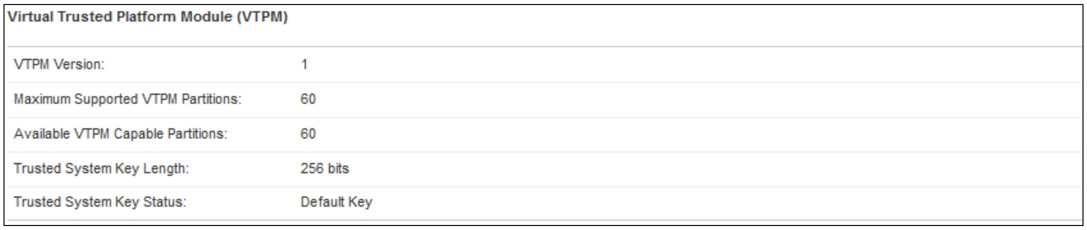
	Current Value	Next Value
Turbocore Support: ?	Off	

Figure 5-87 Processor Performance limit view

You can set the next Turbocore mode and the next SPPL value. The SPPL applies to both dedicated processor partitions and shared processor partitions.

The Memory Mirroring option displays the current mirroring mode and the current system firmware mirroring status. You can set the next mirroring mode. You can also launch the memory optimization tool.

You can view the Virtual Trusted Partition Module (VTPM) settings (Figure 5-88).



Virtual Trusted Platform Module (VTPM)

VTPM Version:	1
Maximum Supported VTPM Partitions:	60
Available VTPM Capable Partitions:	60
Trusted System Key Length:	256 bits
Trusted System Key Status:	Default Key

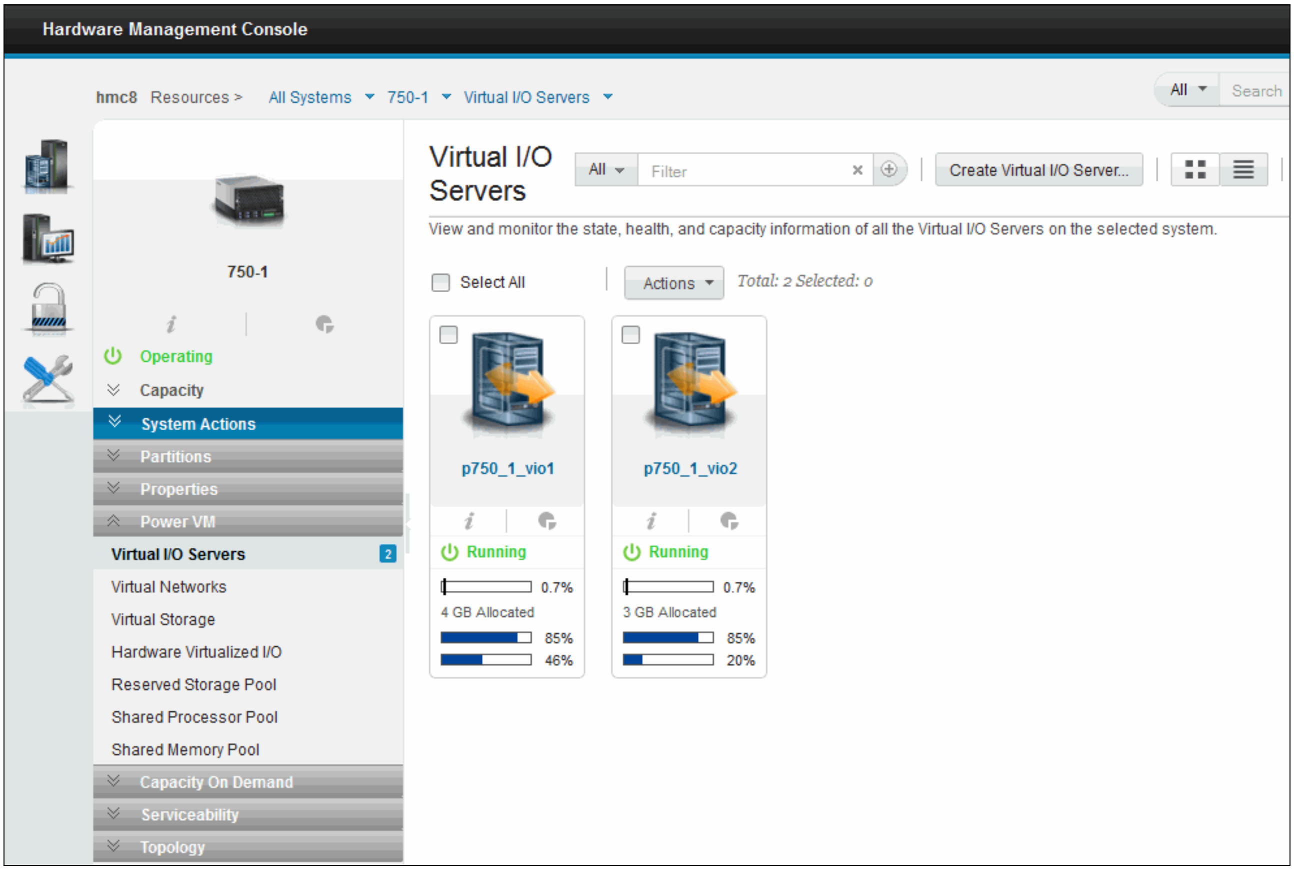
Figure 5-88 VTPM view

Serviceability

Use this task to view specific events for selected systems. Problem Analysis on the HMC automatically detects error conditions and reports to you any problem that requires service to repair it. These problems are reported to you as serviceable events. This task is explained in 6.3.1, “Serviceable Events Manager” on page 427.

PowerVM

Use the PowerVM tasks (Figure 5-89) to view and monitor the state, health, and capacity information of all the Virtual I/O Servers on the selected system.



View and monitor the state, health, and capacity information of all the Virtual I/O Servers on the selected system.

Figure 5-89 PowerVM view

The available PowerVM tasks are as follows:

- Virtual I/O Servers

  For further details, see 5.4.3, “All Virtual I/O Servers” on page 328.

- Virtual Networks
- Virtual Storage
- Hardware Virtualized I/O

  Displays all the I/O adapters that are configured for the managed system. You can view and modify the properties for the SRIOV, HEA, and HCA adapters.

  – HEA Adapters

    Displays the port configuration of the physical Host Ethernet Adapters (HEAs) that are assigned to the managed system. Select the required HEA to display a table that contains the port configuration details. Select any port in this table and use the Actions menu to modify the port configuration and view the partitions that are associated with the selected HEA port. Select Modify HEA Adapter to modify the HEA adapter properties.

  – HCA Adapters

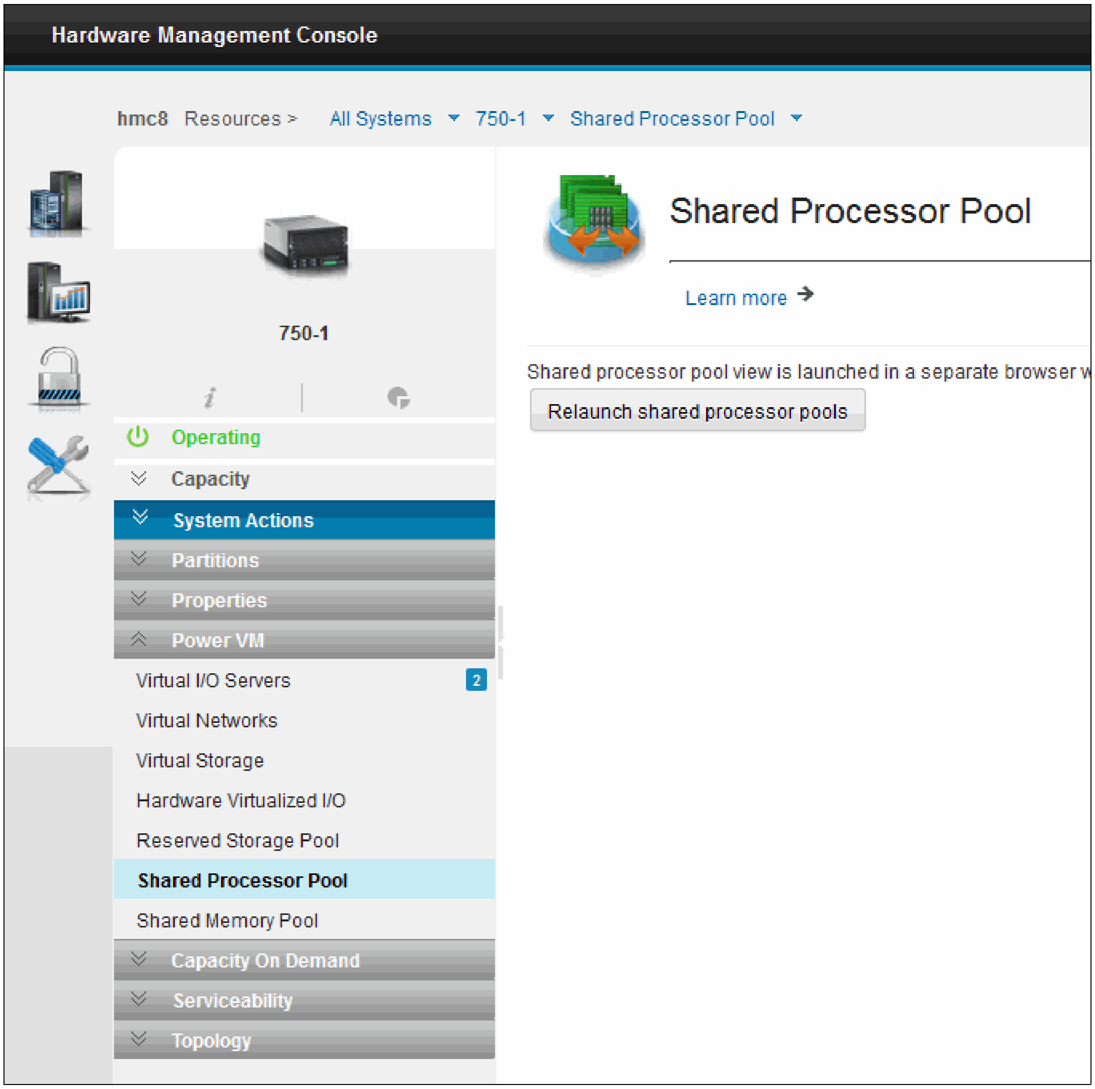
    You can view and manage the host channel adapters (HCAs) from the legacy HMC page. Click **Launch Manage Host Channel Adapters**, to launch the HCA page.

- Reserved Storage Pool

    Use this task to associate one or more VIOS partitions with the reserved storage device pool. If supported, a second VIOS can be added to provide a redundant path and higher availability to the reserved storage device.

- Shared Processor Pool

  The Shared Processor Pool view is launched in a separate browser window by clicking **Relaunch shared processor pools** (Figure 5-90).



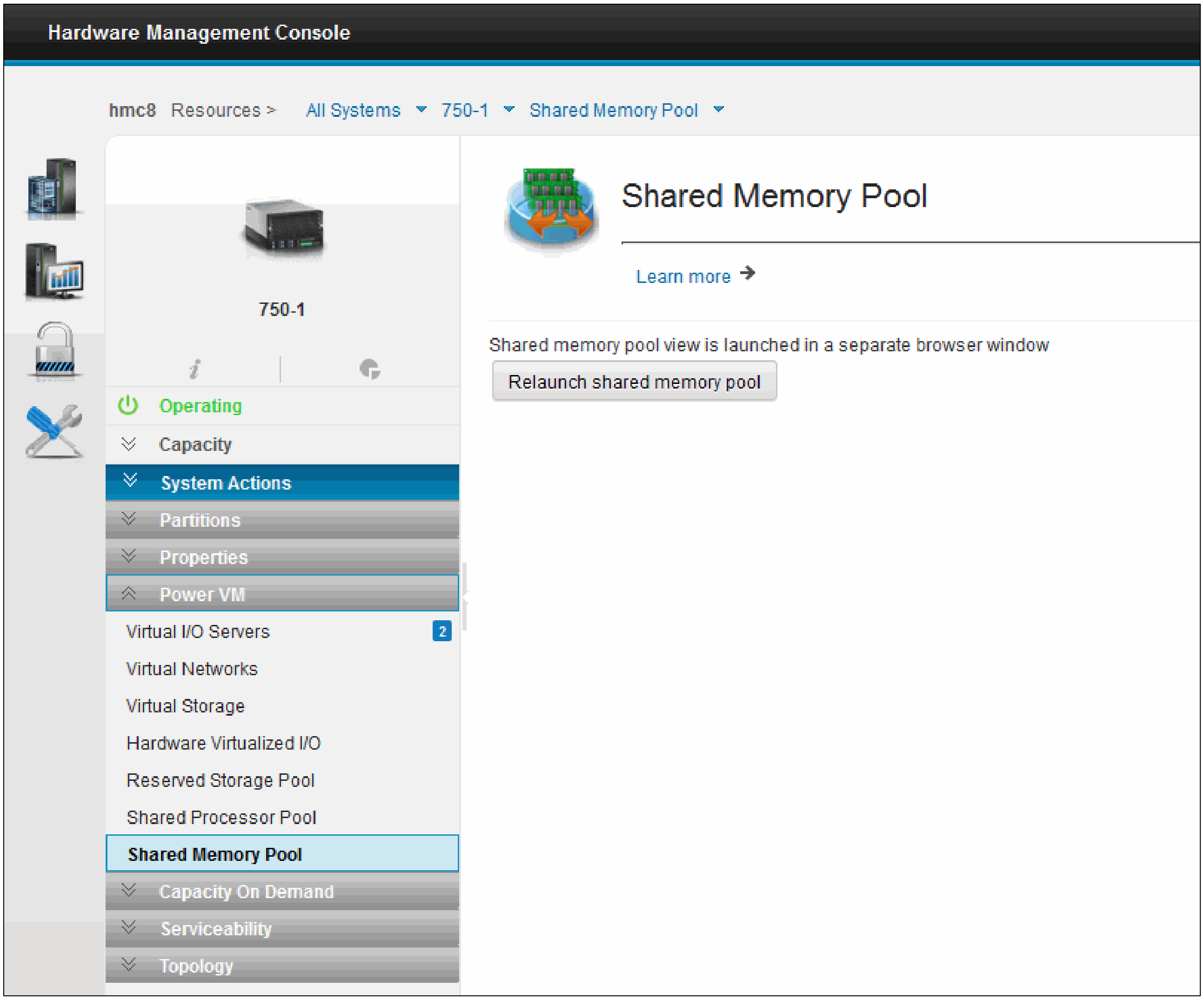
Shared processor pool view is launched in a separate browser w

Figure 5-90 Shared Processor Pool

This page displays information about the shared processor pools that exist for the selected managed system. You can also change the properties of any shared processor pool except for the default shared processor pool.

- Shared Memory Pool

  The Shared Memory Pool view is launched in a separate browser window, by clicking **Relaunch Shared memory pool** (Figure 5-91).



Shared memory pool view is launched in a separate browser window

Figure 5-91 Shared memory pools

In the view that is launched, you can do these tasks:

- Specify the size of the memory pool.
- Choose the paging VIOS partition or partitions to be associated with the pool.
- Choose paging space devices available to the pool.
- Enable/Disable Active Memory Deduplication (if supported).

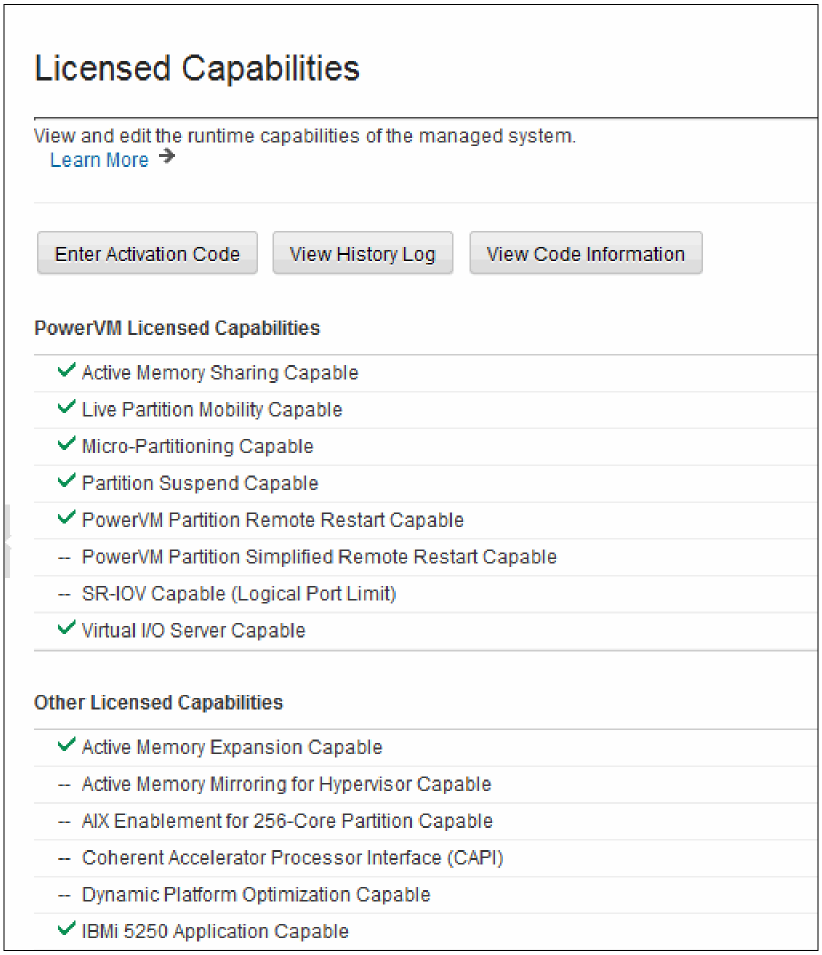
Note: Memory assigned to the pool will not be available for use by dedicated memory partitions.

Capacity on Demand

Use Capacity on Demand (CoD) to nondisruptively activate (no boot is required) processors and memory. CoD also gives you the option to temporarily activate capacity to meet intermittent performance needs to activate extra capacity on a trial basis, and to access capacity to support operations in times of need. This task is explained in 5.11, “Capacity on Demand (CoD)” on page 405.

Licensed Capabilities

The Licensed Capabilities panel (Figure 5-92) of the Capacity On Demanded task displays the runtime capabilities of this server.



Licensed Capabilities

View and edit the runtime capabilities of the managed system.
Learn More →

PowerVM Licensed Capabilities

- ✓ Active Memory Sharing Capable
- ✓ Live Partition Mobility Capable
- ✓ Micro-Partitioning Capable
- ✓ Partition Suspend Capable
- ✓ PowerVM Partition Remote Restart Capable
- -- PowerVM Partition Simplified Remote Restart Capable
- -- SR-IOV Capable (Logical Port Limit)
- ✓ Virtual I/O Server Capable

Other Licensed Capabilities

- ✓ Active Memory Expansion Capable
- -- Active Memory Mirroring for Hypervisor Capable
- -- AIX Enablement for 256-Core Partition Capable
- -- Coherent Accelerator Processor Interface (CAPI)
- -- Dynamic Platform Optimization Capable
- ✓ IBMi 5250 Application Capable

Figure 5-92 Licensed Capabilities

You can verify that the server supports Virtual Trusted Platform Module (VTPM), Virtual Server Network (VSN), Dynamic Platform Optimization (DPO), and SR-IOV capabilities.

Topology

The Topology task provides two diagrams views:

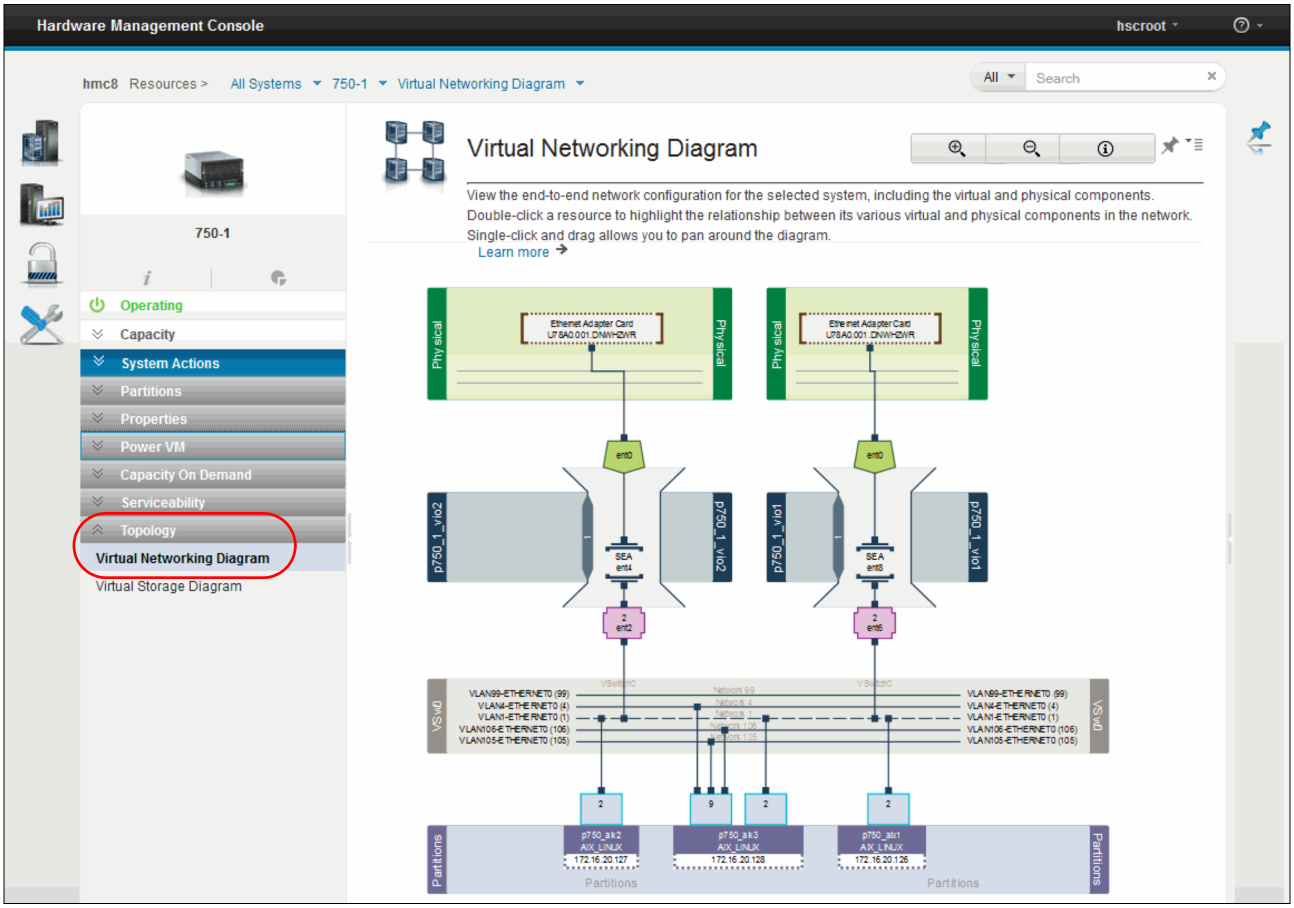
- Virtual Networking Diagram

  View the end-to-end network configuration for the selected system, including the virtual and physical components. Double-click a resource to highlight the relationship between its various virtual and physical components in the network. Single-click and drag allows you to pan around the diagram.

- Virtual Storage Diagram

  View the virtual storage configuration for the selected system, including the physical and virtual components of system storage. This diagram displays a high-level overview of the contents of the system rather than the specific component relationships. Double-click a resource to highlight the relationship between its various virtual and physical components. Single-click and drag, allows you to pan around the diagram.

An example of the Virtual Network Diagram view is shown in Figure 5-93.



Virtual Networking Diagram

View the end-to-end network configuration for the selected system, including the virtual and physical components. Double-click a resource to highlight the relationship between its various virtual and physical components in the network. Single-click and drag allows you to pan around the diagram.

Figure 5-93 Virtual Networking Diagram

5.6 Partition management

In HMC V8.8.4.0, the user interface (UI) is updated for partition management. Although you may still manager the partition by using the existing UI (which is the only way for certain functions), actions such as dynamic partitioning and managing a partition profile can be performed by using the new UI.

5.6.1 Viewing and changing the partition properties

To access the partition management pane, click the **Resources** icon in the left navigation pane, and select **All Partitions** (Figure 5-94).

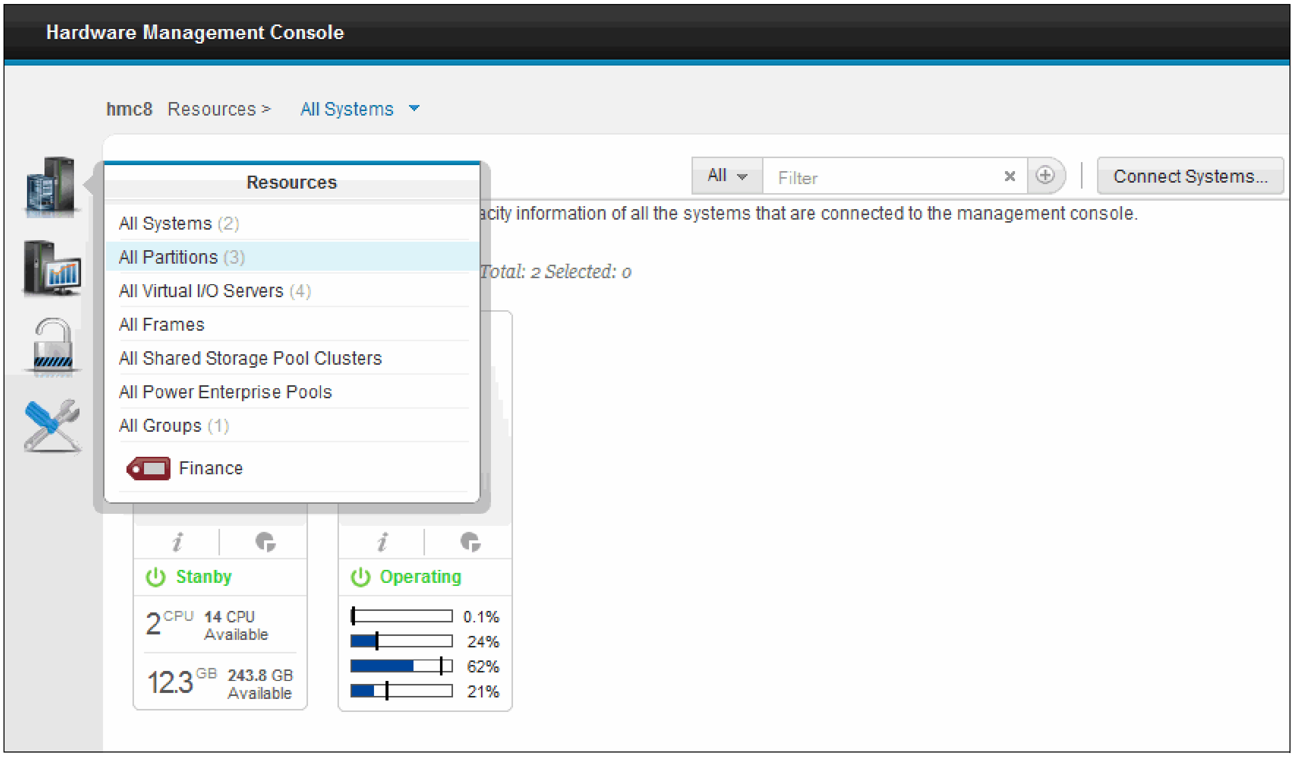

Hardware Management Console
hmc8 Resources > All Systems
Resources
All Systems (2)
All Partitions (3)
All Virtual I/O Servers (4)
All Frames
All Shared Storage Pool Clusters
All Power Enterprise Pools
All Groups (1)
Finance
All
Filter
Connect Systems...
acity information of all the systems that are connected to the management console.
Total: 2 Selected: 0
Stanby
2 CPU 14 CPU Available
12.3 GB 243.8 GB Available
Operating
0.1%
24%
62%
21%

Figure 5-94 Open the All Partitions pane

From the All Partitions pane, select one of the logical partitions, and select **Actions** → **View All Actions** (Figure 5-95).

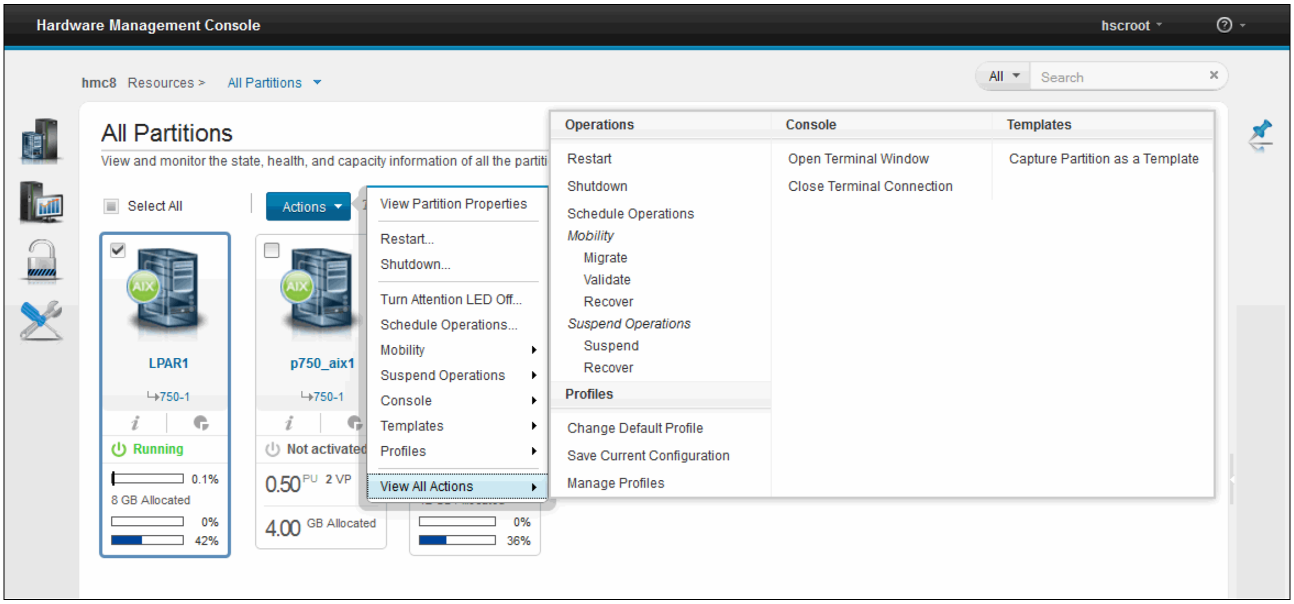
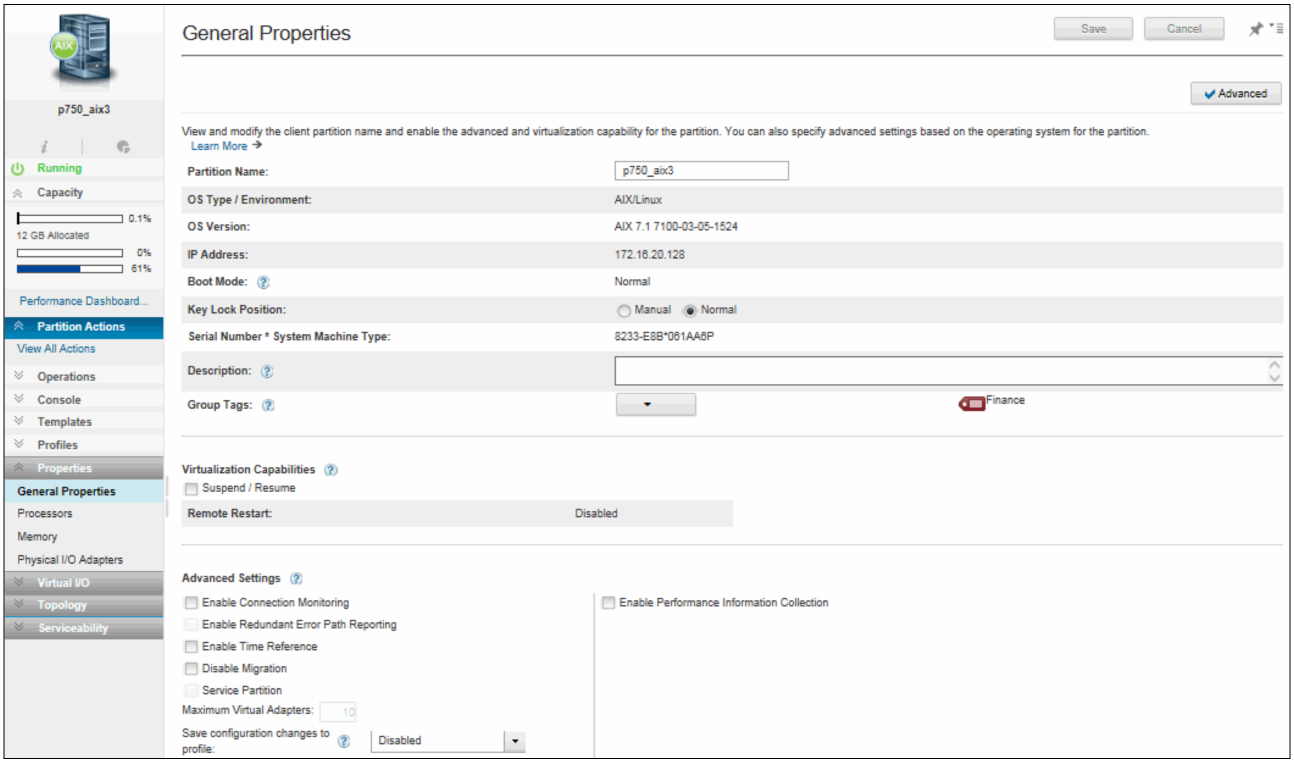


Figure 5-95 View All Actions menu

If you select **Actions** → **View Partitions Properties**, the General Properties window opens (Figure 5-96).



General Properties

View and modify the client partition name and enable the advanced and virtualization capability for the partition. You can also specify advanced settings based on the operating system for the partition.

Partition Name:	p750_aix3
OS Type / Environment:	AIX/Linux
OS Version:	AIX 7.1 7100-03-05-1524
IP Address:	172.16.20.128
Boot Mode:	Normal
Key Lock Position:	○ Manual ● Normal
Serial Number * System Machine Type:	8233-E8B*061AA6P
Description:	
Group Tags:	Finance

Virtualization Capabilities

□ Suspend / Resume

Remote Restart: Disabled

Advanced Settings

□ Enable Connection Monitoring
□ Enable Redundant Error Path Reporting
□ Enable Time Reference
□ Disable Migration
□ Service Partition
Maximum Virtual Adapters: 10
Save configuration changes to profile: Disabled

□ Enable Performance Information Collection

Figure 5-96 Manage partition window general and advanced options

This pane shows the following information about the partition:

- Partition NAME
- Operating system (OS) Type and Environment
- OS Version
- IP Address
- Boot Mode
- Serial Number

To access more partition configuration options, click **Advanced**. These partition configuration options are available:

- Enable Connection Monitoring
- Enable Time Reference
- Disable Migration
- Enable Performance Information Collection

A new addition is the `Save configuration changes to profile` parameter. Setting it to **Enabled** copies changes to the partition configuration by using dynamic partitioning on the partition profile.

> **Note:** The `Save configuration changes to profile` setting also can be set in the Properties window of the logical partition in the previous HMC UI. In this window, it is referred to as *Sync current configuration Capability*.

On the left side you see the menu, which is described in further detail. The upper part has some status information about the selected logical partition.

Capacity

The Capacity section displays an overview of some performance data. For a further detailed view, select the **Performance Dashboard** link in the menu. The Performance and Capacity (PCM) page opens. For more details, see Chapter 7, “Performance and capacity monitoring” on page 511.

Partition Actions

Partition Actions section includes operations Console, Templates, Profiles.

Operations

Use the Operations section for the following basic management tasks of the selected logical partition:

- Restart

  Select **Restart** to reboot the logical partition. Options include restarting in any of the following ways:

  - Dump

    Initiates a system memory dump on the logical partition and restarts the logical partition when complete.

  - Operating System

    Issues the operating system command to restart the logical partition normally.

  - Immediate

    Restarts the logical partition as quickly as possible, without notifying it. This option might cause undesirable results if data was partially updated.

  - Operating System Immediate

    Issues the operating system command to restart the logical partition immediately.

  - Dump Retry

    Retries a system memory dump for the logical partition and restarts the logical partition when complete.

- Shutdown

  Select **Shutdown** to shut down the selected logical partition. Options include shutting down in any of the following ways:

  - Delayed

    Shuts down the logical partition by starting the delayed power-off sequence.

  - Immediate

    Shuts down the logical partition as quickly as possible, without notifying it. This option might cause undesirable results if data has been partially updated.

  - Operating System

    Issues the operating system command to shut down the logical partition normally.

  - Operating System Immediate

    Issues the operating system command to shut down the logical partition immediately.

- Schedule Operations

  Select **Schedule Operations** to schedule an operation for the selected logical partition. The task is further explained in 5.3.2, "Schedule Operations" on page 317.

- Mobility

  Use the Mobility section to manage the Live Partition Mobility (LPM) tasks for the selected logical partition. For further information about Live Partition Mobility, see *IBM PowerVM Virtualization Introduction and Configuration*, SG24-7940 and *IBM PowerVM Virtualization Managing and Monitoring*, SG24-7590.

  - Migrate

    If you select **Migrate**, the Migration Wizard opens, which guides you through the migration of the selected logical partition to another managed system. The wizard consist of following chronological panes:

    - Migration Information

      View information about the selected logical partition. Furthermore you can override some error settings.

    - Profile Name

      You can specify a new destination profile name.

    - Remote HMC

      You can specify a remote HMC that has a connection to the destination system.

    - Destination

      You can select the destination system.

    - Validation Errors/Warnings

      A validation will be carried out and possible errors or warnings are displayed.

    - Mover Service Partitions

      You can specify the Virtual I/O Servers that you want involved in the LPM operation.

    - VLAN Configuration

      You can change the VLAN configuration of the selected logical partition for the destination system.

    - Virtual Storage Adapters

      You can change the Virtual Storage Adapter configuration of the selected logical partition for the destination system.

    - Shared Processor Pools

      You can specify another Shared Processor Pool for the selected logical partition on the destination system.

    - Wait Time

      You can specify a wait time (in minutes) for the operating system to wait for applications to acknowledge the migration is about to happen.

    - Summary

      You can view a summary of your selections. If you click **Finish** the migration starts.

  - Validate

    Select **Validate** to specify the migration options, as in the wizard (described above) in the Partition Migration Validation window. By clicking **Validate**, the HMC checks whether migration can be performed. Possible errors or warnings are listed. If no errors occur, you can click **Migrate** to start a migration.

  - Recover

    If the migration failed, the partition might be in an invalid state. Select **Recover** to start a recovery procedure that cleans up and bring the partition to a valid state.

- Suspend Operations

  Use the Suspend Operations section to manage the suspend and recover options of the selected logical partition.

  - Suspend

    Select **Suspend** to suspect the selected partition. If the suspend operation succeeds without failure, instead of the Suspend task, a Resume task is available. Select **Resume** to activate the logical partition again.

  - Recover

    If suspend or resume actions fail, the partition might not be in a valid state. Select **Recover**, to start a recovery procedure that cleans up and brings the partition to a valid state.

Console

Use the Console section to manage terminals for the selected logical partition:

- Open Terminal Window

  Select **Open Terminal Window** to open a terminal window to the selected logical partition. You can have only one open terminal window for a logical partition at a time, independent how many HMCs you have.

- Close Terminal Connection

  Select **Close Terminal Connection** to close an open terminal window. Be aware that another administrator might be using this window and therefore might lose work.

Templates

Use the Templates section to manage the templates for a logical partition:

- Capture Partition as a Template

  Select **Capture partition as a template** to capture the selected logical partition. For further information about templates and how to manage them, see 2.6, “Partition templates” on page 108.

Profiles

Use the *Profiles* section to manage the profiles of the selected logical partition:

- Change Default Profile

  Select **Change Default Profile** to make another profile the default profile.

- Save Current Configuration

  Select **Save Current Configuration** to save the state of a running partition to a new profile, or overwrite an existing profile, which you can select. This option is useful if you made changes to a logical partition using DLPAR (CPU, Memory, I/O), but now you want theses changes to be permanent.

- Manage Profiles

  Select **Manage Profiles** to edit every aspect of an existing profile. Also you can make a new profile, copy a profile, delete a profile, or activate a profile.

Properties

Use the Properties section to view and dynamically change resources of a selected partition:

- General Properties

  The General Properties view is shown in Figure 5-96 on page 371.

- Processors

  The Processors view is discussed in 5.7.1, “Changing processor or memory settings” on page 376.

- Memory

  The Memory view is discussed in 5.7.1, “Changing processor or memory settings” on page 376.

- Physical I/O Adapters

  The Physical I/O Adapters view is discussed in 5.7.2, “Adding or removing a physical adapter” on page 378.

Virtual I/O

Use the Virtual I/O section to view and edit the virtual settings, such as network and storage, for the selected logical partition:

- Virtual Networks

  The Virtual Networks view is discussed in 5.8, “Virtual Network management” on page 379.

- Virtual Storage

  The Virtual Storage view is discussed in 5.9, “Virtual Storage management” on page 382.

- Hardware Virtualized I/O

  The Hardware Virtualized I/O view is discussed in 5.10, “Managing hardware-virtualized I/O adapters” on page 402.

Topology

Use the Topology section to view the topology of the selected logical partition:

- Partition Virtual Storage Diagram

  Select **Partition Virtual Storage Diagram** to see a graphical presentation of the virtual storage connections of the selected logical partition, such as the one for the network shown in Figure 5-93 on page 369.

Serviceability

Use the Serviceability section to view the Reference Code Log of the selected logical partition:

- Reference Code Log

  Select **Reference Code Log** to see a list of the most recent reference codes. Reference codes provide general diagnostic, troubleshooting, and debugging information. To view the details of a specific reference code, select the reference code.

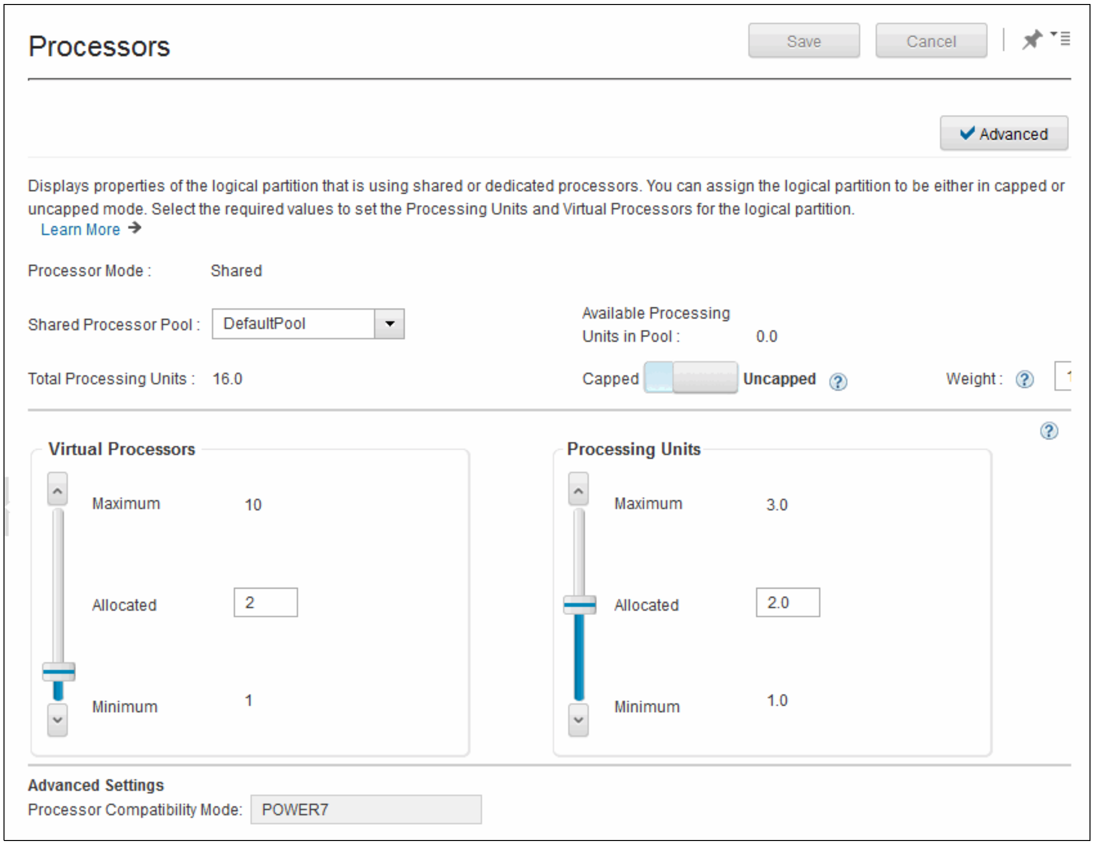
5.7 Dynamic partitioning

Dynamic partitioning can be performed on the partition by selecting the tab of the resource that you want to change.

5.7.1 Changing processor or memory settings

The methods of changing processor or memory settings are similar, so only changing the processor settings is described.

To change the processor allocation, select **Properties** → **Processors**. In the Processors window (Figure 5-97), change the value by moving the slider of the resource (Virtual Processors or Processing Units) to another value.



Processors

Displays properties of the logical partition that is using shared or dedicated processors. You can assign the logical partition to be either in capped or uncapped mode. Select the required values to set the Processing Units and Virtual Processors for the logical partition.

Learn More →

Processor Mode : Shared

Shared Processor Pool : DefaultPool

Available Processing Units in Pool : 0.0

Total Processing Units : 16.0

Capped / **Uncapped**

Weight :

Virtual Processors

Maximum	10
Allocated	2
Minimum	1

Processing Units

Maximum	3.0
Allocated	2.0
Minimum	1.0

Advanced Settings

Processor Compatibility Mode: POWER7

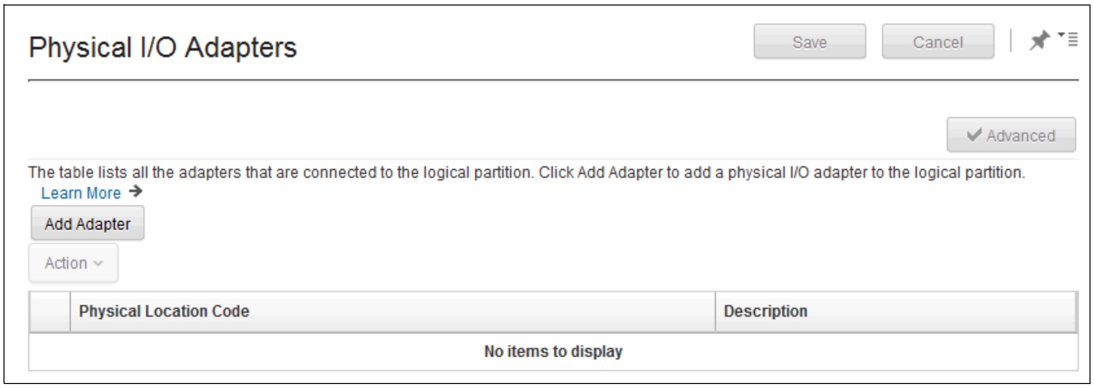
Figure 5-97 Changing resource values

Note: Another way to change the value of the resource is to enter a number by entering in the **Allocated** box. The value can be less than 1, for example 0.8; the leading zero (0) must be included or the box shows an error indicating an invalid value.

To change the memory settings, select **Properties** → **Memory**. Adjust the memory settings as required, and click **OK**, or if additional changes must be made, click **Apply**.

5.7.2 Adding or removing a physical adapter

To add a physical adapter, select **Properties** → **Physical I/O Adapter**. The Physical I/O Adapters window opens (Figure 5-98).



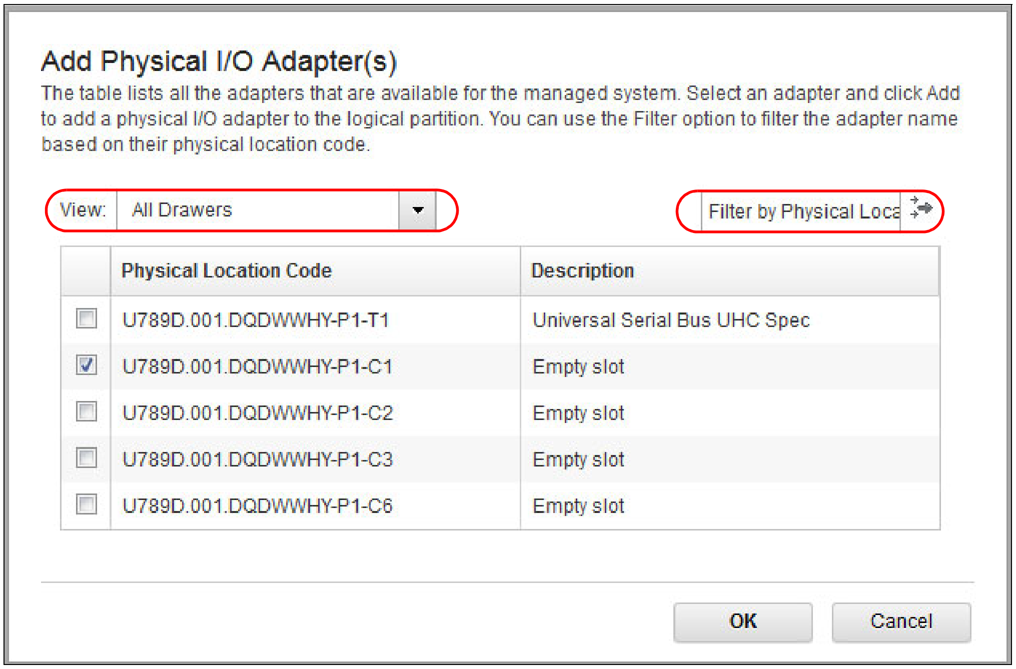
Physical I/O Adapters

The table lists all the adapters that are connected to the logical partition. Click Add Adapter to add a physical I/O adapter to the logical partition.

	Physical Location Code	Description
	No items to display	

Figure 5-98 Physical I/O Adapter window

To add an adapter, click **Add Adapter**. A window with the available adapters in the system opens (Figure 5-99). The default filter shows all the available adapters in the system. On systems with multiple I/O drawers, to filter by I/O drawer, select the I/O drawer from the **View** menu. A filter also can be applied to show only a specific slot in each I/O drawer, for example, slot C1, by entering the filter parameter in the Filter by Physical Location text box.



Add Physical I/O Adapter(s)

The table lists all the adapters that are available for the managed system. Select an adapter and click Add to add a physical I/O adapter to the logical partition. You can use the Filter option to filter the adapter name based on their physical location code.

View: All Drawers

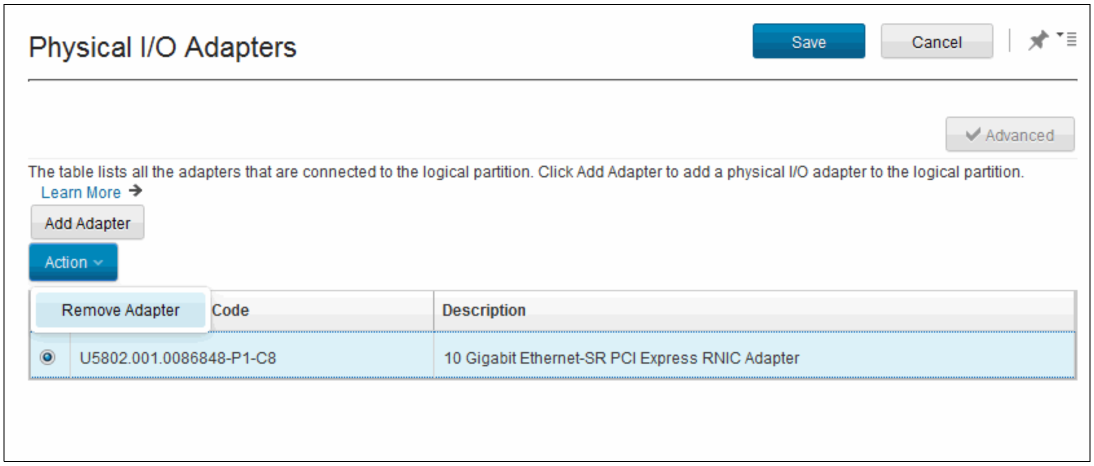
Filter by Physical Loca

	Physical Location Code	Description
□	U789D.001.DQDWWHY-P1-T1	Universal Serial Bus UHC Spec
☑	U789D.001.DQDWWHY-P1-C1	Empty slot
□	U789D.001.DQDWWHY-P1-C2	Empty slot
□	U789D.001.DQDWWHY-P1-C3	Empty slot
□	U789D.001.DQDWWHY-P1-C6	Empty slot

Figure 5-99 Available I/O adapters

To allocate this selected slot to the partition, click **OK**. This adapter is added to the partition by using dynamic partitioning.

To remove a physical adapter, select the adapter to be removed at the Physical I/O Adapter window (Figure 5-100). Click **OK** in the confirmation box to remove the adapter from the partition configuration.



The table lists all the adapters that are connected to the logical partition. Click Add Adapter to add a physical I/O adapter to the logical partition.

	Code	Description
●	U5802.001.0086848-P1-C8	10 Gigabit Ethernet-SR PCI Express RNIC Adapter

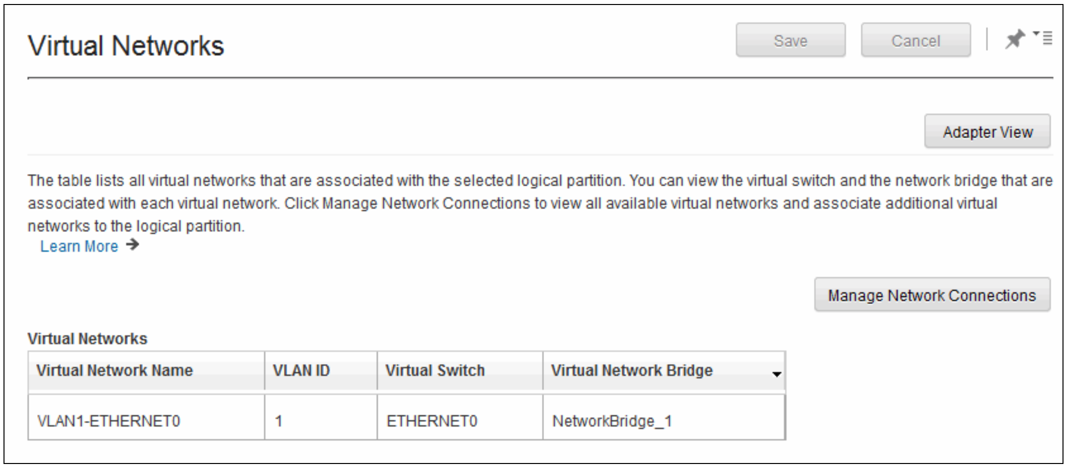
Figure 5-100 Physical adapter removal

5.8 Virtual Network management

Network management is simplified in HMC V8.8.4.0. Previously, the network information was available by looking at the partition profile or the Virtual Network Management window. With the new UI, the virtual network configuration is easier to understand and manage.

5.8.1 Adding new virtual networks

To add a new virtual network, click **Virtual Networks** in the Partition Management window. The Virtual Networks window opens (Figure 5-101), showing the details of the currently configured virtual network on the partition.



The table lists all virtual networks that are associated with the selected logical partition. You can view the virtual switch and the network bridge that are associated with each virtual network. Click Manage Network Connections to view all available virtual networks and associate additional virtual networks to the logical partition.

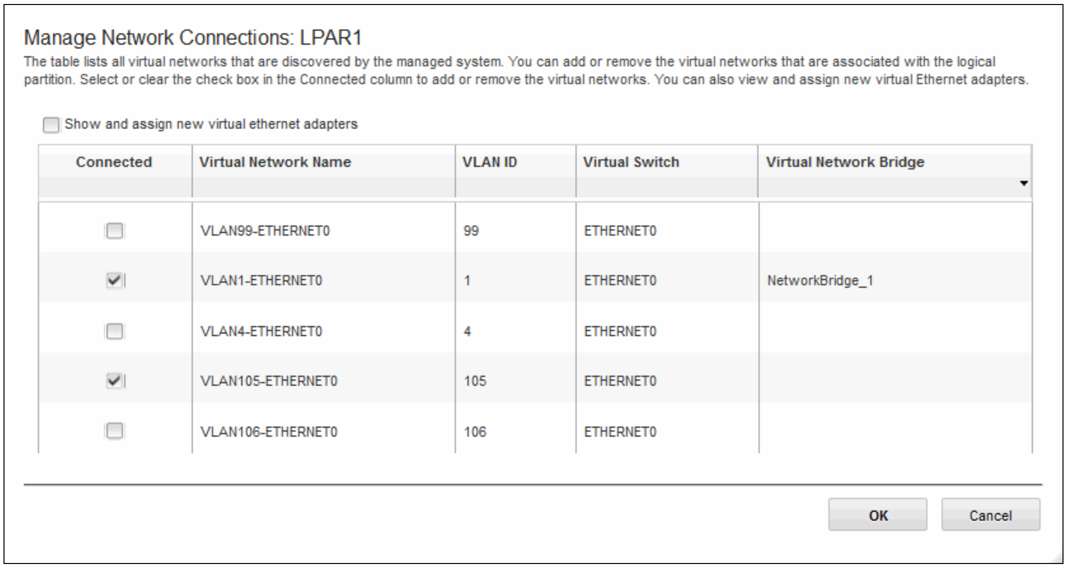
Virtual Networks

Virtual Network Name	VLAN ID	Virtual Switch	Virtual Network Bridge
VLAN1-ETHERNET0	1	ETHERNET0	NetworkBridge_1

Figure 5-101 Configured VLANs

To add a network, click **Manage Network Connections**. The Manage Network Connections window opens (Figure 5-102) and lists all available virtual networks that are configured on the managed host.

> **Note:** If a network bridge is shown in this window, then it is an adapter with an external connection. Networks that are internal to the managed host do not have a network bridge entry.



Manage Network Connections: LPAR1

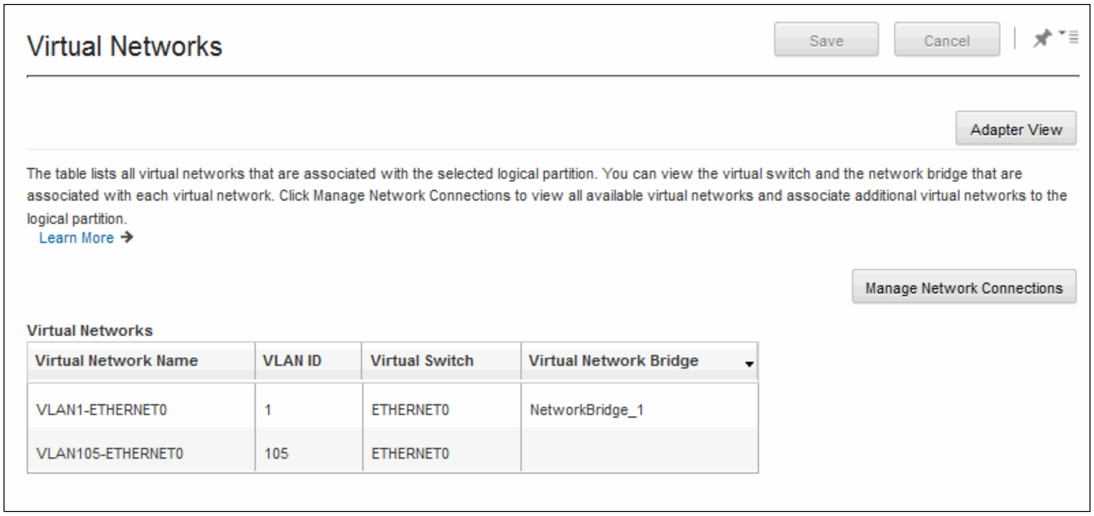
The table lists all virtual networks that are discovered by the managed system. You can add or remove the virtual networks that are associated with the logical partition. Select or clear the check box in the Connected column to add or remove the virtual networks. You can also view and assign new virtual Ethernet adapters.

□ Show and assign new virtual ethernet adapters

Connected	Virtual Network Name	VLAN ID	Virtual Switch	Virtual Network Bridge
□	VLAN99-ETHERNET0	99	ETHERNET0	
☑	VLAN1-ETHERNET0	1	ETHERNET0	NetworkBridge_1
□	VLAN4-ETHERNET0	4	ETHERNET0	
☑	VLAN105-ETHERNET0	105	ETHERNET0	
□	VLAN106-ETHERNET0	106	ETHERNET0	

Figure 5-102 Add a VLAN

The list of VLANs that are configured on the VIOS are displayed on the required network, or networks can be selected. Click **OK** to add them to the pending configuration changes and return to the window that is shown in Figure 5-103.



Virtual Networks

The table lists all virtual networks that are associated with the selected logical partition. You can view the virtual switch and the network bridge that are associated with each virtual network. Click Manage Network Connections to view all available virtual networks and associate additional virtual networks to the logical partition.

Virtual Networks

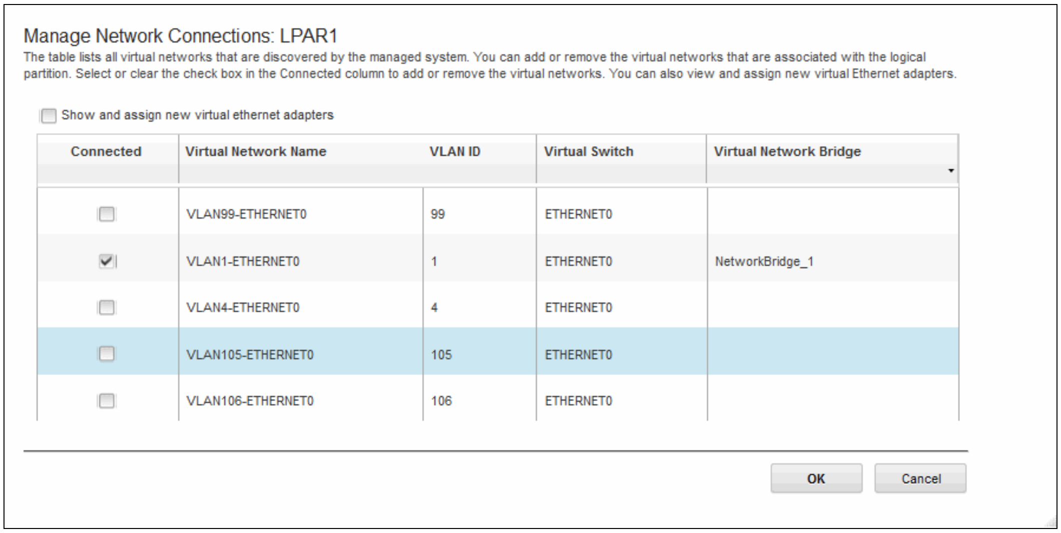
Virtual Network Name	VLAN ID	Virtual Switch	Virtual Network Bridge
VLAN1-ETHERNET0	1	ETHERNET0	NetworkBridge_1
VLAN105-ETHERNET0	105	ETHERNET0	

Figure 5-103 Configured VLAN after it is added

Click **OK** to add the adapters to the partition configuration. The HMC adds an adapter or adapters to the partition configuration.

5.8.2 Removing a VLAN

The process of removing a VLAN is similar to the process of adding a VLAN. Click **Virtual Networks** → **Manage Network Connections**. The window that opens lists all the configured networks on the partition (Figure 5-104). Select the VLAN you want o remove and click **OK**.



Manage Network Connections: LPAR1

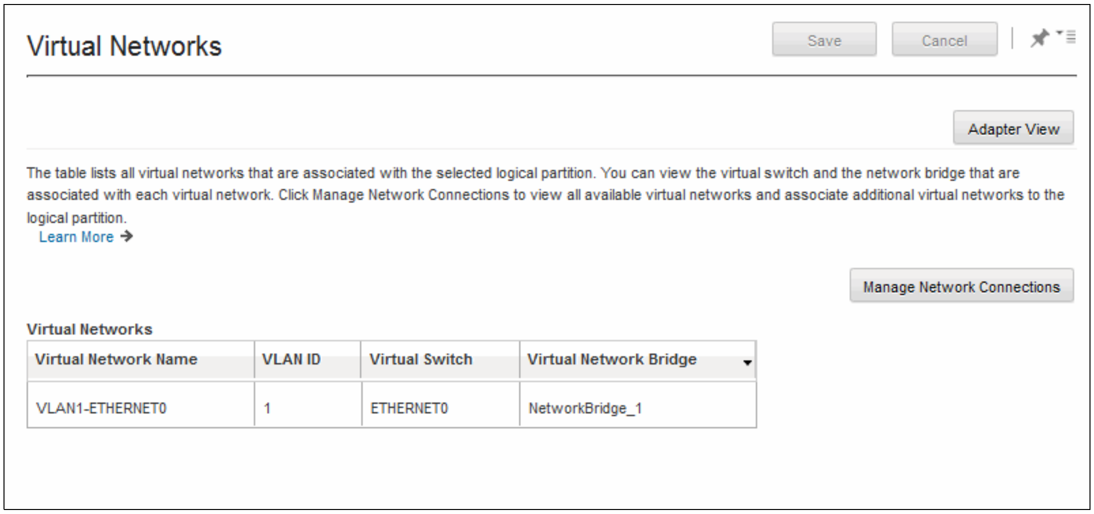
The table lists all virtual networks that are discovered by the managed system. You can add or remove the virtual networks that are associated with the logical partition. Select or clear the check box in the Connected column to add or remove the virtual networks. You can also view and assign new virtual Ethernet adapters.

□ Show and assign new virtual ethernet adapters

Connected	Virtual Network Name	VLAN ID	Virtual Switch	Virtual Network Bridge
□	VLAN99-ETHERNET0	99	ETHERNET0	
☑	VLAN1-ETHERNET0	1	ETHERNET0	NetworkBridge_1
□	VLAN4-ETHERNET0	4	ETHERNET0	
□	VLAN105-ETHERNET0	105	ETHERNET0	
□	VLAN106-ETHERNET0	106	ETHERNET0	

Figure 5-104 Remove VLAN

The Virtual Networks window is displayed again (Figure 5-105). Click **OK** to complete the removal of the VLAN, which also removes the adapter from the partition configuration.



Virtual Networks

The table lists all virtual networks that are associated with the selected logical partition. You can view the virtual switch and the network bridge that are associated with each virtual network. Click Manage Network Connections to view all available virtual networks and associate additional virtual networks to the logical partition.

Learn More →

Virtual Networks

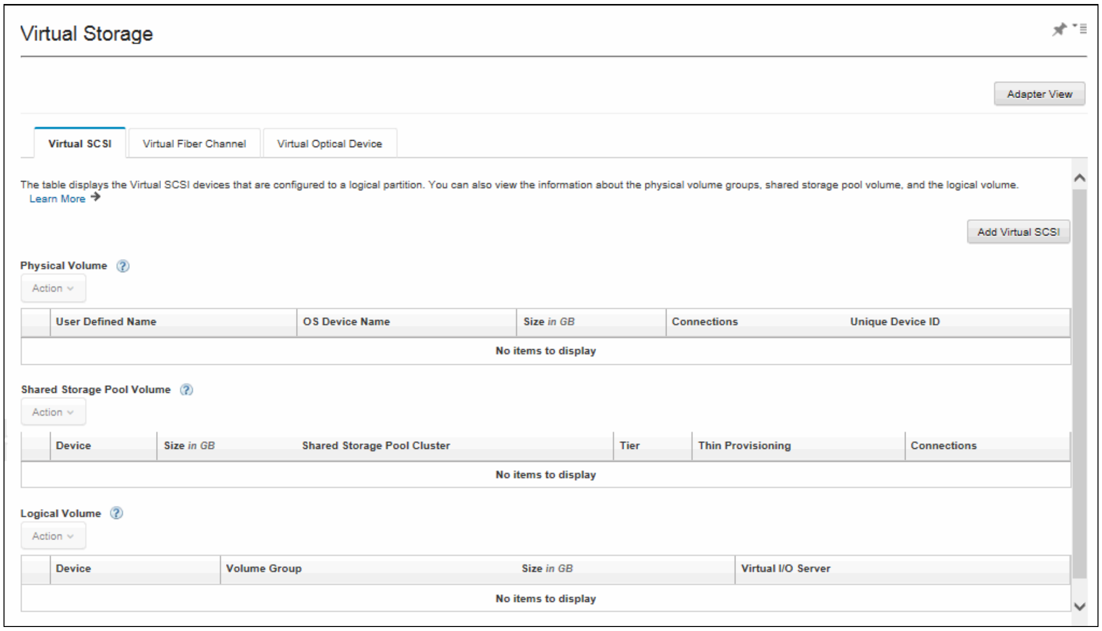
Virtual Network Name	VLAN ID	Virtual Switch	Virtual Network Bridge
VLAN1-ETHERNET0	1	ETHERNET0	NetworkBridge_1

Figure 5-105 Return to the Virtual Networks window

Note: The network configuration in the operating system must be removed from the adapter. The adapter resource and logical resources also must be removed from the operating system configuration or the removal operation fails.

5.9 Virtual Storage management

The UI has an updated virtual storage management window (Figure 5-106).



Virtual Storage

The table displays the Virtual SCSI devices that are configured to a logical partition. You can also view the information about the physical volume groups, shared storage pool volume, and the logical volume.
Learn More →

Physical Volume

	User Defined Name	OS Device Name	Size *in GB*	Connections	Unique Device ID
		No items to display			

Shared Storage Pool Volume

	Device	Size *in GB*	Shared Storage Pool Cluster	Tier	Thin Provisioning	Connections
			No items to display			

Logical Volume

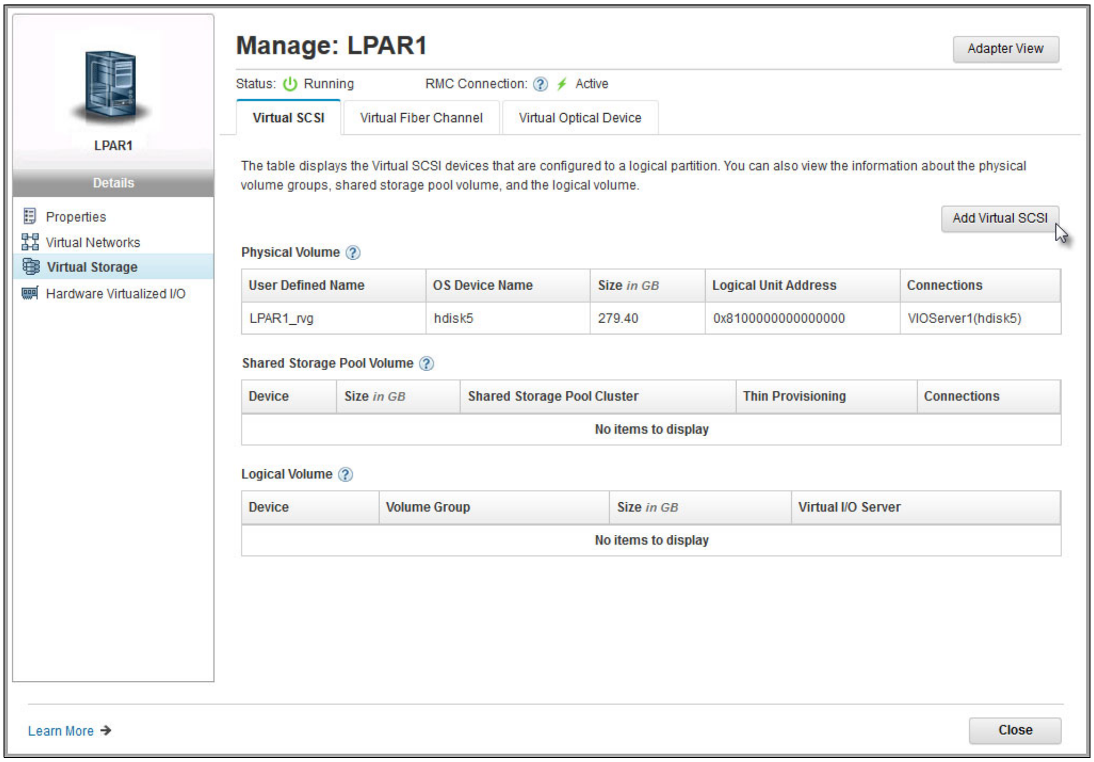
	Device	Volume Group	Size *in GB*	Virtual I/O Server
			No items to display	

Figure 5-106 Updated virtual storage window

Use this window to see the currently assigned storage and the mapping on the VIOS. You can also add and remove storage from the partition and load or unload any virtual optical devices that are assigned to the partition.

5.9.1 Allocation of a physical volume

To add a new virtual storage device, click **Add Virtual SCSI** on the Virtual Storage window, as shown in Figure 5-107.



The table displays the Virtual SCSI devices that are configured to a logical partition. You can also view the information about the physical volume groups, shared storage pool volume, and the logical volume.

Physical Volume

User Defined Name	OS Device Name	Size *in GB*	Logical Unit Address	Connections
LPAR1_rvg	hdisk5	279.40	0x8100000000000000	VIOServer1(hdisk5)

Shared Storage Pool Volume

Device	Size *in GB*	Shared Storage Pool Cluster	Thin Provisioning	Connections
No items to display				

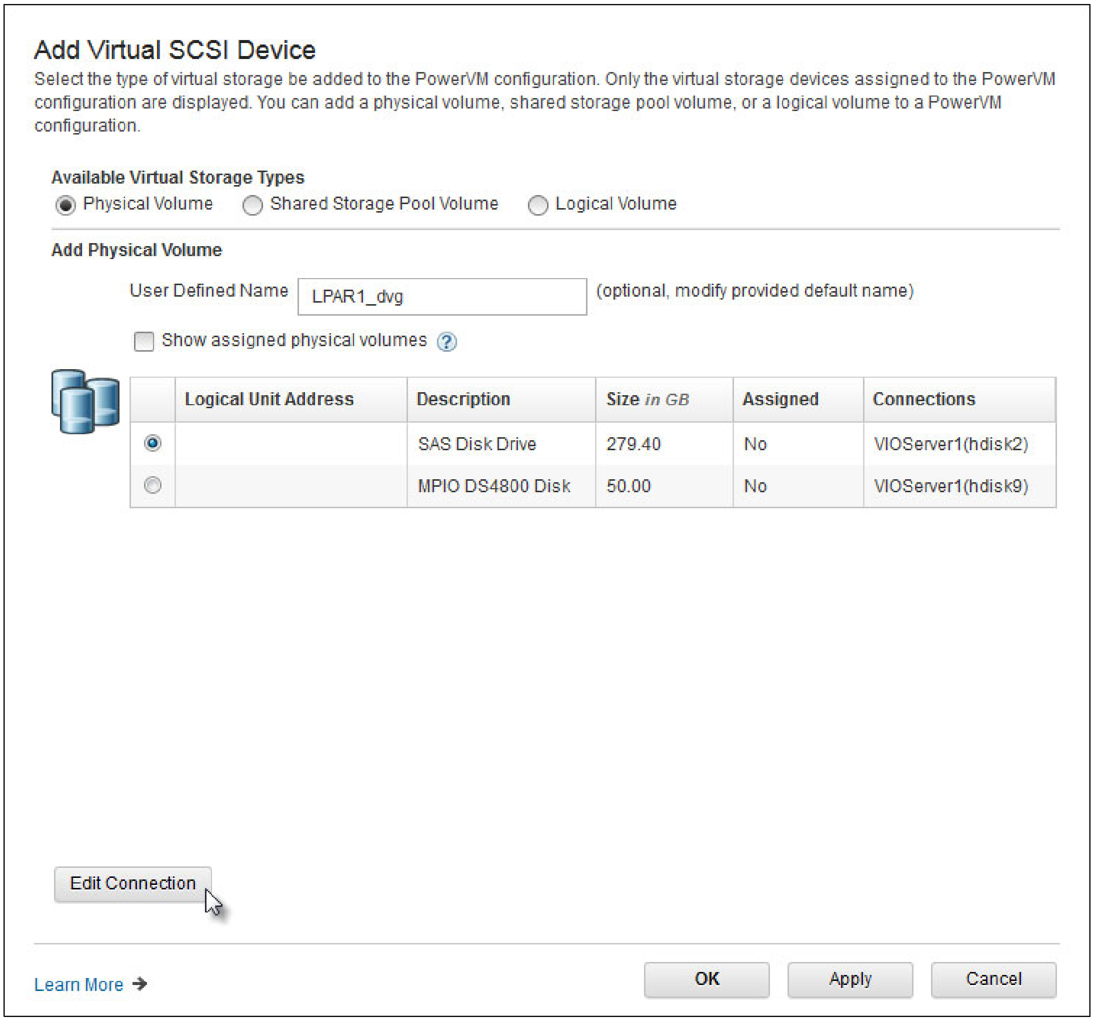
Logical Volume

Device	Volume Group	Size *in GB*	Virtual I/O Server
No items to display			

Figure 5-107 Add Virtual SCSI window

The Add Virtual SCSI Device window opens (Figure 5-108 on page 384). To add a physical volume, select **Physical Volume** in the Available Virtual Storage Types section. A list of the available volumes with a description about the device, its capacity, and which VIOS it is attached to is displayed.

Figure 5-108 shows that the SAS Disk Drive is configured and has the name LPAR1_dvg.



Add Virtual SCSI Device

Select the type of virtual storage be added to the PowerVM configuration. Only the virtual storage devices assigned to the PowerVM configuration are displayed. You can add a physical volume, shared storage pool volume, or a logical volume to a PowerVM configuration.

Available Virtual Storage Types

● Physical Volume ○ Shared Storage Pool Volume ○ Logical Volume

Add Physical Volume

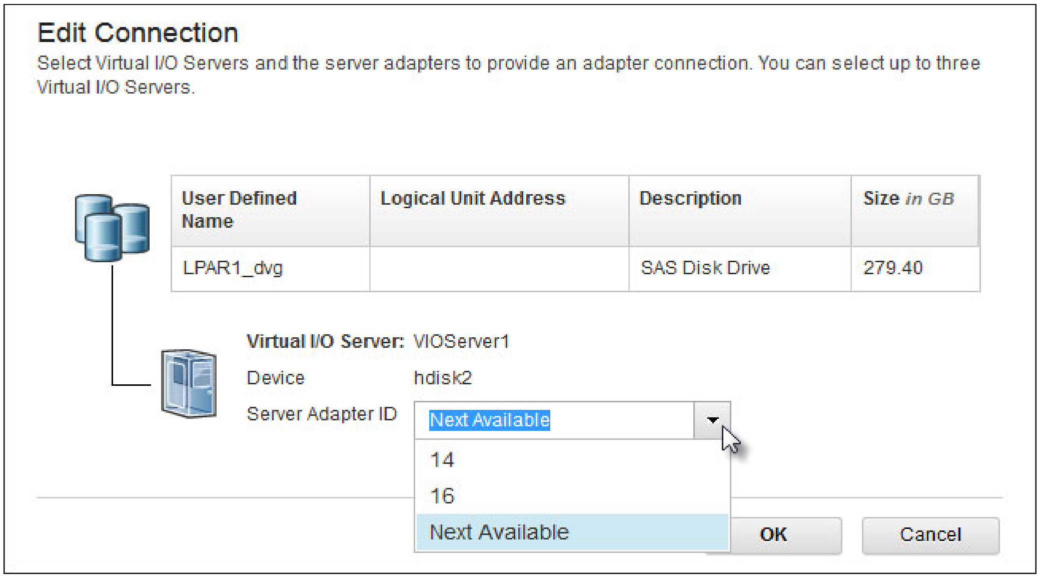
User Defined Name: LPAR1_dvg (optional, modify provided default name)

□ Show assigned physical volumes

	Logical Unit Address	Description	Size *in GB*	Assigned	Connections
●		SAS Disk Drive	279.40	No	VIOServer1(hdisk2)
○		MPIO DS4800 Disk	50.00	No	VIOServer1(hdisk9)

Figure 5-108 Physical storage device selected and named

The default action for the mapping is to create a virtual SCSI server adapter and map the device to that adapter. You can view this mapping and change the virtual adapter that is used to present the device to the client partition. To do this action, click **Edit Connection**, which opens the Edit Connection window (Figure 5-109).



Edit Connection

Select Virtual I/O Servers and the server adapters to provide an adapter connection. You can select up to three Virtual I/O Servers.

User Defined Name	Logical Unit Address	Description	Size *in GB*
LPAR1_dvg		SAS Disk Drive	279.40

Virtual I/O Server: VIOServer1

Device hdisk2

Server Adapter ID: Next Available

Figure 5-109 Adapter selection

In Figure 5-109, the default action **Next Available** is selected. Two other virtual SCSI adapters are listed and can be selected by clicking the drop-down list and selecting the adapter from the list. Click **OK** to accept the connection, which returns you to the previous window. Click **OK** in that window also.

If you do select **Next Available** adapter, a virtual SCSI adapter is created on the VIOS and the mapping is made between the physical disk and the virtual SCSI adapter. A virtual SCSI adapter also is created on the client partition, with the required settings to enable a connection to the virtual SCSI server adapter. If an existing virtual SCSI server adapter is chosen, the physical disk is mapped to that adapter. Run the `cfgmgr` command on the client partition to make the new disk available for use.

5.9.2 Allocation of a Shared Storage Pool volume

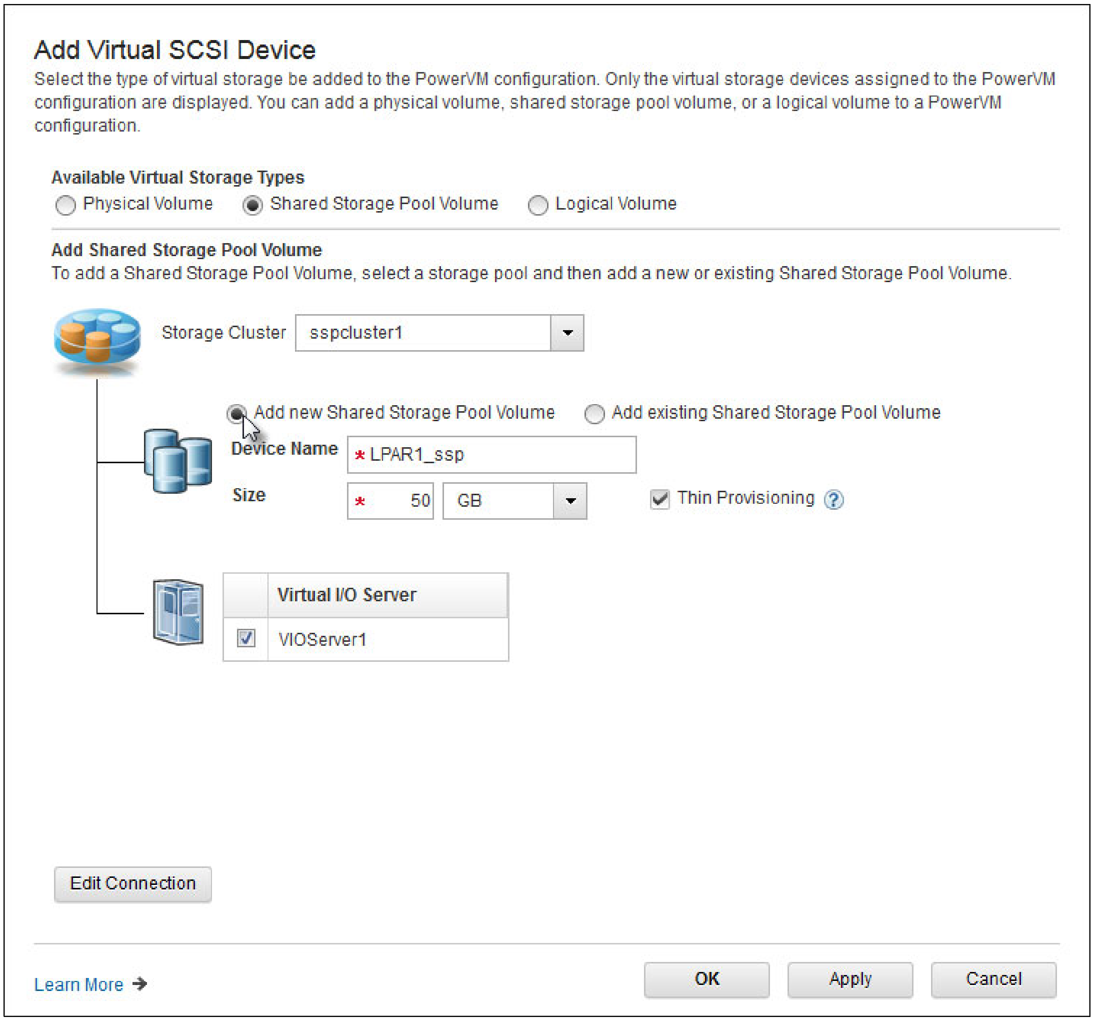
The process to allocate a Shared Storage Pool volume is nearly the same as the process that is described in 5.9.1, “Allocation of a physical volume” on page 383. However, in this section, only the changes are highlighted.

To access the Shared Storage Pool window, click **Add Virtual SCSI** from the Storage Management window, as shown in Figure 5-107 on page 383.

The following options are now available:

- Add new Shared Storage Pool Volume
- Add existing Shared Storage Pool volume

To create a Shared Storage Pool volume, click **Add new Shared Storage Pool Volume**, (Figure 5-110).



Add Virtual SCSI Device

Select the type of virtual storage be added to the PowerVM configuration. Only the virtual storage devices assigned to the PowerVM configuration are displayed. You can add a physical volume, shared storage pool volume, or a logical volume to a PowerVM configuration.

Available Virtual Storage Types

○ Physical Volume ● Shared Storage Pool Volume ○ Logical Volume

Add Shared Storage Pool Volume

To add a Shared Storage Pool Volume, select a storage pool and then add a new or existing Shared Storage Pool Volume.

Storage Cluster: sspcluster1

● Add new Shared Storage Pool Volume ○ Add existing Shared Storage Pool Volume

Device Name: * LPAR1_ssp

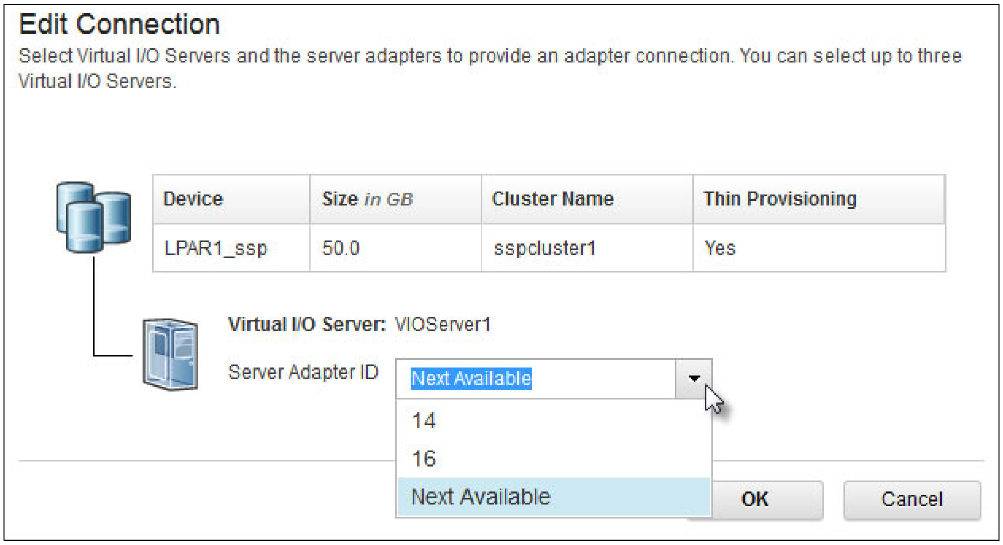
Size: * 50 GB ☑ Thin Provisioning

	Virtual I/O Server
☑	VIOServer1

Figure 5-110 Add a Shared Storage Pool volume

This window shows the details of which Storage Cluster to use, the name and size of the volume, and which VIOS to use. To change the virtual SCSI connection, click **Edit Connection**.

The Edit Connection window opens (Figure 5-111).



Edit Connection

Select Virtual I/O Servers and the server adapters to provide an adapter connection. You can select up to three Virtual I/O Servers.

Device	Size *in GB*	Cluster Name	Thin Provisioning
LPAR1_ssp	50.0	sspcluster1	Yes

Virtual I/O Server: VIOServer1

Server Adapter ID: Next Available

Figure 5-111 Adapter selection

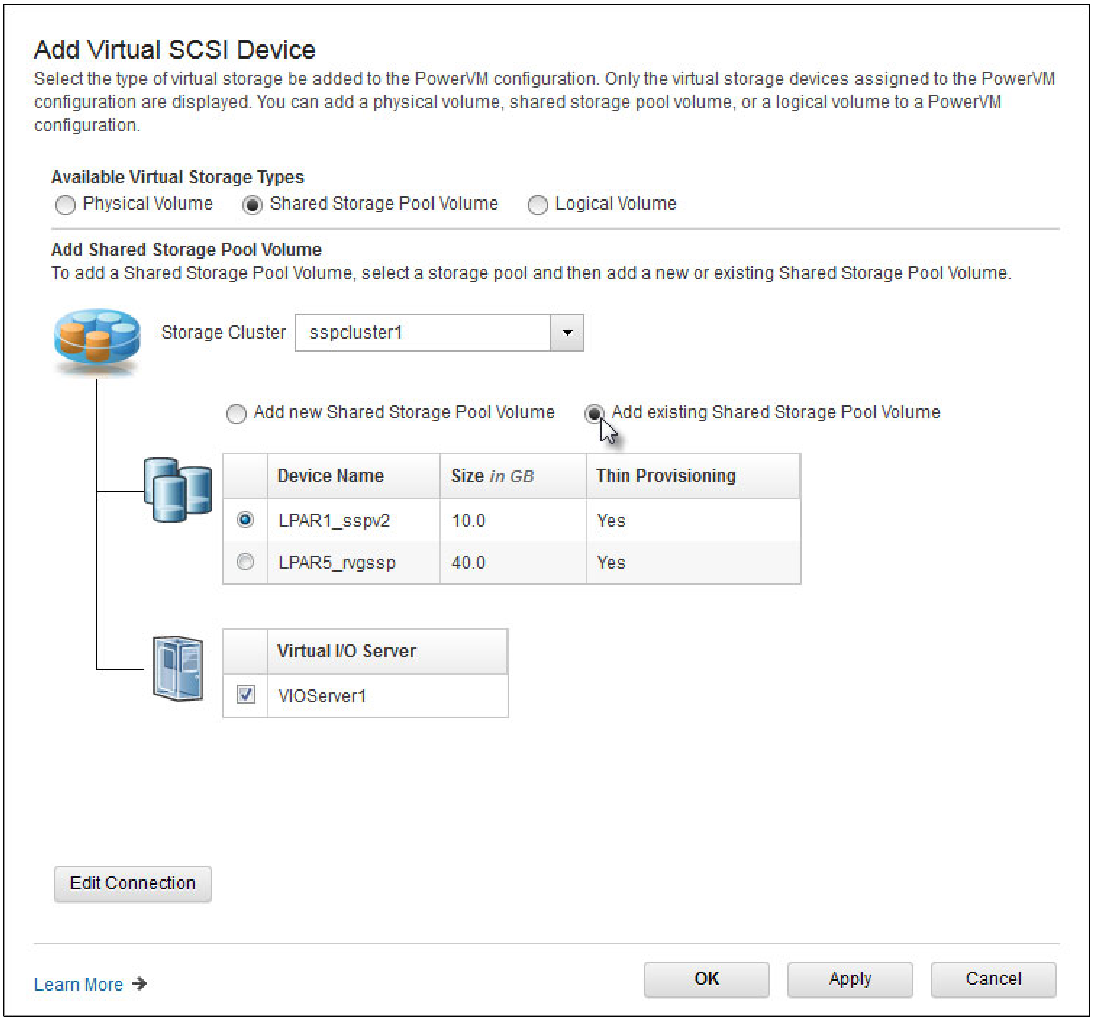
The default action, **Next Available**, is selected. In this example, two other adapters in the list can be selected. Click **OK** to return to the previous window if this is the only volume to be added and then click **OK** again; otherwise, click **Apply** and enter the required details for additional volumes.

After all the required volumes are added, click **OK** to complete the volume addition task.

In this example, only one volume was created and the default option for the connection was used. A volume is created in the specified Shared Storage Pool, and a new virtual SCSI adapter is added by using dynamic partitioning to the VIOS. The connection between the volume and the virtual SCSI adapter is created and a new adapter is added to the client partition.

To use an existing volume, use the same procedure, but click **Add Virtual SCSI** → **Shared Storage Pool Volume** and then click **Add existing Shared Storage Pool volume**, as shown in Figure 5-112. In this window, you can select an existing volume from the table of volumes. You can change the adapter connection by clicking **Edit Connection**. The default action is **Next Available**; if other adapters are available, they also are shown.

If this volume is the only one to be added, click **OK**; otherwise, click **Apply** and add more volumes as required.



Add Virtual SCSI Device

Select the type of virtual storage be added to the PowerVM configuration. Only the virtual storage devices assigned to the PowerVM configuration are displayed. You can add a physical volume, shared storage pool volume, or a logical volume to a PowerVM configuration.

Available Virtual Storage Types

○ Physical Volume ● Shared Storage Pool Volume ○ Logical Volume

Add Shared Storage Pool Volume

To add a Shared Storage Pool Volume, select a storage pool and then add a new or existing Shared Storage Pool Volume.

Storage Cluster: sspcluster1

○ Add new Shared Storage Pool Volume ● Add existing Shared Storage Pool Volume

	Device Name	Size *in GB*	Thin Provisioning
●	LPAR1_sspv2	10.0	Yes
○	LPAR5_rvgssp	40.0	Yes

	Virtual I/O Server
☑	VIOServer1

Figure 5-112 Existing volume selection

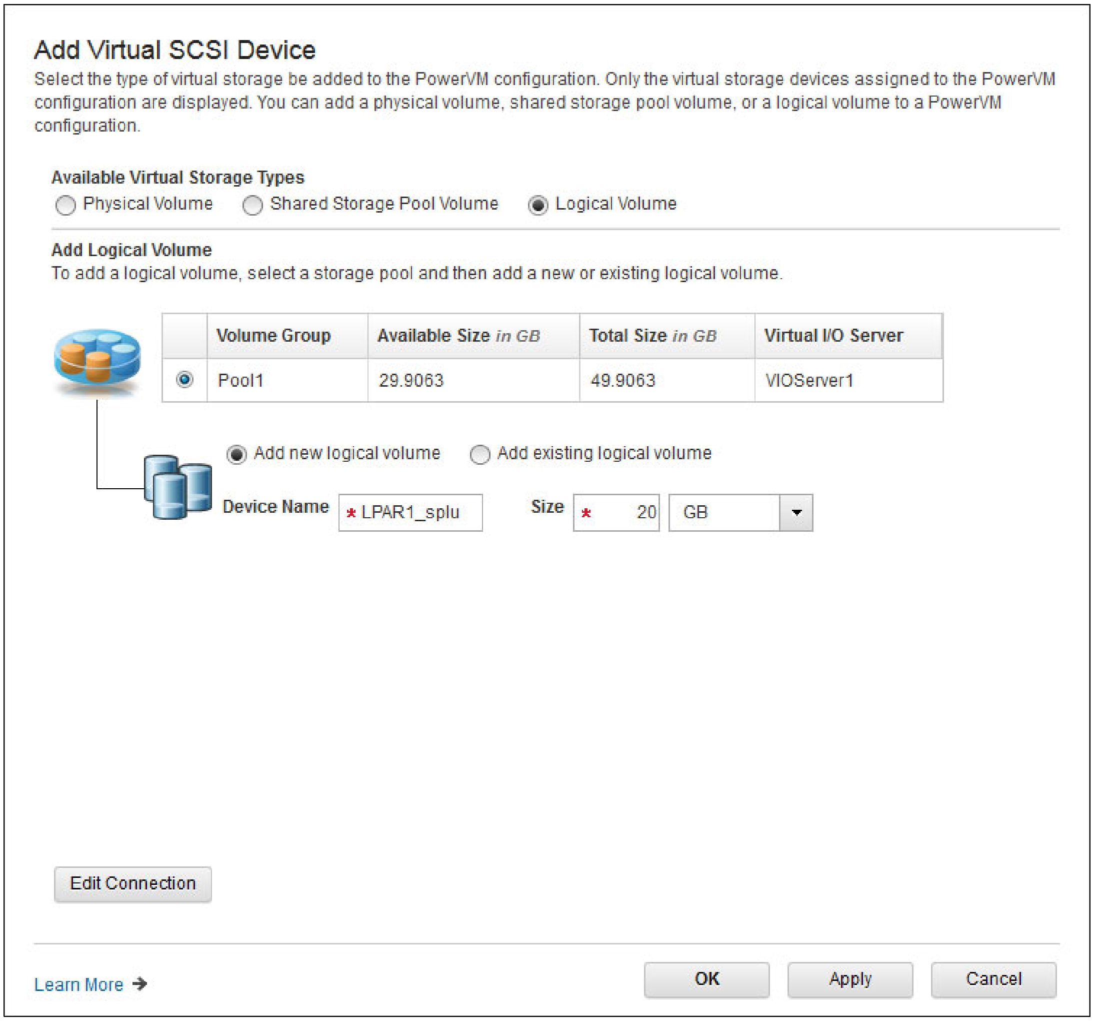
5.9.3 Allocation of a logical volume

The process to allocate a logical volume is nearly the same as the process that is described in 5.9.1, “Allocation of a physical volume” on page 383. Only the changes are highlighted in this section. To access the Logical Volume window, click **Add Virtual SCSI** in the window shown in Figure 5-107 on page 383.

Select **Logical Volume** (Figure 5-113). Two options are now available:

- Add new logical volume
- Add existing logical volume

Figure 5-113 shows the **Add new logical volume** option is selected.



Add Virtual SCSI Device

Select the type of virtual storage be added to the PowerVM configuration. Only the virtual storage devices assigned to the PowerVM configuration are displayed. You can add a physical volume, shared storage pool volume, or a logical volume to a PowerVM configuration.

Available Virtual Storage Types

○ Physical Volume ○ Shared Storage Pool Volume ● Logical Volume

Add Logical Volume

To add a logical volume, select a storage pool and then add a new or existing logical volume.

	Volume Group	Available Size *in GB*	Total Size *in GB*	Virtual I/O Server
●	Pool1	29.9063	49.9063	VIOServer1

● Add new logical volume ○ Add existing logical volume

Device Name * LPAR1_splu Size * 20 GB

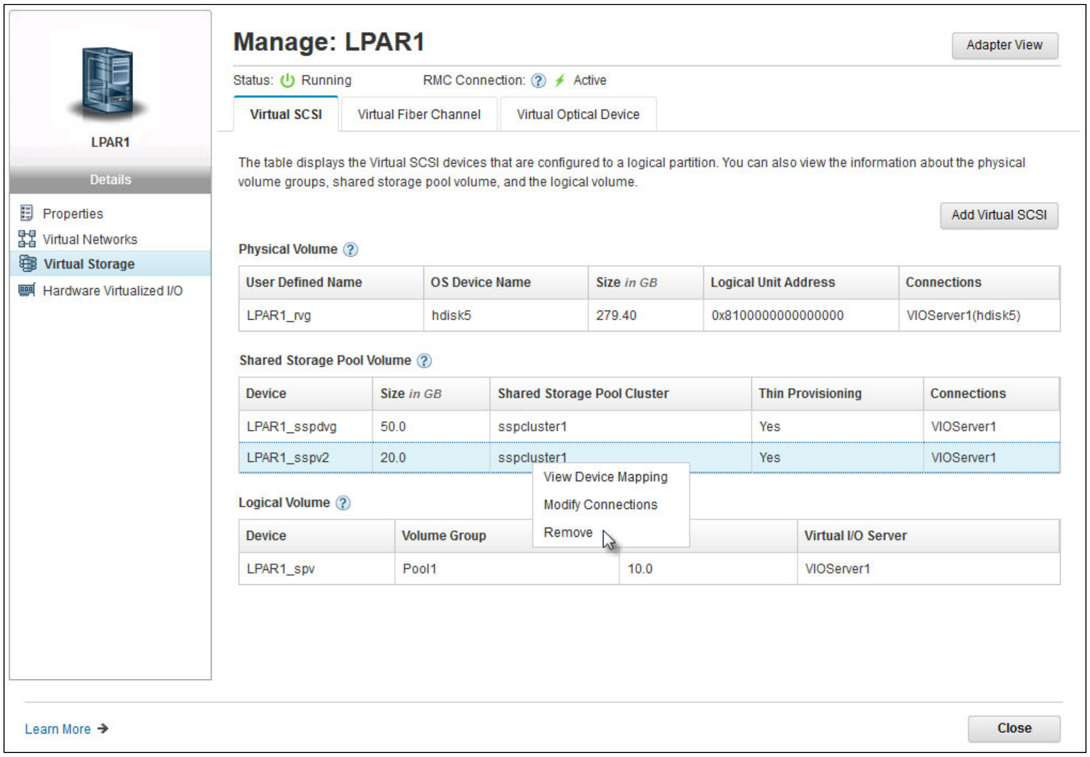
Figure 5-113 Add new logical volume option

The settings are the same for the logical volume as for the other volume options. The connection can be changed by clicking **Edit Connection**, which shows the same options as the other volume types.

5.9.4 Removing storage

The process to remove a volume is the same whether it is a physical volume, Shared Storage Pool volume, or logical volume.

To remove a volume, click **Virtual Storage** → **Virtual SCSI** and right-click the volume to be removed. The Manage window opens (Figure 5-114).



Manage: LPAR1

Status: Running RMC Connection: Active

The table displays the Virtual SCSI devices that are configured to a logical partition. You can also view the information about the physical volume groups, shared storage pool volume, and the logical volume.

Physical Volume

User Defined Name	OS Device Name	Size *in GB*	Logical Unit Address	Connections
LPAR1_rvg	hdisk5	279.40	0x8100000000000000	VIOServer1(hdisk5)

Shared Storage Pool Volume

Device	Size *in GB*	Shared Storage Pool Cluster	Thin Provisioning	Connections
LPAR1_sspdvg	50.0	sspcluster1	Yes	VIOServer1
LPAR1_sspv2	20.0	sspcluster1	Yes	VIOServer1

Logical Volume

Device	Volume Group		Virtual I/O Server
LPAR1_spv	Pool1	10.0	VIOServer1

Figure 5-114 Remove storage volume

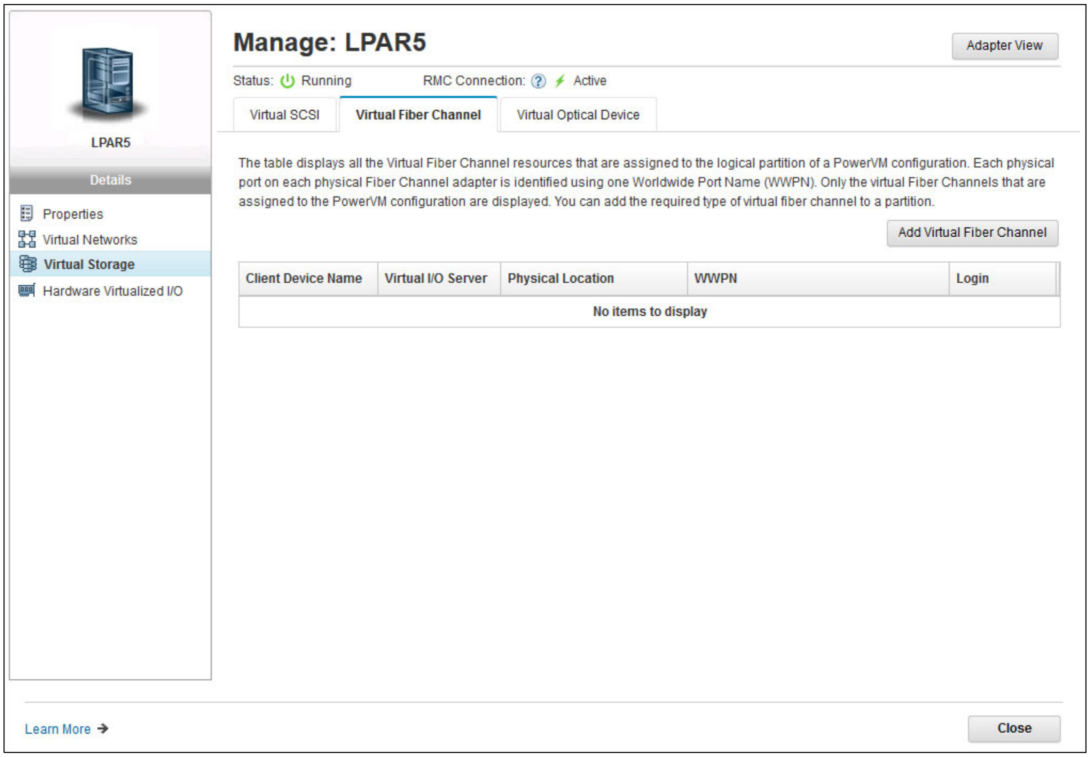
Click **Remove**, which removes the connection between the volume and the virtual SCSI server adapter. If the adapters in either the VIOS or client partition have no other connections, then the adapters will be removed. In the case of the Shared Storage Pool volumes, the volume also is removed from the Shared Storage Pool.

5.9.5 Allocation of a Fibre Channel Storage adapter

The process for adding Fibre Channel storage is similar to the process for adding a virtual SCSI device.

To access the Fibre Channel configuration, click **Virtual Storage** → **Virtual Fibre Channel**.

The Manage window opens (Figure 5-115). Click **Add Virtual Fibre Channel**.



Manage: LPAR5

Status: Running RMC Connection: Active

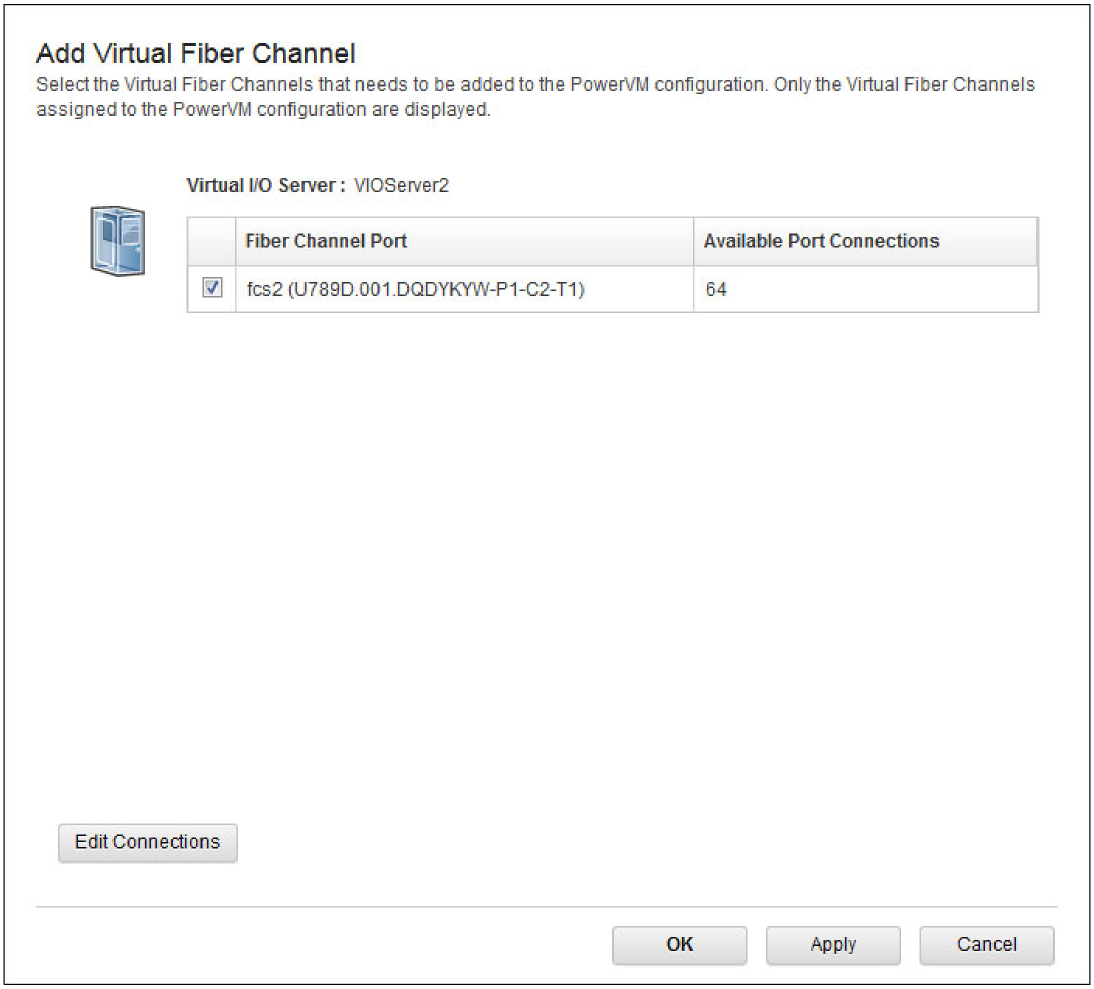
The table displays all the Virtual Fiber Channel resources that are assigned to the logical partition of a PowerVM configuration. Each physical port on each physical Fiber Channel adapter is identified using one Worldwide Port Name (WWPN). Only the virtual Fiber Channels that are assigned to the PowerVM configuration are displayed. You can add the required type of virtual fiber channel to a partition.

Client Device Name	Virtual I/O Server	Physical Location	WWPN	Login
No items to display				

Figure 5-115 Add Fibre Channel Storage adapter

The physical adapters that are available for a virtual Fibre Channel connection (in this example, `fcs2`) are listed (Figure 5-116).

Select the physical adapter that you will use for the virtual Fibre Channel connection and click **Edit Connection**.



Add Virtual Fiber Channel

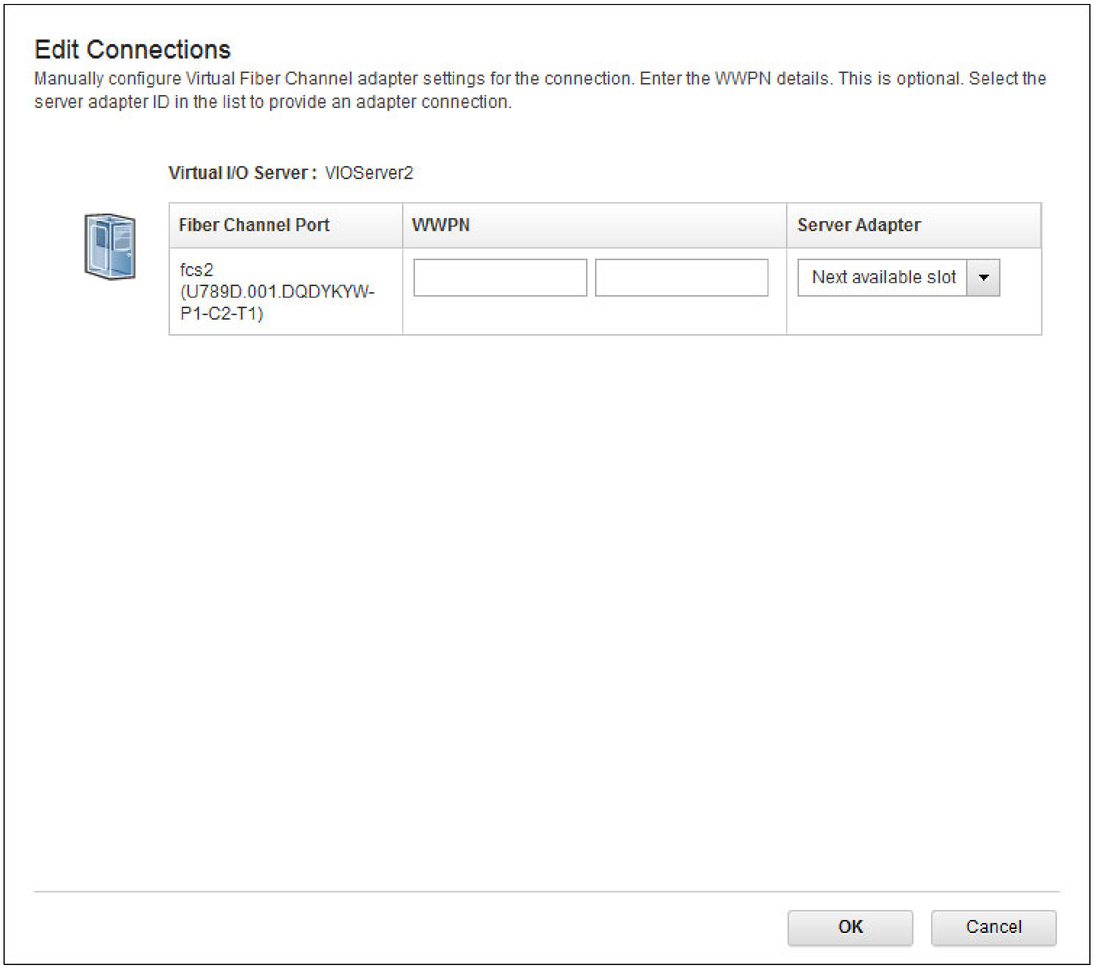
Select the Virtual Fiber Channels that needs to be added to the PowerVM configuration. Only the Virtual Fiber Channels assigned to the PowerVM configuration are displayed.

Virtual I/O Server : VIOServer2

	Fiber Channel Port	Available Port Connections
☑	fcs2 (U789D.001.DQDYKYW-P1-C2-T1)	64

Figure 5-116 Physical adapter selection

The Edit Connections window opens (Figure 5-117).



Edit Connections

Manually configure Virtual Fiber Channel adapter settings for the connection. Enter the WWPN details. This is optional. Select the server adapter ID in the list to provide an adapter connection.

Virtual I/O Server : VIOServer2

Fiber Channel Port	WWPN	Server Adapter
fcs2 (U789D.001.DQDYKYW-P1-C2-T1)		Next available slot

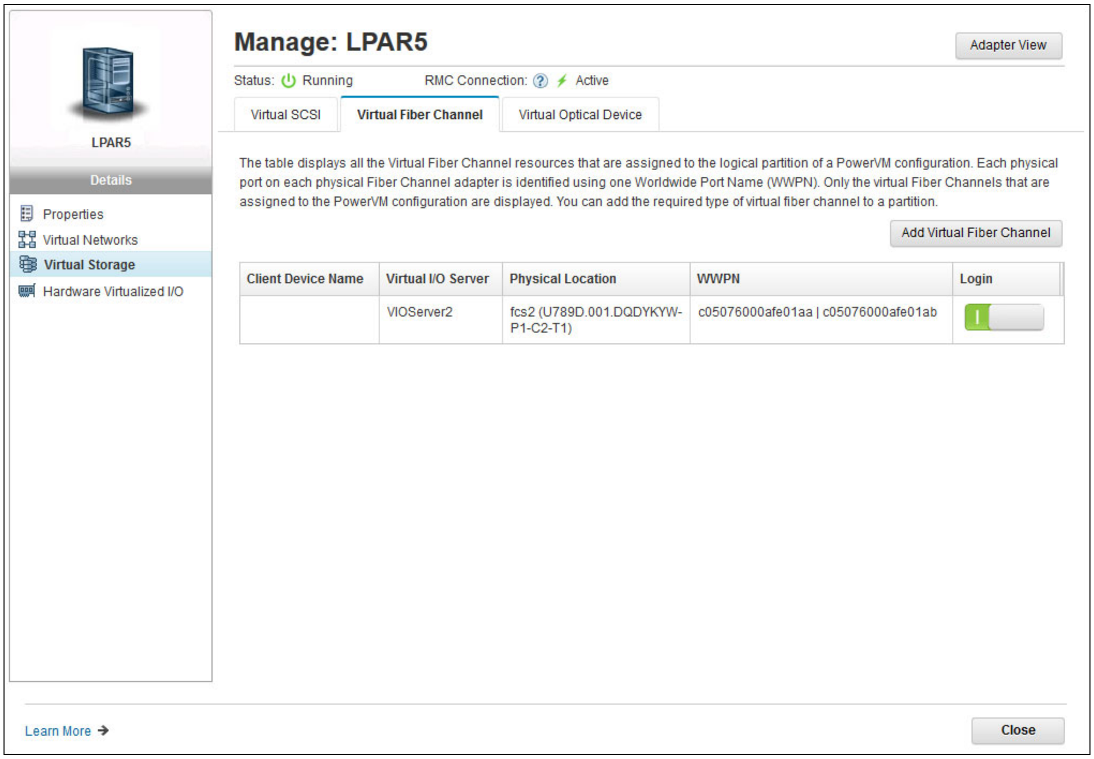
Figure 5-117 Adapter details

In this window, you can specify the worldwide port name (WWPN) that the adapter uses and the connection. Select either **Next available slot**, which creates an adapter, or select an existing adapter.

Click **OK** to return to the previous window, and then click **OK** again to configure the adapter.

If there are additional adapters to configure, click **Apply** and repeat the procedure to add additional adapters.

The configured adapters are now listed as shown in Figure 5-118.



Manage: LPAR5

Status: Running   RMC Connection: Active

The table displays all the Virtual Fiber Channel resources that are assigned to the logical partition of a PowerVM configuration. Each physical port on each physical Fiber Channel adapter is identified using one Worldwide Port Name (WWPN). Only the virtual Fiber Channels that are assigned to the PowerVM configuration are displayed. You can add the required type of virtual fiber channel to a partition.

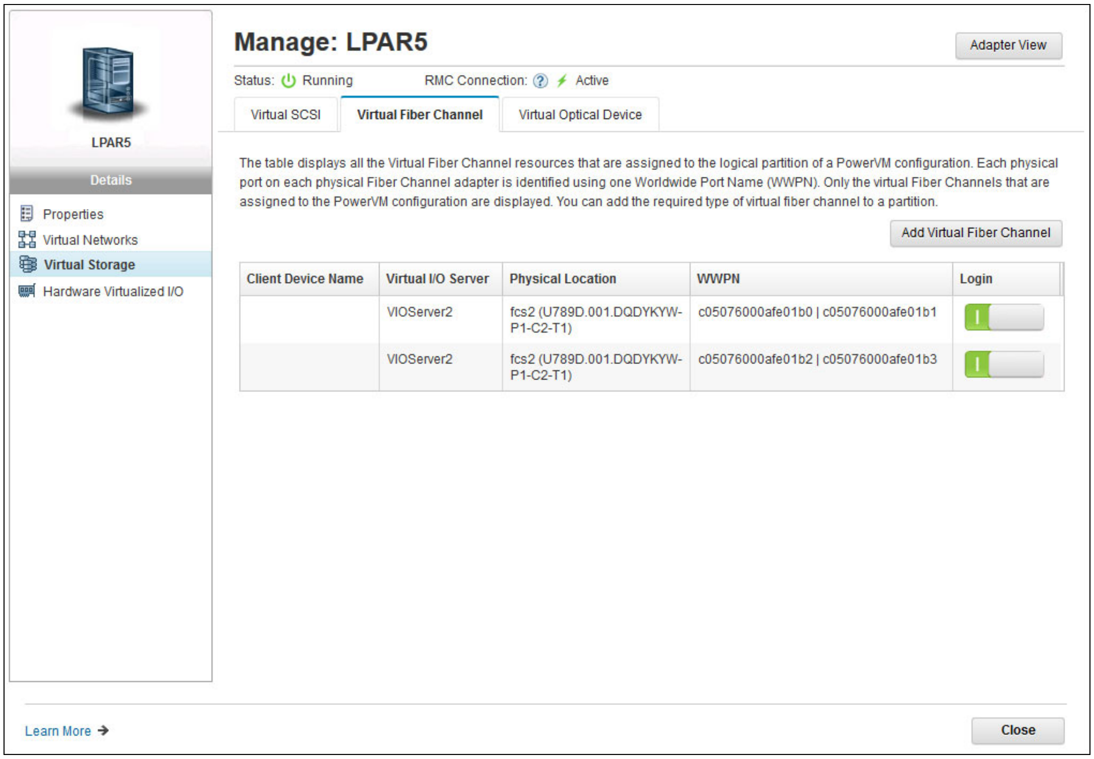
Client Device Name	Virtual I/O Server	Physical Location	WWPN	Login
	VIOServer2	fcs2 (U789D.001.DQDYKYW-P1-C2-T1)	c05076000afe01aa | c05076000afe01ab	I

Figure 5-118   Configured virtual Fibre Channel adapters

5.9.6 Removing a virtual Fibre Channel adapter

To remove a virtual Fibre Channel adapter, you must first unconfigure it and any child devices on the client partition. Then, you can click **Virtual Storage** → **Virtual Fibre Channel**.

The list looks like the one in Figure 5-119.



Manage: LPAR5

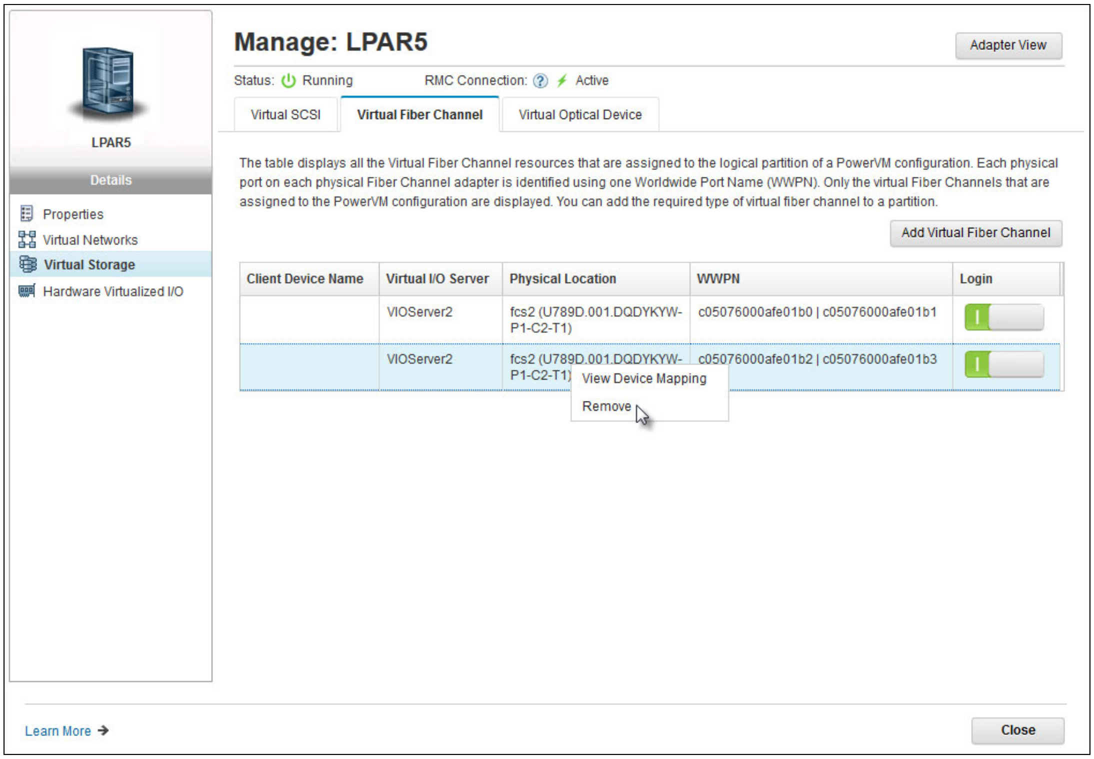
Status: Running RMC Connection: Active

The table displays all the Virtual Fiber Channel resources that are assigned to the logical partition of a PowerVM configuration. Each physical port on each physical Fiber Channel adapter is identified using one Worldwide Port Name (WWPN). Only the virtual Fiber Channels that are assigned to the PowerVM configuration are displayed. You can add the required type of virtual fiber channel to a partition.

Client Device Name	Virtual I/O Server	Physical Location	WWPN	Login
	VIOServer2	fcs2 (U789D.001.DQDYKYW-P1-C2-T1)	c05076000afe01b0 | c05076000afe01b1	I
	VIOServer2	fcs2 (U789D.001.DQDYKYW-P1-C2-T1)	c05076000afe01b2 | c05076000afe01b3	I

Figure 5-119 Configured virtual Fibre Channel adapters

In this window, right-click the adapter to remove and select **Remove** (Figure 5-120).



Manage: LPAR5

Status: Running RMC Connection: Active

The table displays all the Virtual Fiber Channel resources that are assigned to the logical partition of a PowerVM configuration. Each physical port on each physical Fiber Channel adapter is identified using one Worldwide Port Name (WWPN). Only the virtual Fiber Channels that are assigned to the PowerVM configuration are displayed. You can add the required type of virtual fiber channel to a partition.

Client Device Name	Virtual I/O Server	Physical Location	WWPN	Login
	VIOServer2	fcs2 (U789D.001.DQDYKYW-P1-C2-T1)	c05076000afe01b0 | c05076000afe01b1	I
	VIOServer2	fcs2 (U789D.001.DQDYKYW-P1-C2-T1)	c05076000afe01b2 | c05076000afe01b3	I

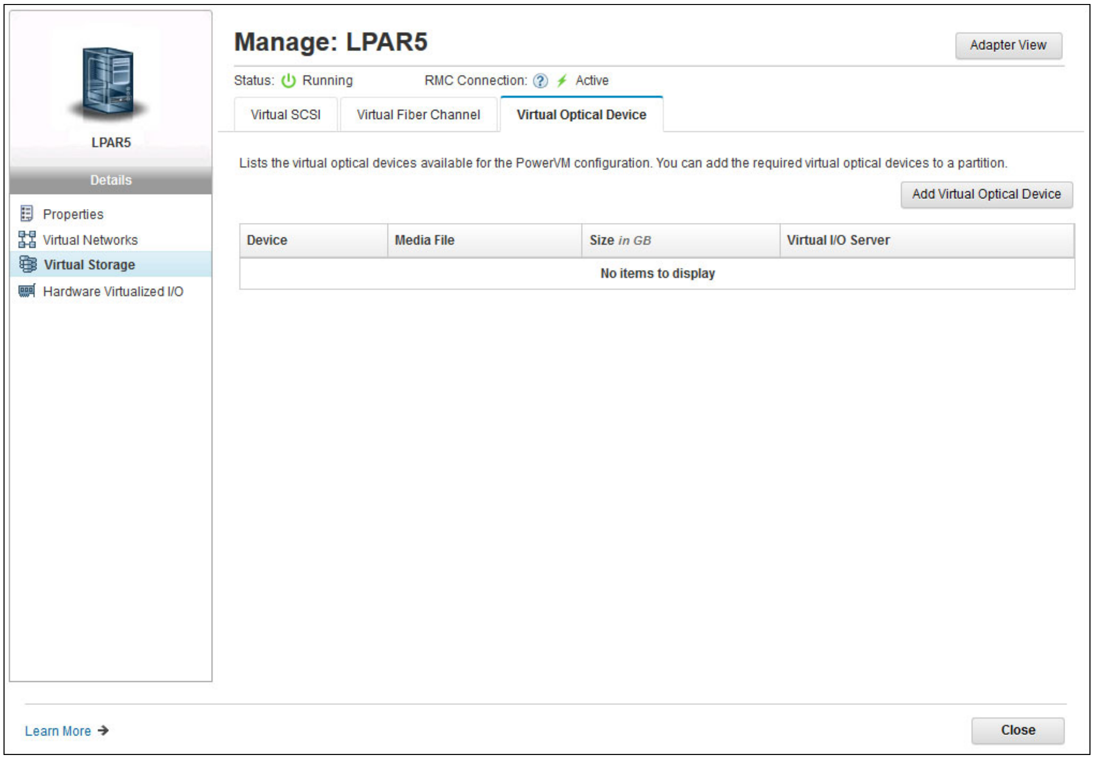
Figure 5-120 Fibre Channel adapter removal selected

The adapter is removed from the client partition. On the VIOS, the connection is removed between the physical Fibre Channel adapter and the virtual Fibre Channel adapter. The virtual Fibre Channel adapter then is removed from the VIOS configuration by using dynamic partitioning.

5.9.7 Virtual optical devices

Virtual optical devices can be added and removed by using the same process that is used for virtual SCSI devices.

To manage a virtual optical device, select **Virtual Storage** → **Virtual Optical Device**. The window that opens (Figure 5-121) shows the virtual optical devices that are assigned to the partition.



Manage: LPAR5

Status: Running RMC Connection: Active

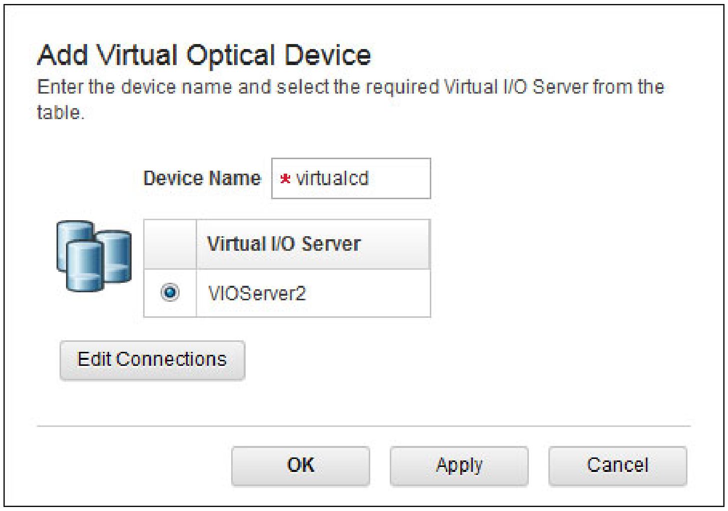
Lists the virtual optical devices available for the PowerVM configuration. You can add the required virtual optical devices to a partition.

Device	Media File	Size *in GB*	Virtual I/O Server
No items to display			

Figure 5-121 Virtual Optical Device window

Adding a new virtual optical device

To add a new virtual optical device, click **Add Virtual Optical Device**. The Add Virtual Optical Device window opens (Figure 5-122). The name of the device, VIOS, and the adapter that is used for connecting to the partition can be specified. To change the adapter connections, click **Edit Connections**.



Add Virtual Optical Device

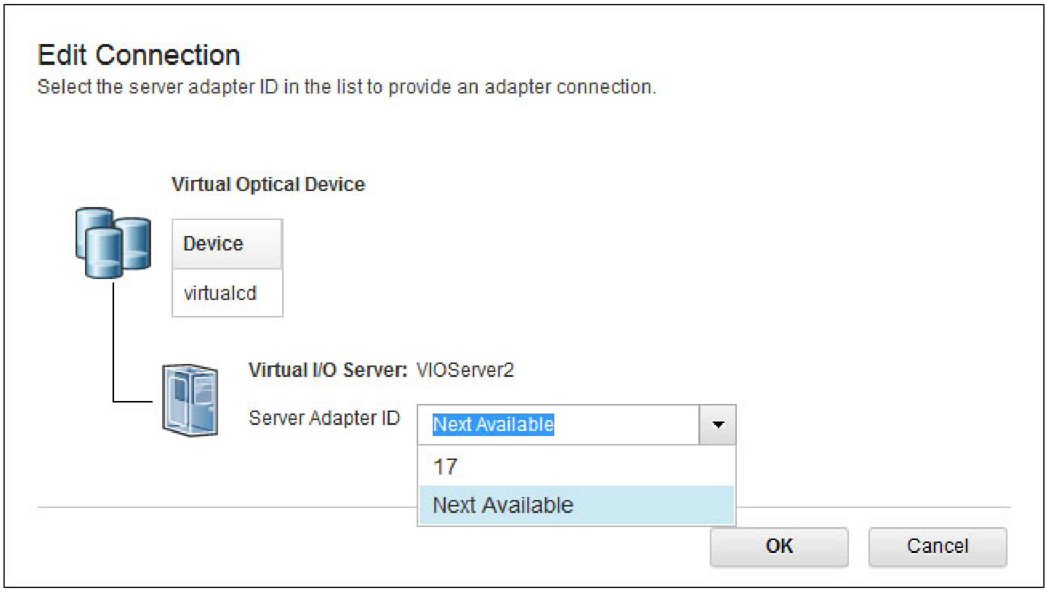
Enter the device name and select the required Virtual I/O Server from the table.

Device Name * virtualcd

	Virtual I/O Server
●	VIOServer2

Figure 5-122 Add Virtual Optical Device window

The Edit Connection window opens (Figure 5-123). As with the Virtual Storage, the default action is to add an adapter. Although, as shown in the figure, an adapter in slot 17 can be used for the connection, this example shows that **Next Available** is selected.



Edit Connection

Select the server adapter ID in the list to provide an adapter connection.

Virtual Optical Device

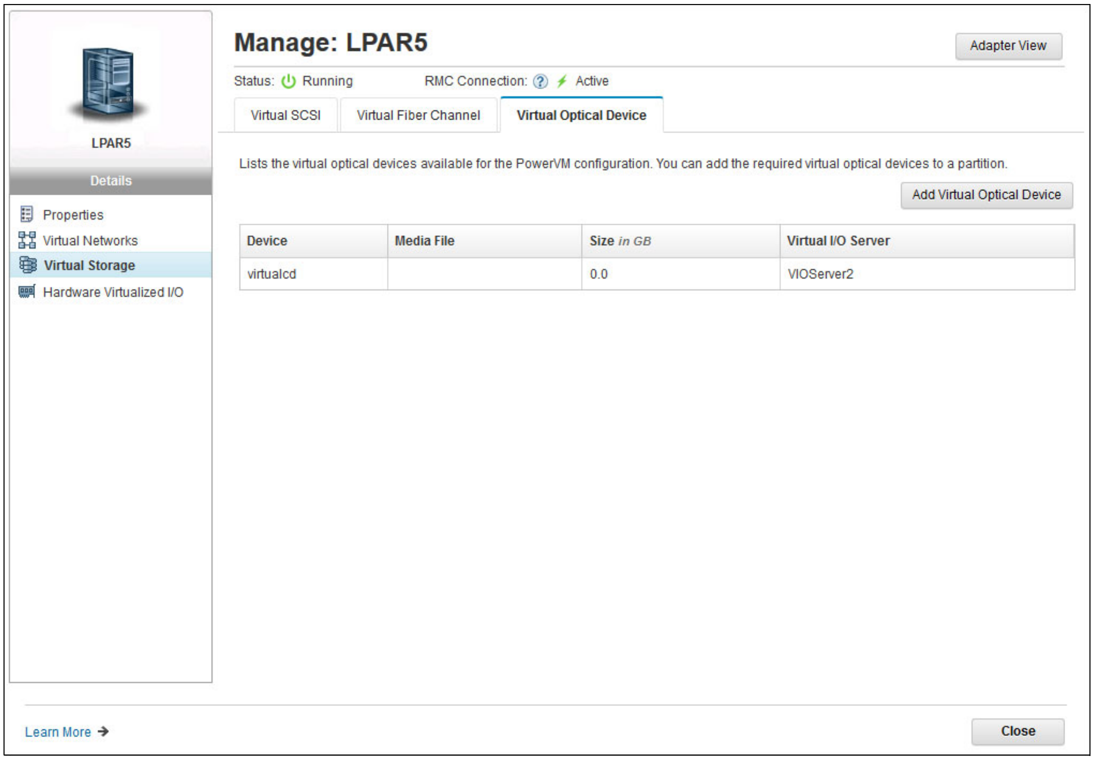
Device
virtualcd

Virtual I/O Server: VIOServer2

Server Adapter ID: Next Available

Figure 5-123 Edit connection

Click **OK** to add the new adapter connection and return to the window that is shown in Figure 5-122 on page 397. Click **OK**, which, if required, adds a new virtual SCSI adapter to the VIOS and the client partition, creates the file-backed optical device, and maps it to the specified adapter, as shown in Figure 5-124.



Manage: LPAR5

Status: Running RMC Connection: Active

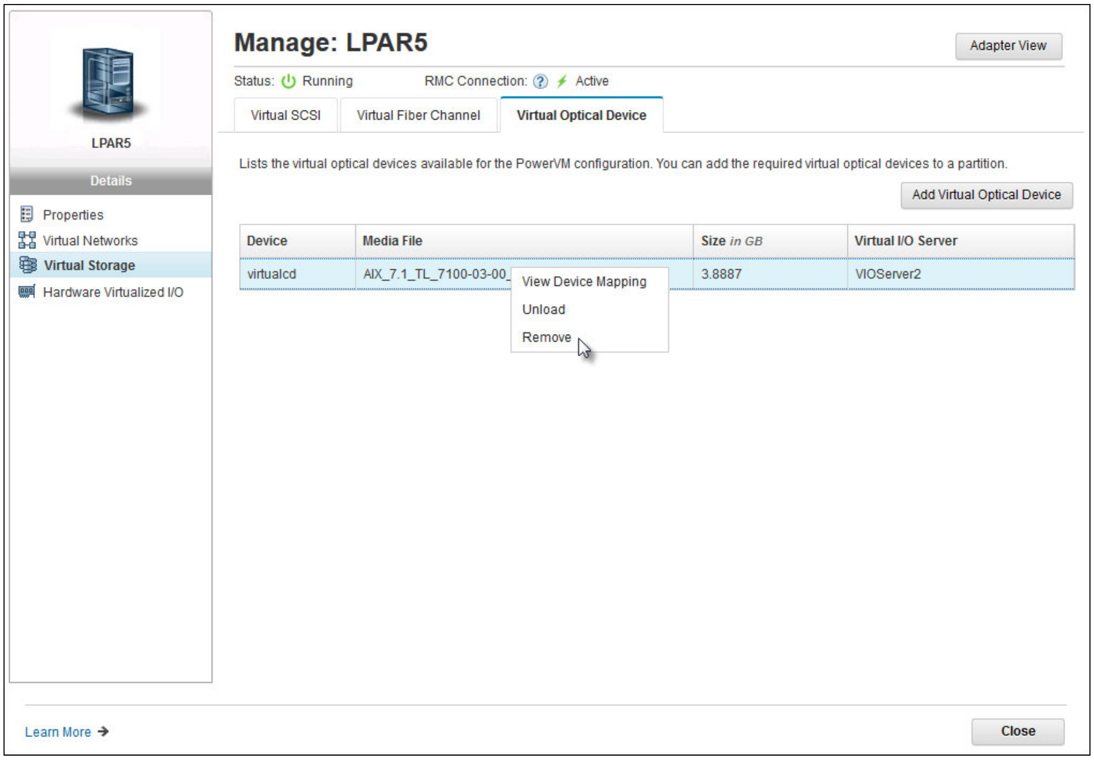
Lists the virtual optical devices available for the PowerVM configuration. You can add the required virtual optical devices to a partition.

Device	Media File	Size *in GB*	Virtual I/O Server
virtualcd		0.0	VIOServer2

Figure 5-124 New Virtual Optical Device

Removing a virtual optical device

To remove the virtual optical device, click **Virtual Storage** → **Virtual Optical Device** in the Manage partition window. The list of virtual optical devices that are allocated to the partition is displayed. Right-click the device to be removed and select **Remove** (Figure 5-125). This action removes the device from the partition, and if no other virtual devices are connected to the virtual SCSI adapter, this device is removed from the VIOS and the client partition.



Manage: LPAR5

Status: Running   RMC Connection: Active

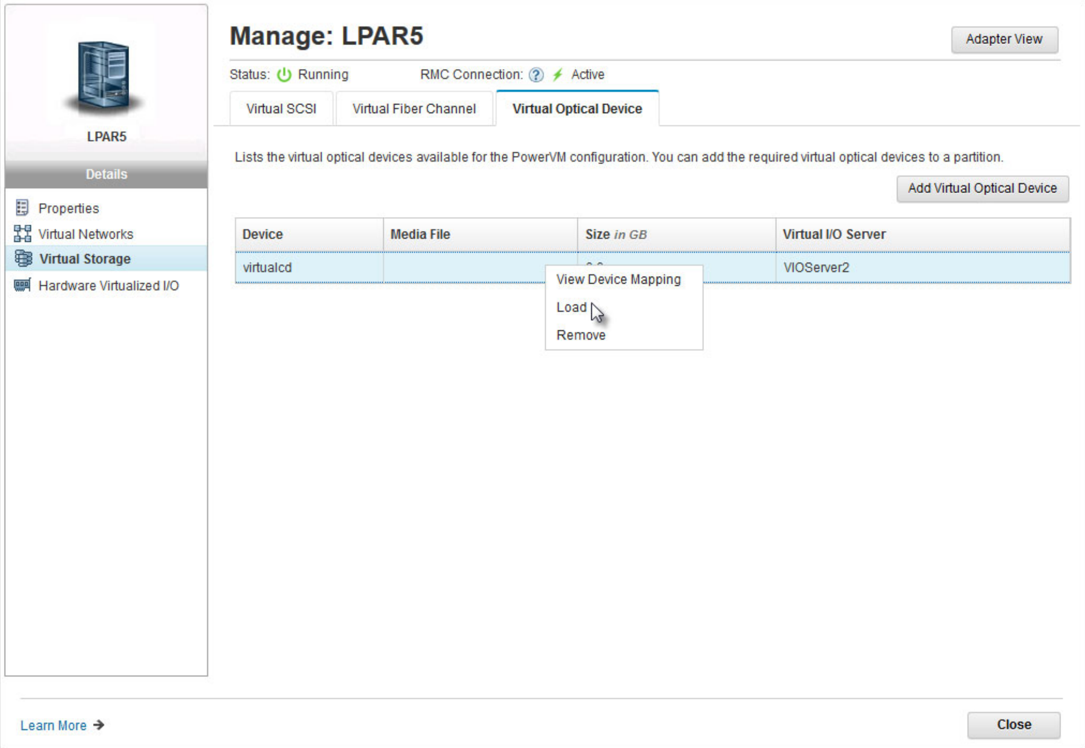
Lists the virtual optical devices available for the PowerVM configuration. You can add the required virtual optical devices to a partition.

Device	Media File	Size *in GB*	Virtual I/O Server
virtualcd	AIX_7.1_TL_7100-03-00_	3.8887	VIOServer2

Figure 5-125 Remove virtual optical device

Loading and unloading a virtual optical device

To load a virtual optical device, right-click the device and select **Load** (Figure 5-126).



Manage: LPAR5

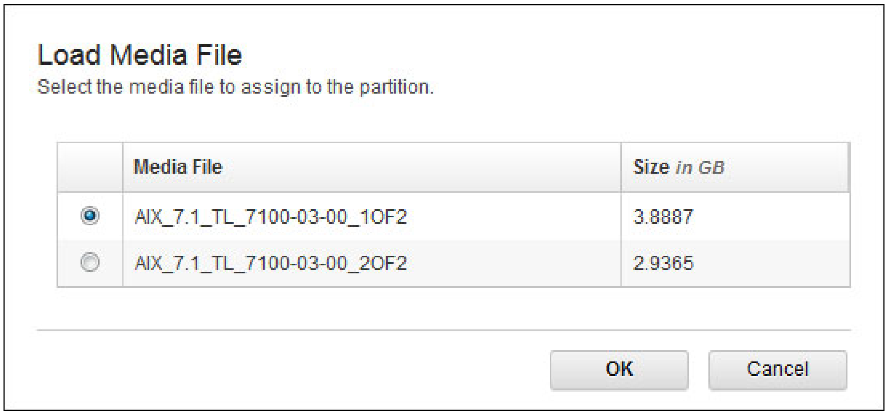
Status: Running RMC Connection: Active

Lists the virtual optical devices available for the PowerVM configuration. You can add the required virtual optical devices to a partition.

Device	Media File	Size *in GB*	Virtual I/O Server
virtualcd		0.0	VIOServer2

Figure 5-126 Load Virtual Optical Device

The media files in the repository on the VIOS are listed (Figure 5-127). Select a media file and click **OK**. This action loads the virtual optical device with the required media file.



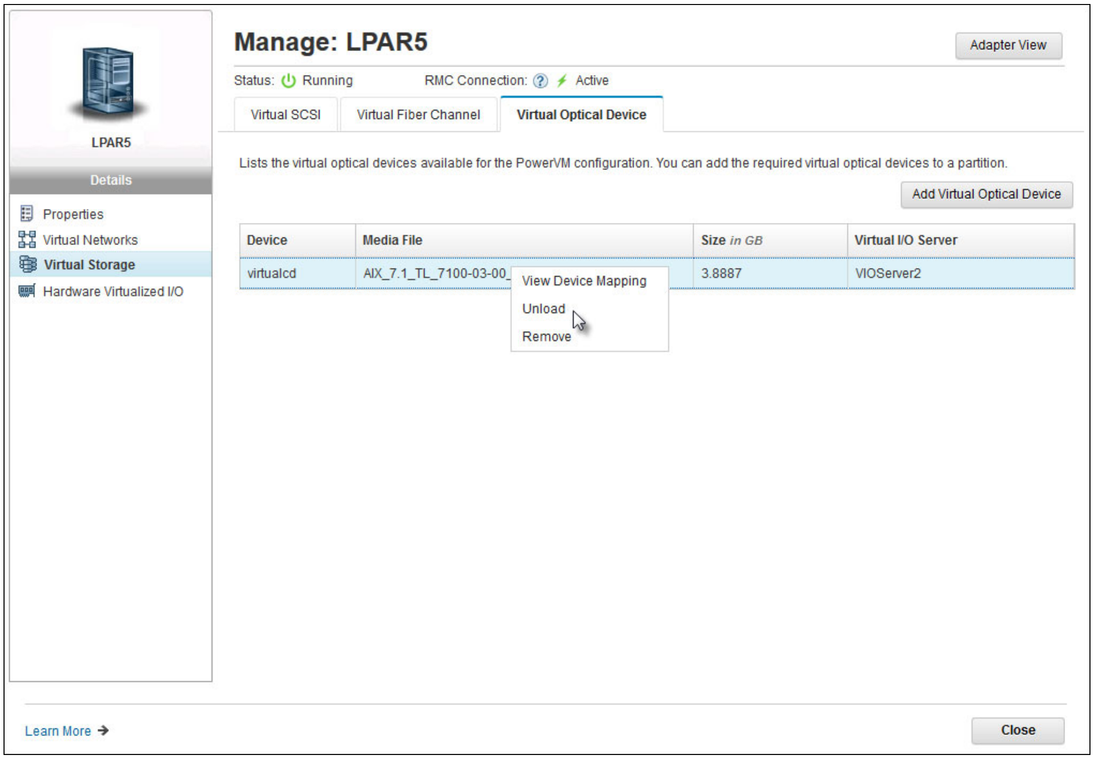
Load Media File

Select the media file to assign to the partition.

	Media File	Size *in GB*
●	AIX_7.1_TL_7100-03-00_1OF2	3.8887
○	AIX_7.1_TL_7100-03-00_2OF2	2.9365

Figure 5-127 Media file selection

To unload the virtual optical device, right-click the device and select **Unload** (Figure 5-128).



Manage: LPAR5

Status: Running RMC Connection: Active

Lists the virtual optical devices available for the PowerVM configuration. You can add the required virtual optical devices to a partition.

Device	Media File	Size *in GB*	Virtual I/O Server
virtualcd	AIX_7.1_TL_7100-03-00_	3.8887	VIOServer2

Figure 5-128 Unload virtual optical device

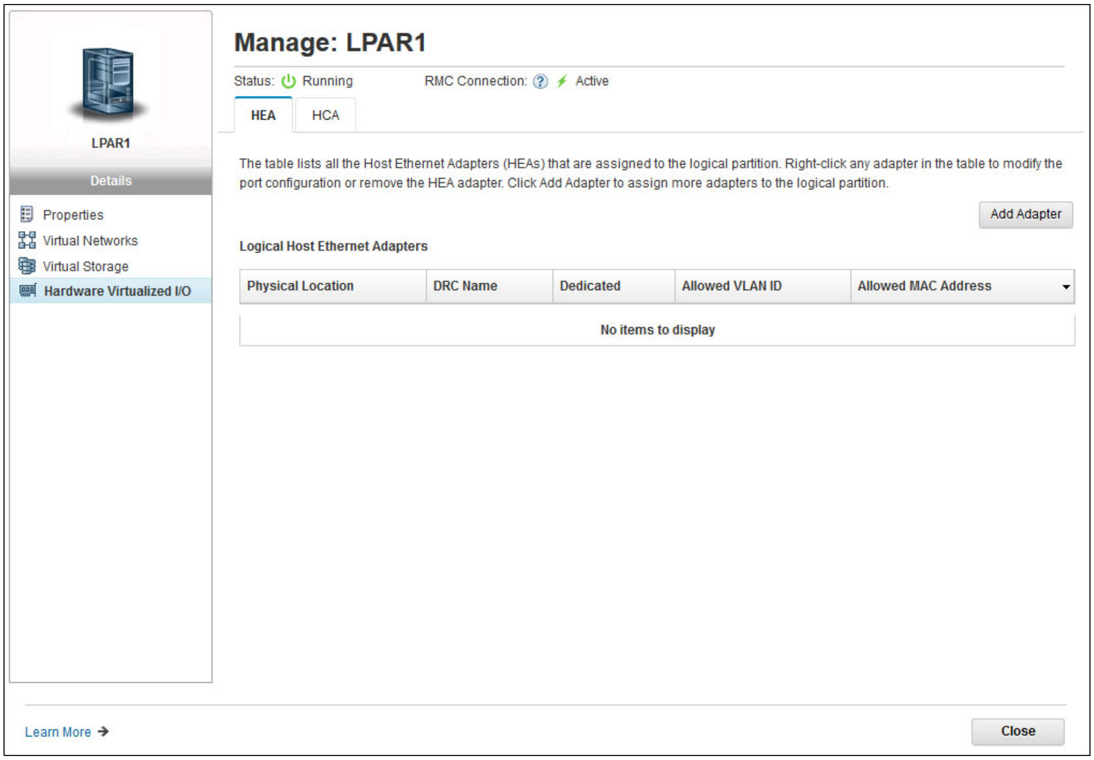
Note: The unload operation completes without error even if the virtual optical device is mounted on the client partition.

5.10 Managing hardware-virtualized I/O adapters

You can add, change, and remove logical host Ethernet ports from the partition configuration by using the Manage Partition function on the HMC.

5.10.1 Adding a logical host Ethernet port

To add a logical host Ethernet port, click **Add Adapter** (Figure 5-129).



Manage: LPAR1

Status: Running RMC Connection: Active

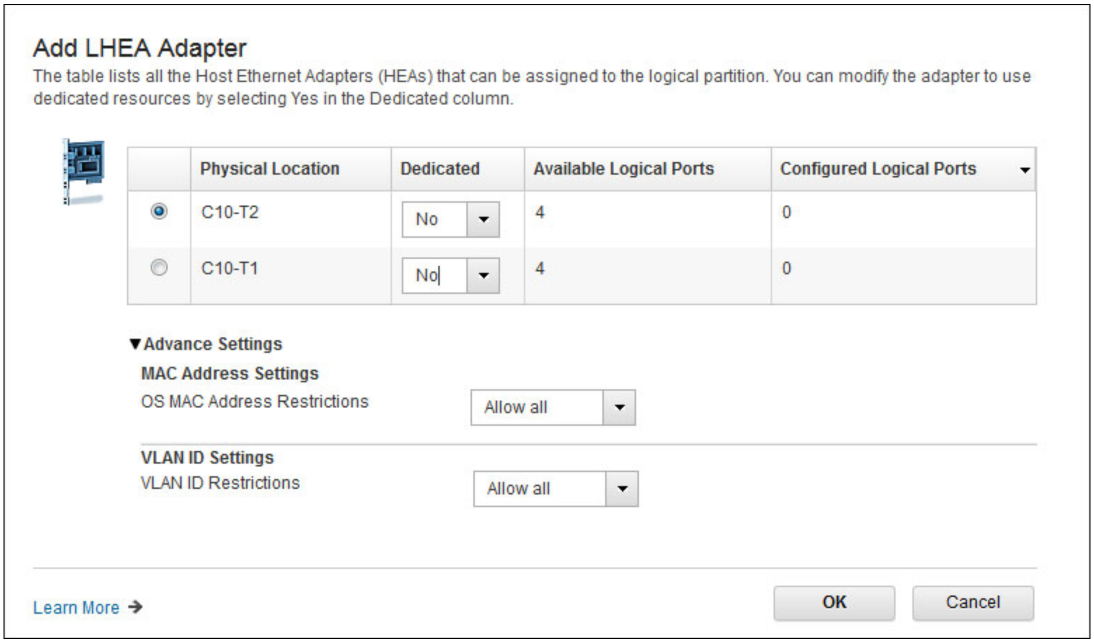
The table lists all the Host Ethernet Adapters (HEAs) that are assigned to the logical partition. Right-click any adapter in the table to modify the port configuration or remove the HEA adapter. Click Add Adapter to assign more adapters to the logical partition.

Logical Host Ethernet Adapters

Physical Location	DRC Name	Dedicated	Allowed VLAN ID	Allowed MAC Address
No items to display				

Figure 5-129 Adding a Host Ethernet Adapter

A window opens (Figure 5-130) that lists the adapters with available ports that can be added to the partition. From the list, select the adapter to be added, change the settings (if necessary), and then click **OK** to apply the settings.



Add LHEA Adapter

The table lists all the Host Ethernet Adapters (HEAs) that can be assigned to the logical partition. You can modify the adapter to use dedicated resources by selecting Yes in the Dedicated column.

	Physical Location	Dedicated	Available Logical Ports	Configured Logical Ports
●	C10-T2	No	4	0
○	C10-T1	No	4	0

▼Advance Settings

MAC Address Settings

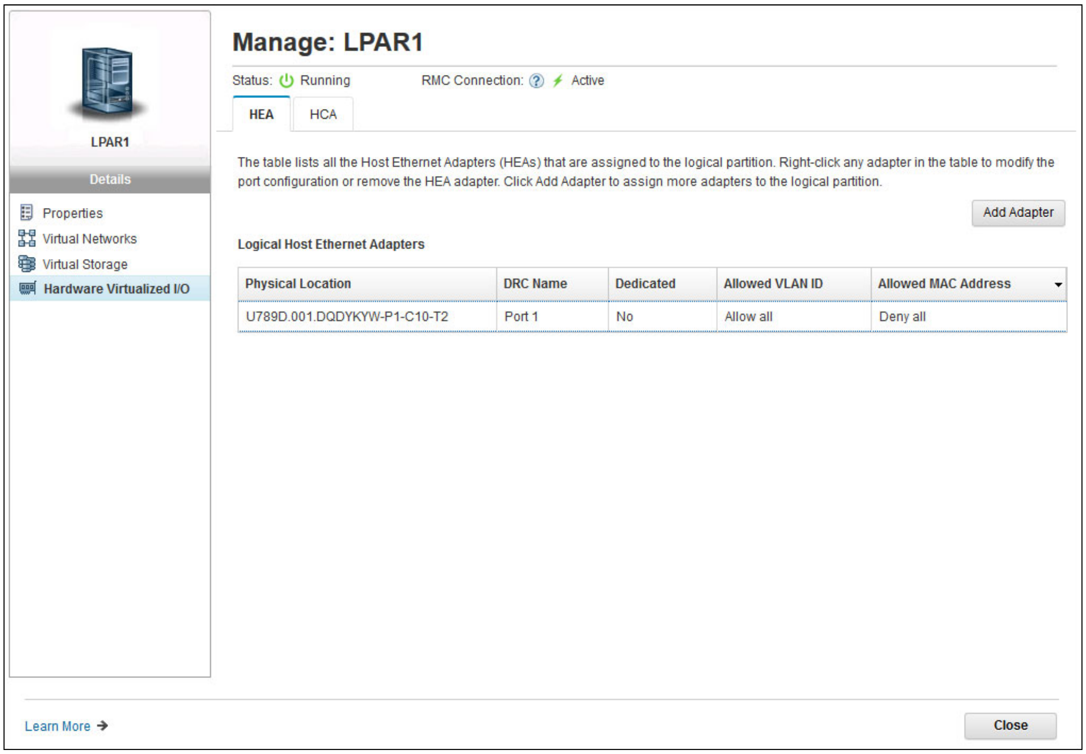
OS MAC Address Restrictions: Allow all

VLAN ID Settings

VLAN ID Restrictions: Allow all

Figure 5-130 Port assignment to the partition

This action returns you to the Hardware Virtualized I/O, Manage window (Figure 5-131), which shows that the adapter with the settings from Figure 5-130 are applied.



Manage: LPAR1

Status: Running   RMC Connection: Active

The table lists all the Host Ethernet Adapters (HEAs) that are assigned to the logical partition. Right-click any adapter in the table to modify the port configuration or remove the HEA adapter. Click Add Adapter to assign more adapters to the logical partition.

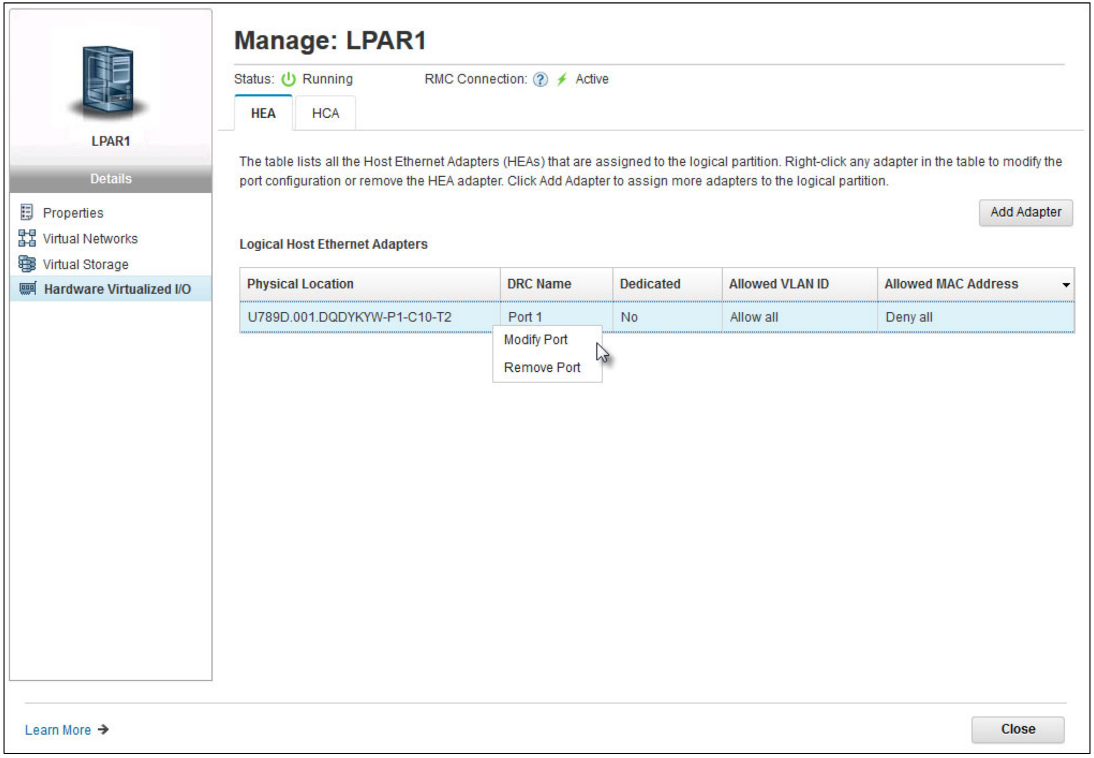
Logical Host Ethernet Adapters

Physical Location	DRC Name	Dedicated	Allowed VLAN ID	Allowed MAC Address
U789D.001.DQDYKYW-P1-C10-T2	Port 1	No	Allow all	Deny all

Figure 5-131 View of the added adapter

5.10.2 Modifying a logical host Ethernet port

To modify the settings on a logical host Ethernet port, right-click the port to be changed and select **Modify Port** (Figure 5-132).



Manage: LPAR1

Status: Running   RMC Connection: Active

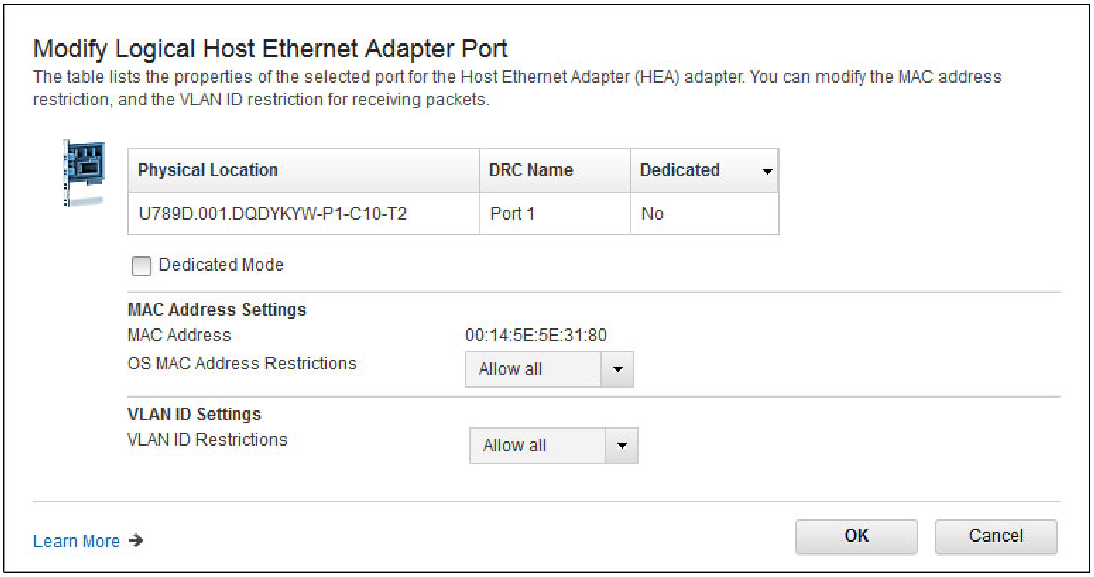
The table lists all the Host Ethernet Adapters (HEAs) that are assigned to the logical partition. Right-click any adapter in the table to modify the port configuration or remove the HEA adapter. Click Add Adapter to assign more adapters to the logical partition.

Logical Host Ethernet Adapters

Physical Location	DRC Name	Dedicated	Allowed VLAN ID	Allowed MAC Address
U789D.001.DQDYKYW-P1-C10-T2	Port 1	No	Allow all	Deny all

Figure 5-132 Modify port selection

A window similar to Figure 5-133 opens. In this window, you can change the settings of the assigned logical host Ethernet port. When the changes are complete, click **OK** to save the settings, and you return to the window that is shown in Figure 5-132.



Modify Logical Host Ethernet Adapter Port

The table lists the properties of the selected port for the Host Ethernet Adapter (HEA) adapter. You can modify the MAC address restriction, and the VLAN ID restriction for receiving packets.

Physical Location	DRC Name	Dedicated
U789D.001.DQDYKYW-P1-C10-T2	Port 1	No

☐ Dedicated Mode

MAC Address Settings

MAC Address: 00:14:5E:5E:31:80

OS MAC Address Restrictions: Allow all

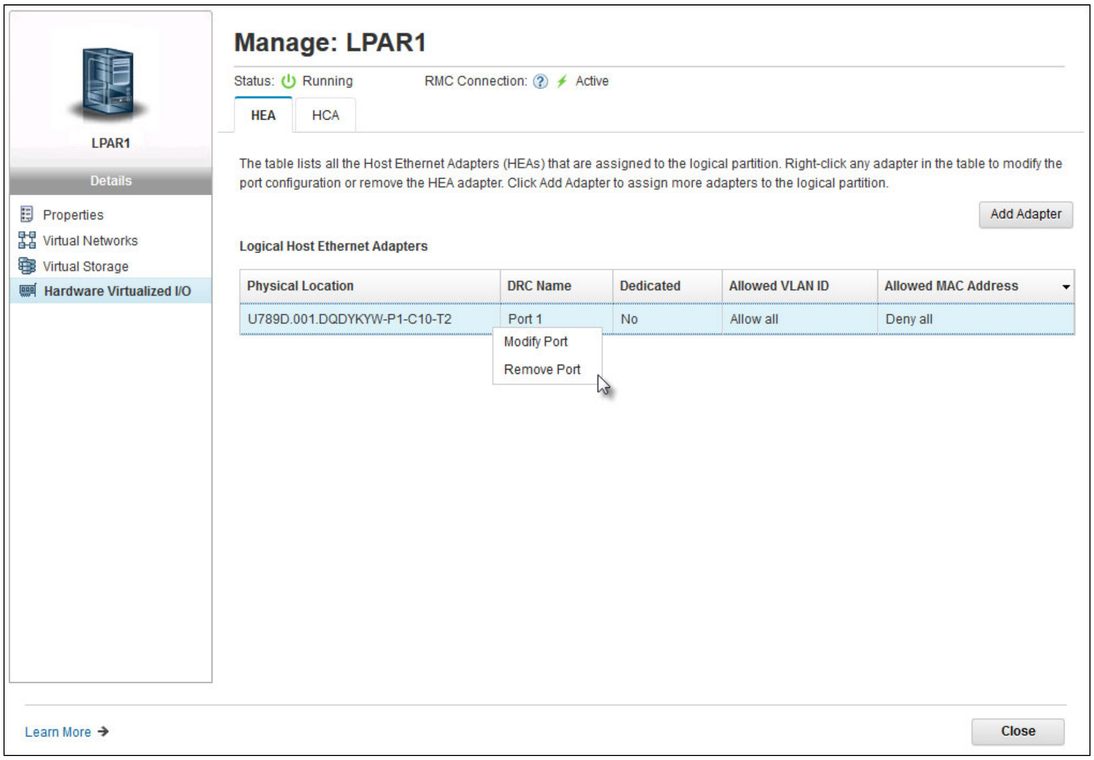
VLAN ID Settings

VLAN ID Restrictions: Allow all

Figure 5-133 Modify Host Ethernet Adapter

5.10.3 Removing a logical host Ethernet port

To remove a logical host Ethernet port, right-click the port to be removed and select **Remove Port** (Figure 5-134). Then, click **OK**.



Manage: LPAR1

Status: Running   RMC Connection: Active

The table lists all the Host Ethernet Adapters (HEAs) that are assigned to the logical partition. Right-click any adapter in the table to modify the port configuration or remove the HEA adapter. Click Add Adapter to assign more adapters to the logical partition.

Logical Host Ethernet Adapters

Physical Location	DRC Name	Dedicated	Allowed VLAN ID	Allowed MAC Address
U789D.001.DQDYKYW-P1-C10-T2	Port 1	No	Allow all	Deny all

Figure 5-134 Remove Host Ethernet Adapter

5.11 Capacity on Demand (CoD)

This section describes the various types of CoD, how to acquire enablement and activation codes, and how to enter these enablement and activation codes on your HMC to gain benefits of the various CoD types. The enablement of the PowerVM features are also described.

5.11.1 Advantages of CoD

CoD provides several advantages to IBM clients:

- Clients can plan for later expansion.

  An IBM client can order a 64-way E870 system now with 16-way active, and then can scale up the system performance granularity to a 64-way without a hardware installation.

  Similarly, a client can order an E870 with 2 TB of system memory and 1 TB active, and then increase memory capacity without extra hardware installation.

- Clients can work around budget constraints by taking advantage of CoD.

  A client might want a 32-way E870 now but can afford only an 8-way within the current budget. In this scenario, the client can buy the 32-way with 8-way active. Then, when the budget allows, the client can activate the additional processors without having to order more hardware.

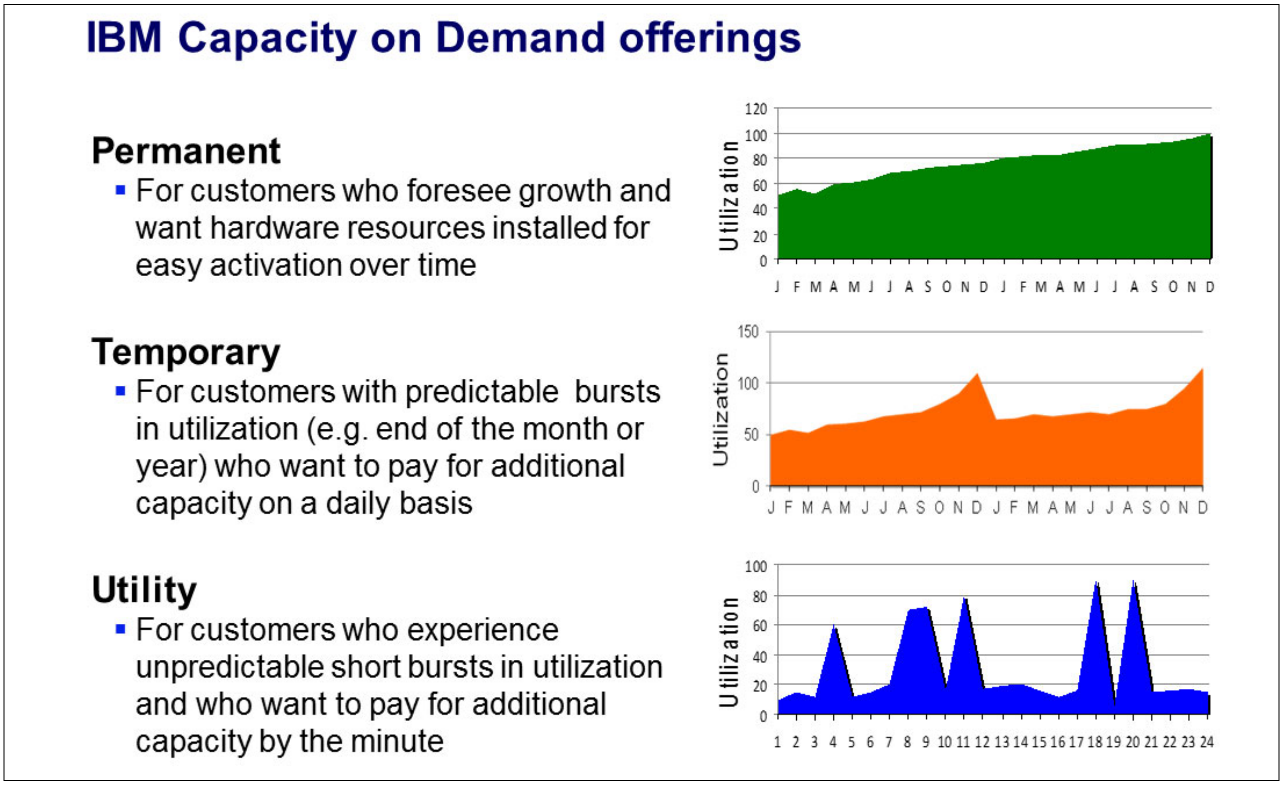
- Clients can plan for scaled usage or billing of Power7 and Power8 technology-based servers.

  A client can use Utility Capacity on Demand or On/Off Capacity on Demand (Elastic CoD) to have resources in reserve, saving money on servers by paying only for what is used.

- Clients can take advantage of increased reliability, availability, and serviceability (RAS).

  Processor sparing allows for inactive processors to be activated immediately in the event of a processor failure. Processor sparing incurs no activation charge to the client.

Based on your current workload and foreseeable growth, the chart in Figure 5-135 can help you decide what CoD offering best fits your needs.



IBM Capacity on Demand offerings

Permanent

- For customers who foresee growth and want hardware resources installed for easy activation over time

Temporary

- For customers with predictable bursts in utilization (e.g. end of the month or year) who want to pay for additional capacity on a daily basis

Utility

- For customers who experience unpredictable short bursts in utilization and who want to pay for additional capacity by the minute

Figure 5-135 Workload patterns for Capacity on Demand

5.11.2 CoD offerings

With CoD offerings, you can dynamically activate one or more resources on your server as your business peaks dictate. You can activate inactive processor cores or memory units that are already installed on your server on a temporary or permanent basis.

For further information about the Capacity on Demand offerings, see the following web page:

http://www.ibm.com/systems/power/hardware/cod

Capacity Upgrade on Demand (CUoD)

With CUoD, you can permanently activate one or more inactive processor cores or memory units without restart your server or interrupting your business:

- Processors can be activated in increments of one processor.
- Memory can be activated in increments of 1 GB.

As your workload demands require more processing power, you can activate inactive processors or memory by placing an order for an activation feature. Hardware does not need to be shipped or installed, and no additional contract is required.

Trial Capacity on Demand

Trial CoD provides no-charge temporary capacity to enable you to test new functions on your server, or to evaluate how more resources affect system workloads. You can evaluate the use of inactive processor cores, memory, or both, at no charge. After you start the trial, the trial period is available for 30 power-on days.

Elastic Capacity on Demand

Elastic CoD (formerly known as On/Off Capacity on Demand) allows you to temporarily activate and deactivate processor cores and memory units to help meet the demands of business peaks. After you request that a number of processor cores or memory units are temporarily available for a specified number of days, those processor cores and memory units are available immediately. You can start and stop requests for Elastic Capacity on Demand, and you are billed for usage at the end of each quarter.

Utility Capacity on Demand

The Utility CoD offering is for customers with unpredictable, short workload increases who need an automated and affordable way to help assure that an adequate server resource is available as needed:

- Usage is measured in processor minute increments.
- Capacity can be paid for either before or after usage.
- Resource usage reporting is required.
- Capacity can be turned on or off by the client.

When you add Utility Capacity on Demand processor cores, they are automatically placed in the default shared processor pool. These processor cores are available to any uncapped partition in any shared processor pool.

The processor cores become available to the pools resource manager. When the system recognizes that the combined processor utilization within the shared pool exceeds 200% of the level of base (purchased or active) processor cores assigned across uncapped partitions, a Utility Capacity on Demand Processor Minute is charged, and this level of performance is available for the next minute of use. If additional workload requires a higher level of performance, the system will automatically allow the additional Utility Capacity on Demand processor cores to be used. The system automatically and continuously monitors and charges for the performance needed above the base (permanent) level.

Power Enterprise Pool

A Power Enterprise Pool is a group of systems that can share Mobile Capacity on Demand processor resources and memory resources.

You can move Mobile Capacity on Demand resource activations among the systems in a pool. These operations provide flexibility when you manage large workloads in a pool of systems and help to rebalance the resources to respond to business needs. This feature is useful for providing continuous application availability during maintenance. You can both move workloads to alternate systems through Live Partition Mobility (LPM), and also can easily move processor and memory activations. Disaster recovery planning is also more manageable with the ability to move activations where and when they are required.

5.11.3 Managing CoD with the HMC

To reach the CoD functions, select **Resources** → **All Systems** from the main window. Then, select the server that you want to manage, and select **Actions** → **View System Partitions**. The Partitions view opens (Figure 5-136). The Capacity on Demand menu on the left has two Options: CoD Functions and Licensed Capabilities.

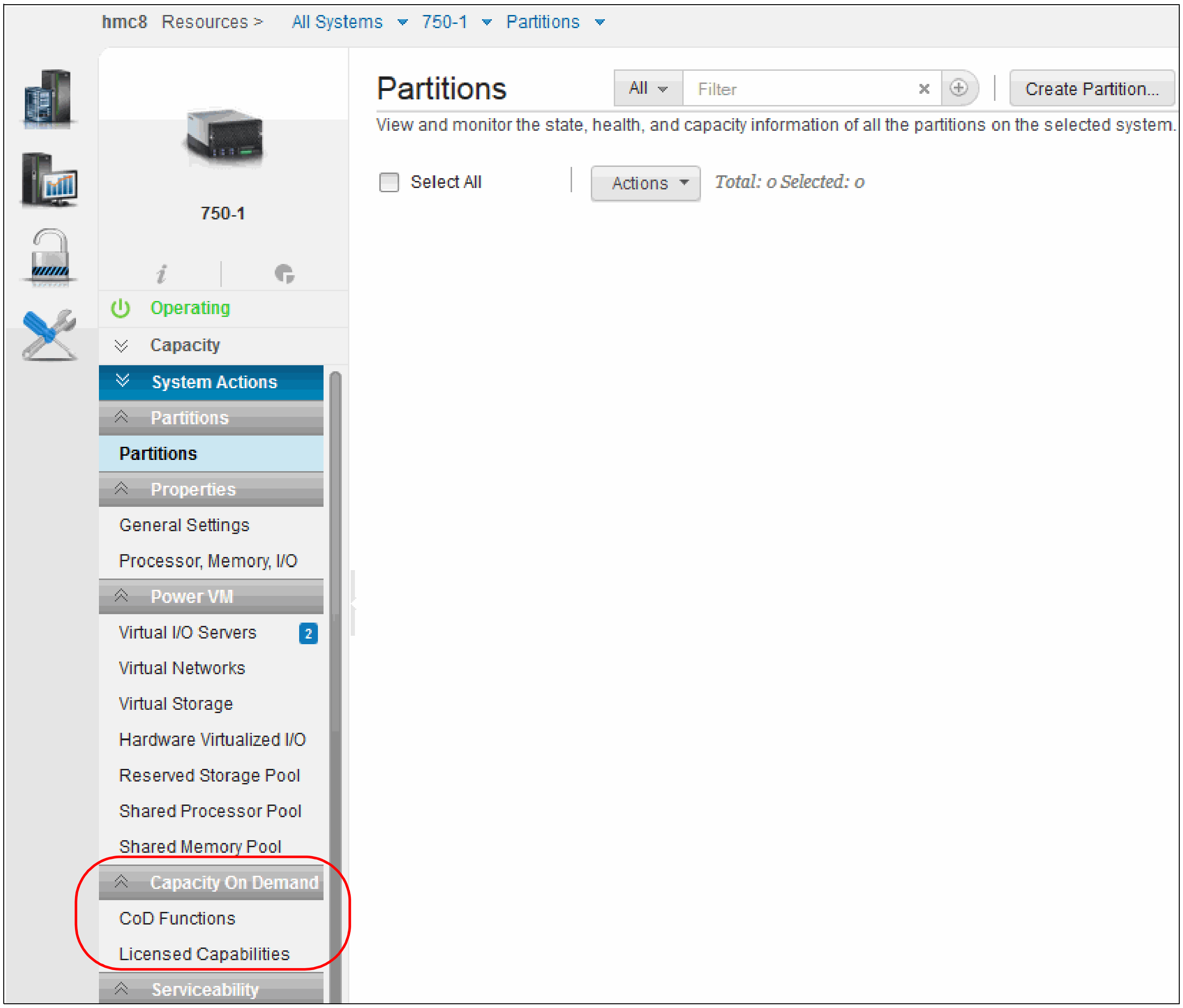
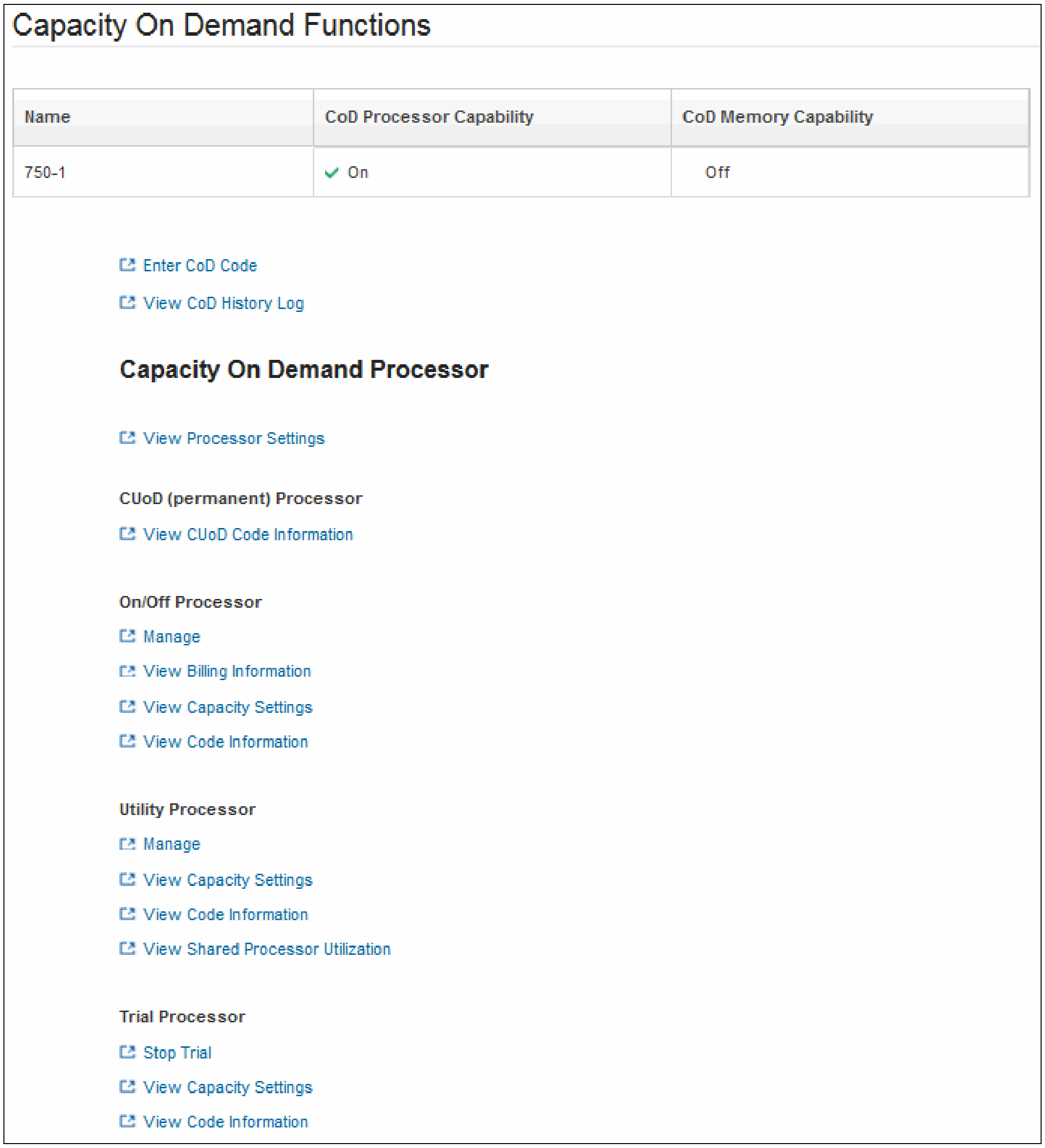


Figure 5-136 Partition overview with Capacity On Demand functions

If you select **CoD Functions**, the Capacity On Demand Functions menu opens (Figure 5-137). At the top, the system you selected is listed with the CoD capabilities for the processor and memory of this system.



Capacity On Demand Functions

Name	CoD Processor Capability	CoD Memory Capability
750-1	✓ On	Off

Capacity On Demand Processor

CUoD (permanent) Processor

On/Off Processor

Utility Processor

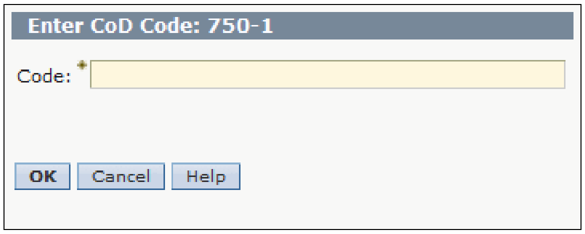
Trial Processor

Figure 5-137 Capacity On Demand Functions menu

The CoD functions are as follows:

- Enter CoD Code

  Select **Enter CoD Code** to open a window (Figure 5-138) where you specify a CoD Code that you obtained for your system.



Enter CoD Code: 750-1

Code: *

Figure 5-138 CoD Code entering window

  The CoD code can be any of the following types:

  – Capacity Upgrade on Demand (CUoD) processor activation code
  – Capacity Upgrade on Demand (CUoD) memory activation code
  – Trial Capacity on Demand processor code
  – Trial Capacity on Demand memory code
  – On/Off Capacity on Demand processor enablement code
  – On/Off Capacity on Demand memory enablement code
  – On/Off CoD capacity termination code
  – Reserved on Demand capacity prepaid code
  – Utility Capacity on Demand enablement code
  – Utility Capacity on Demand reporting code
  – Utility Capacity on Demand termination code
  – Utility Capacity on Demand unlimited activation code

- View CoD History Log

  Select **View CoD History Log** to open a history of the CoD events that occurred on your system. The entries are listed chronologically, starting with the most recent entry.

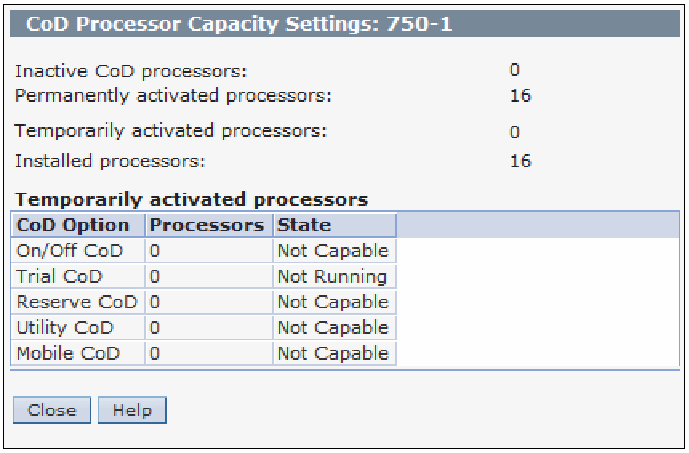
  After the history log reaches the maximum number of entries for your system, subsequent entries cause the history log to wrap, that is, the newest entry overlays the oldest entry.

Capacity on Demand Processor

Figure 5-137 on page 409 lists the Processor Capacity on Demand option:

- View Processor Settings

  Select **View Processor Settings** to see an overview of the state of the processors and of the CoD options for the processors (Figure 5-139).



CoD Processor Capacity Settings: 750-1

Inactive CoD processors:	0
Permanently activated processors:	16
Temporarily activated processors:	0
Installed processors:	16

Temporarily activated processors

CoD Option	Processors	State
On/Off CoD	0	Not Capable
Trial CoD	0	Not Running
Reserve CoD	0	Not Capable
Utility CoD	0	Not Capable
Mobile CoD	0	Not Capable

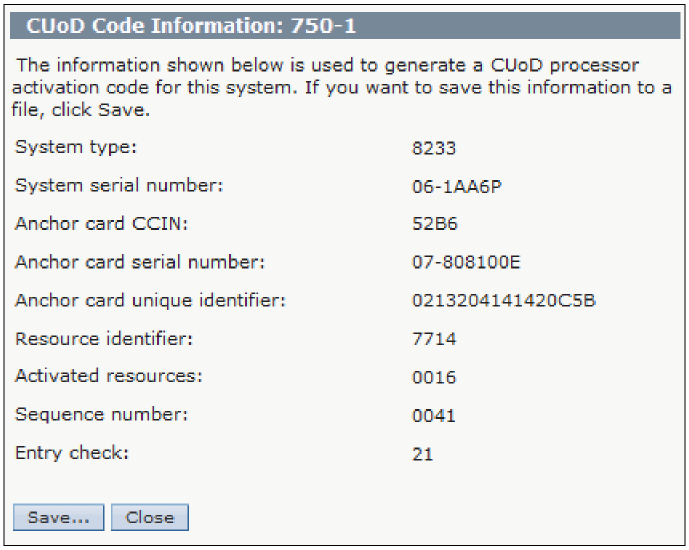
Figure 5-139 CoD Processor Capacity Settings window

CUoD (permanent) Processor

For an overview of CUoD see "Capacity Upgrade on Demand (CUoD)" on page 406. The CUoD (permanent) Processor is as follows:

- View Processor Settings

  Select **View Processor Settings** to see the information (Figure 5-140) you need to generate a CUoD processor activation code for the selected system.



CUoD Code Information: 750-1

The information shown below is used to generate a CUoD processor activation code for this system. If you want to save this information to a file, click Save.

System type:	8233
System serial number:	06-1AA6P
Anchor card CCIN:	52B6
Anchor card serial number:	07-808100E
Anchor card unique identifier:	0213204141420C5B
Resource identifier:	7714
Activated resources:	0016
Sequence number:	0041
Entry check:	21

Figure 5-140 CUoD Code Information for processor activation

You can save this information either to a file on a remote system, which you can specify, or to media (for example DVD-RAM or USB Flash Memory Drive). Then, you can attach the file to an email or print it and fax it to your Service Representative.

On/Off Processor

For an Overview of Elastic Capacity on Demand see “Elastic Capacity on Demand” on page 407.

The Elastic Capacity on Demand Processor (formerly known as On/Off Processor) options are as follows:

- Manage

  Select **Manage** to temporarily activate, change, or stop an Elastic Capacity on Demand request.

  After you order Elastic Capacity on Demand and enable it, you can request temporary activation of Elastic Capacity on Demand resources.

  In a running Elastic Capacity on Demand request, you can change the number of resources, number of days, or both the number of resources and number of days. You do not need to stop the current request to start a new request or wait until the current request expires.

  You can stop a request for temporary capacity at any time during the period of requested temporary capacity.

- View Billing Information

  Select **View Billing Information** to view billing information and send it as an email.

  The customer contract that is required prior to receiving your Elastic Capacity on Demand enablement code requires you to report billing data, at least once per month, regardless of wether you used temporary capacity during the period. You can use several methods to report information about your request. One of them is using email.

- View Capacity Settings

  Select **View Capacity Settings** to see how many Elastic Capacity on Demand processor cores you have, how many are active, and how many are available for activation.

- View Code Information

  Select **View Code Information** to see the information you need to order Elastic Capacity on Demand for processor.

Utility Processor

For an Overview of Utility Processor see “Utility Capacity on Demand” on page 407.

The Utility Processor options are as follows:

- Manage

  Select **Manage** to set a usage limit on the processor minutes that you use.

- View Capacity Settings

  Select **View Capacity Settings** to review the used or reported processor minutes.

- View Code Information

  Select **View Code Information** to see the information you need to order Utility Capacity on Demand.

- View Shared Processor Utilization

  Select **View Shared Processor Utilization** to see the Shared Processor Utilization.

Trial Processor

For an Overview of Trial Capacity on Demand see “Trial Capacity on Demand” on page 407.

The Trial Processor options are as follows:

- Stop Trial

  Select **Stop Trial** to stop the current Capacity on Demand trial for processor cores before the trial automatically expires. If you stop the trial before it expires, you cannot restart it and your forfeit any remaining days.

- View Capacity Settings

  Select **View Capacity Settings** to see how many trial processor cores you have and how much time remains in the current trial Capacity on Demand period.

- View Code Information

  Select **View Code Information** to see the information you need to order Trial Processor Capacity on Demand.

Capacity on Demand Memory

The Capacity on Demand Memory options are mostly the same options as the Capacity on Demand Processor options, except for the following option:

- View Memory Settings

  Select **View Memory Settings** to see an overview of the state of the memory and of the CoD options for the memory.

CUoD (permanent) Memory

For an Overview of CUoD, see “Capacity Upgrade on Demand (CUoD)” on page 406.

The Capacity Upgrade on Demand (CUoD) Memory option is as follows:

- View Memory Settings

  Select **View Memory Settings** to see the information you need to generate a CUoD Memory activation code for the selected system.

  You can save these information either to a file on a remote system which you can specify or to a media. Supported media are DVD-RAM or USB Flash Memory Drive.

On/Off Memory

For an Overview of Elastic Capacity on Demand, see “Elastic Capacity on Demand” on page 407.

The Elastic Capacity on Demand Memory options you select from the Capacity on Demand Functions menu are as follows:

- Manage

  Select **Manage** to open a window where you can temporarily activate, change, or stop an Elastic Capacity on Demand request.

  After you order Elastic Capacity on Demand and enable it, you can request temporary activation of Elastic Capacity on Demand resources.

  In a running Elastic Capacity on Demand request, you can change the number of resources, number of days, or both the number of resources and number of days. You do not need to stop the current request to start a new request or wait until the current request expires.

You can stop a request for temporary capacity at any time during the period of requested temporary capacity.

- View Billing Information

  Select **View Billing Information** at the Capacity on Demand Functions menu you get a window where you can view your billing information and send them as an email containing your billing information.

  The customer contract that is required prior to receiving your Elastic Capacity on Demand enablement code requires you to report billing data, at least once per month, regardless of wether you have used temporary capacity during the period. You can use several methods to report information about your request. One of them is using email.

- **View Capacity Settings**

  If you select **View Capacity Settings** at the Capacity on Demand Functions menu you can see how many Elastic Capacity on Demand memory units you have, how many are active, and how many are available for activation.

- **View Code Information**

  If you select **View Code Information** at the Capacity on Demand Functions menu you get the information you need to order Elastic Capacity on Demand for memory.

Trial Memory

For an Overview of Trial Capacity on Demand see “Trial Capacity on Demand” on page 407.

These are the Trial Memory options on the Capacity on Demand Functions menu:

- Stop Trial

  Select **Stop Trial** to stop the current Capacity on Demand trial for memory units before the trial automatically expires. If you stop the trial before it expires, you cannot restart it and you forfeit any remaining days.

- View Capacity Settings

  Select **View Capacity Settings** to see how many trial memory units you have and how much time is left in the current trial Capacity on Demand period.

- View Code Information

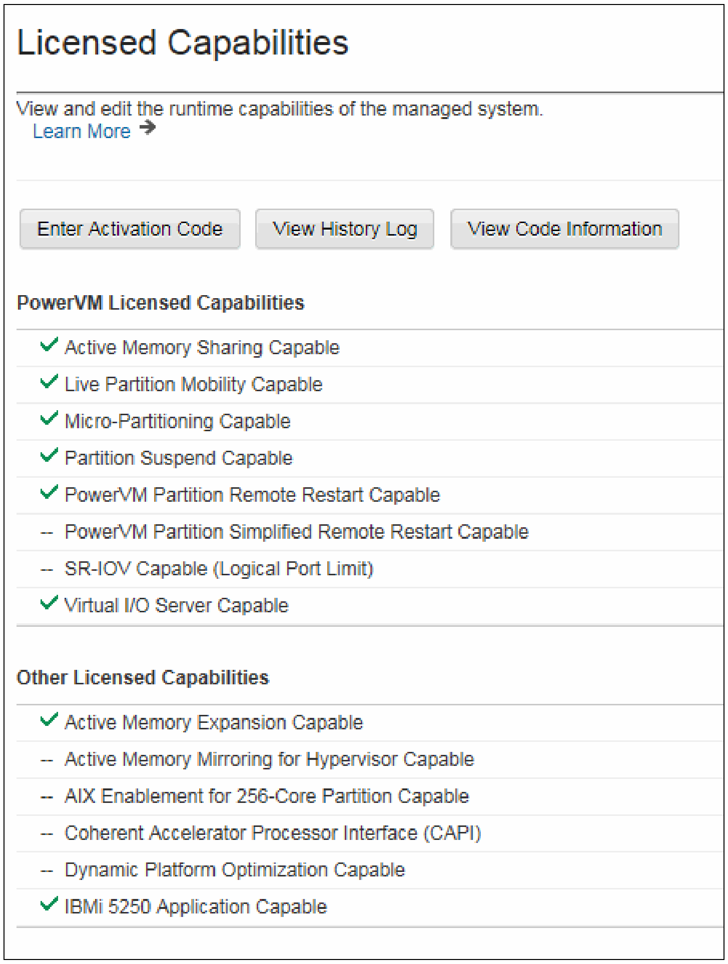
  Select **View Code Information** to see information you need to order Trial Memory Capacity on Demand.

5.11.4 Managing PowerVM with the HMC

To reach the PowerVM functions, select **Resources** → **All Systems** from the main window. Then, select the server that you want to manage, click **Actions** → **View System Partitions**. The Partitions overview is displayed.

The Capacity on Demand menu has two options (shown in Figure 5-136 on page 408): CoD Functions and Licensed Capabilities.

If you select **Licensed Capabilities** on the left, the Licensed Capabilities menu opens (see Figure 5-141), which lists the PowerVM functions you have licensed for the selected system.



Licensed Capabilities

View and edit the runtime capabilities of the managed system.
Learn More →

Enter Activation Code | View History Log | View Code Information

PowerVM Licensed Capabilities

- ✓ Active Memory Sharing Capable
- ✓ Live Partition Mobility Capable
- ✓ Micro-Partitioning Capable
- ✓ Partition Suspend Capable
- ✓ PowerVM Partition Remote Restart Capable
- -- PowerVM Partition Simplified Remote Restart Capable
- -- SR-IOV Capable (Logical Port Limit)
- ✓ Virtual I/O Server Capable

Other Licensed Capabilities

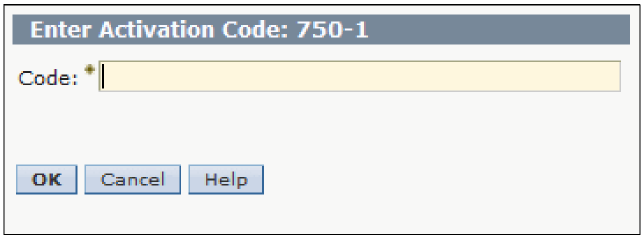
- ✓ Active Memory Expansion Capable
- -- Active Memory Mirroring for Hypervisor Capable
- -- AIX Enablement for 256-Core Partition Capable
- -- Coherent Accelerator Processor Interface (CAPI)
- -- Dynamic Platform Optimization Capable
- ✓ IBMi 5250 Application Capable

Figure 5-141 Licensed Capabilities menu

The top of the menu has three buttons:

- Enter Activation Code

  Click **Enter Activation Code** to open a window (Figure 5-142) where you enter the activation code that you obtained for your selected system.



Enter Activation Code: 750-1

Code: *

Figure 5-142 Enter Activation Code window for Licensed Capabilities

To activate any of the following on-demand functions, specify the appropriate code in the Code field:

  - PowerVM Standard Edition

    Permanently activates the PowerVM Standard Edition capabilities, which can include Virtual I/O Server, IBM Micro-Partitioning®, and Suspend/Resume.

  - PowerVM Enterprise Edition

    Permanently activates the PowerVM Enterprise capabilities, which can include Virtual I/O Server, Micro-Partitioning, Live Partition Mobility, and Active Memory Sharing.

  - Live Partition Mobility Trial

    Temporarily activates Live Partition Mobility.

  - Enterprise Enablement

    Permanently activates the Enterprise Enablement capabilities, which can include 5250 Commercial Processing Workloads (5250 CPW) capacity for application processing. When the managed system is IBM i 5250 Application capable, you can run 5250 applications on the IBM i partitions of the managed system. 5250 applications include all 5250 sessions (such as 5250 emulation, Telnet, and screen scrapers), interactive system monitors, and twin axial printer jobs.

  - WWPN Renewal

    Sets a new worldwide port name (WWPN) prefix, which provides 64 KB WWPNs (32 KB pairs) for use with virtual Fibre Channel adapters.

  - Active Memory Expansion Trial

    Temporarily activates Active Memory Expansion capabilities, which you can use to expand the capacity of physical memory on the system by configuring logical partitions to use compressed memory.

  - Active Memory Expansion

    Permanently activates Active Memory Expansion capabilities, which you can use to expand the capacity of physical memory on the system by configuring logical partitions to use compressed memory.

  - AIX Enablement for 256-core LPAR

    Permanently enables up to 256 processors per partition.

  - Active Memory Mirroring for Hypervisor

    Permanently activates Active Memory Mirroring for Hypervisor capability, which mirrors the main memory used by system firmware to guard against system-wide outages due to memory errors that cannot be corrected.

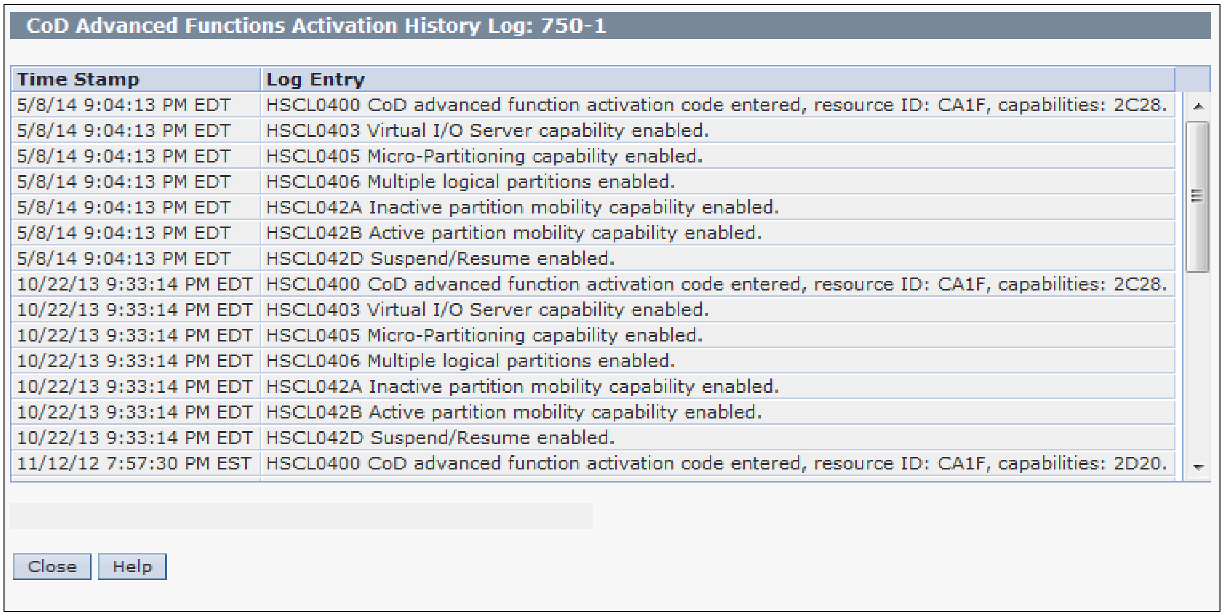
  - Dynamic Platform Optimization

    Activates the Dynamic Platform Optimization (DPO) capability for the managed system. This function is used to dynamically optimize the placement of partitions to increase the processor-memory affinity and to improve performance of the partitions.

- View History Log

  Select **View History Log** to see the activation history of the Licensed Capability functions that occurred on your system (see Figure 5-143 on page 417). A log entry is created each time an activation code is entered successfully, and each time a trial request expires. The entries are shown in chronological order, starting with the most recent entry.

After the history log reaches the maximum number of entries for your system, subsequent entries cause the history log to wrap, that is, the newest entry overlays the oldest entry.



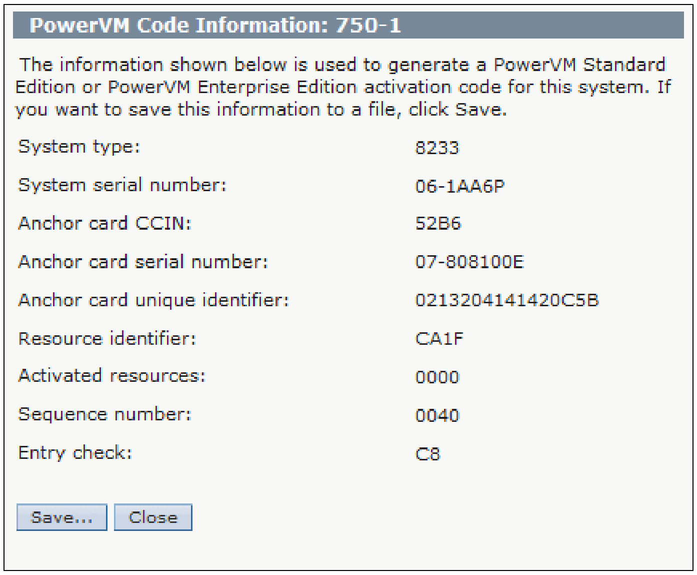
CoD Advanced Functions Activation History Log: 750-1

Time Stamp	Log Entry
5/8/14 9:04:13 PM EDT	HSCL0400 CoD advanced function activation code entered, resource ID: CA1F, capabilities: 2C28.
5/8/14 9:04:13 PM EDT	HSCL0403 Virtual I/O Server capability enabled.
5/8/14 9:04:13 PM EDT	HSCL0405 Micro-Partitioning capability enabled.
5/8/14 9:04:13 PM EDT	HSCL0406 Multiple logical partitions enabled.
5/8/14 9:04:13 PM EDT	HSCL042A Inactive partition mobility capability enabled.
5/8/14 9:04:13 PM EDT	HSCL042B Active partition mobility capability enabled.
5/8/14 9:04:13 PM EDT	HSCL042D Suspend/Resume enabled.
10/22/13 9:33:14 PM EDT	HSCL0400 CoD advanced function activation code entered, resource ID: CA1F, capabilities: 2C28.
10/22/13 9:33:14 PM EDT	HSCL0403 Virtual I/O Server capability enabled.
10/22/13 9:33:14 PM EDT	HSCL0405 Micro-Partitioning capability enabled.
10/22/13 9:33:14 PM EDT	HSCL0406 Multiple logical partitions enabled.
10/22/13 9:33:14 PM EDT	HSCL042A Inactive partition mobility capability enabled.
10/22/13 9:33:14 PM EDT	HSCL042B Active partition mobility capability enabled.
10/22/13 9:33:14 PM EDT	HSCL042D Suspend/Resume enabled.
11/12/12 7:57:30 PM EST	HSCL0400 CoD advanced function activation code entered, resource ID: CA1F, capabilities: 2D20.

Figure 5-143 History Log of the activation of Licensed Capabilities

- View Code Information

  Select **View Code Information** to see the activation code information for the selected system, which you need to order new licensed PowerVM features (Figure 5-144).



PowerVM Code Information: 750-1

The information shown below is used to generate a PowerVM Standard Edition or PowerVM Enterprise Edition activation code for this system. If you want to save this information to a file, click Save.

System type:	8233
System serial number:	06-1AA6P
Anchor card CCIN:	52B6
Anchor card serial number:	07-808100E
Anchor card unique identifier:	0213204141420C5B
Resource identifier:	CA1F
Activated resources:	0000
Sequence number:	0040
Entry check:	C8

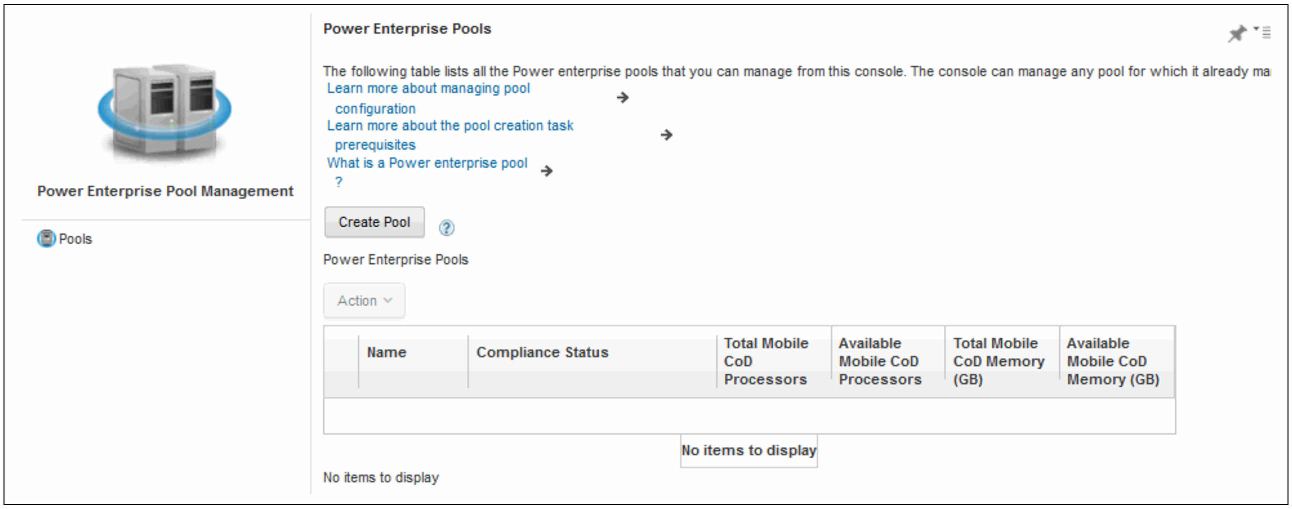
Figure 5-144 PowerVM Code Information window

You can save this information either to a file on a remote system, which you specify, or to media (for example DVD-RAM or USB Flash Memory Drive). Then, you can either attach the file to an email or print it and fax it to your Service Representative.

5.11.5 Managing Power Enterprise Pools

For an overview see “Power Enterprise Pool” on page 407.

To manage Power Enterprise Pools select **Resources** → **All Power Enterprise Pools** from the main window. The Power Enterprise Pools menu opens (Figure 5-145).



Power Enterprise Pool Management

Pools

Power Enterprise Pools

The following table lists all the Power enterprise pools that you can manage from this console. The console can manage any pool for which it already ma

Learn more about managing pool configuration

Learn more about the pool creation task prerequisites

What is a Power enterprise pool ?

Create Pool

Power Enterprise Pools

Action

	Name	Compliance Status	Total Mobile CoD Processors	Available Mobile CoD Processors	Total Mobile CoD Memory (GB)	Available Mobile CoD Memory (GB)

No items to display

No items to display

Figure 5-145 Power Enterprise Pools menu

The main area shows the available Power Enterprise Pools. You can select a Power Enterprise Pool and select an **Action** to do the following functions:

- Mobile Capacity on Demand processor and memory resources can be assigned to systems with inactive resources. Mobile Capacity on Demand resources remain on the system to which they are assigned until they are removed from the system.
- New systems can be added to the pool and existing systems can be removed from the pool.
- New resources can be added to the pool or existing resources can be removed from the pool.
- Pool information can be viewed, including pool assignments, compliance, and history log.

The compliance status of a pool is determined by the compliance status of each server that participates in the pool. A server is in compliance if the server does not have any unreturned Mobile Capacity on Demand resources. When you remove a Mobile Capacity on Demand resource from a server and that resource cannot be reclaimed, the resource is considered as an unreturned Mobile Capacity on Demand resource. Most common, the Mobile Capacity on Demand resource cannot be reclaimed by the server because it is still assigned to one or more partitions. A grace period timer is started when Mobile Capacity on Demand resources that cannot be reclaimed are removed. A separate grace period timer exists for memory resources and processor resources for each server. Also a grace period timer exists for the pool itself.

A Power Enterprise Pool can have one of the following five compliance states:

- In compliance

  None of the servers in the pool have any unreturned Mobile Capacity on Demand resources.

- Approaching out of compliance (within server grace period)

  At least one server in the pool has Mobile Capacity on Demand resources that are unreturned, and the server grace period for those resources is unexpired. None of the servers in the pool have Mobile Capacity on Demand resources that are unreturned and overdue.

- Out of compliance (within pool grace period)

  At least one server in the pool has overdue, unreturned Mobile Capacity on Demand resources and the pool grace period is unexpired.

- Out of compliance

  At least one server in the pool has overdue, unreturned Mobile Capacity on Demand resources and the pool grace period is expired.

- Not available (NA)

  Compliance status is NA because no connection exists between this HMC and the master HMC for the pool.

  Note: Because of the lack of connection between the HMCs, other pool information is not available either. Unavailable information has a value of NA.

You can resolve unreturned Mobile Capacity on Demand resources in any of these ways:

- Migrate a partition to another server, after the partition migrates successfully, any resources that are assigned to the partition on the source server are reclaimed automatically.
- Remove resources from a running partition by using the appropriate dynamic logical partition (DLPAR) task.
- Remove resources from a shutdown partition.
- Delete a partition to free resources that are assigned to that partition.
- Activate Capacity Upgrade on Demand (CUoD), On/Off Capacity on Demand, or Trial Capacity on Demand resources.
- Add Mobile Capacity on Demand resources to the server.

Power Enterprise Pool creation prerequisites

For the creation of a Power Enterprise Pool, contact your service provider to obtain a required Power Enterprise Pool configuration file. This configuration file contains a pool membership activation code for each server that is to be a member of the pool. The file also contains a Mobile Capacity on Demand processor activation code and a Mobile Capacity on Demand memory activation code for the resources in the pool. This file might also contain conversion codes to convert the permanently activated resources on servers in the pool to Mobile Capacity on Demand resources.

Power Enterprise Pool creation

To create a new Power Enterprise Pool, click the **Create Pool** button on the Power Enterprise Pool menu (see Figure 5-145 on page 418). A wizard guides you through the setup of the Power Enterprise Pool. First, provide a name for the new pool you want to create. Next, specify the Power Enterprise configuration file and upload it to the Management Console. Then, specify a backup master HMC and finally the new Enterprise Pool will be created.

Master HMC for the Pool

Each Power Enterprise Pool has a master HMC. Initially, the HMC that you use to create the pool is set as the master HMC of the pool. You must configure a backup master HMC for a pool when you create the pool. The backup master HMC must manage all of the servers in the pool.

Use the following guidelines for designating a new HMC to be the master HMC for a pool:

- Whenever possible, use the current master HMC of a pool to set a new master HMC for the pool. You must use the current HMC to set a new master HMC if the current master HMC is running.
- You must use the latest configuration file for the pool to set a new master HMC for the pool when the master HMC is down and one of the following conditions also applies:
  - The new master HMC is not configured as the backup master HMC for the pool.
  - The new master HMC that is configured as the backup master HMC for the pool does not have valid backup data for the pool.
- When possible, ensure that the following prerequisites are met:
  - Ensure that all of the server that participate in the pool are connected to the new master HMC.
  - Ensure that the participating server are in either the Standby state or the Operating state.
- Set a new master HMC before you perform a clean installation of the current master HMC.

You can perform tasks to view information for a pool from any HMC that manages the pool. You must do all other pool tasks from the master HMC of the pool.

Limitations

At the time of writing, the following limitations for Power Enterprise Pools exist:

- The maximum number of systems in a Power Enterprise Pool is 32 high-end or 48 mid-range systems.
- An HMC can manage multiple Power Enterprise Pools, but is limited to 1000 total partitions.

6

Service support

This chapter describes the service support function on the HMC, including service management, HMC software maintenance, and Advanced System Management Interface (ASMI).

This chapter describes the following topics:

- Overview of menu options
- Session handling
- Serviceability
- Connectivity
- Hardware operations
- Software maintenance introduction
- HMC Data backup
- Restoring HMC data
- Updating, upgrading, and migrating your HMC machine code
- Advanced System Management Interface

6.1 Overview of menu options

The menu options and tasks that are described in Table 6-1 are available in the HMC Enhanced+ interface.

Table 6-1 HMC menu options

Menu	Submenu	Options/Tasks
Resource	All Systems	View All Systems
	All Partitions	View All Partitions
	All Virtual I/O Servers	View All Virtual I/O Servers
	All Frames	View All Frames
	All Power Enterprise Pools	View All Power Enterprise Pools
	All Shared Storage Pool Clusters	View All Shared Storage Pool Clusters
	All Groups	View All Groups

Menu	Submenu	Options/Tasks
HMC Management	Console Settings	Launch Guided Setup Wizard
		View Network Topology
		Test Network Connectivity
		Change Network Settings
		Change Performance Management Settings
		Change Date and Time
		Change Language and Locale
	Console Management	Shut Down or Restart the Management Console
		Schedule Operations
		View Licences
		Update the Hardware Management Console
		Manage Install Resources
		Manage Virtual I/O Server Image Repository
		Format Media
		Backup Management Console Data
		Restore Management Console Data
		Save Upgrade Data
		Manage Data Replication
	Template Library	System and Partition Library
	Updates	Not available (use the Update the Hardware Management Console option instead)
Users and Security	Users and Roles	Change User Password
		Manage User Profiles and Access
		Manage Users and Tasks
		Manage Task and Resource Roles
	Systems and Console Security	Manage Certificates
		Manage LDAP
		Manage KDC
		Enable Remote Command Execution
		Enable Remote Operation
		Enable Remote Virtual Terminal

Menu	Submenu	Options/Tasks
Serviceability	Console Events Logs	View Console Events window
	Serviceable Events Manager	Serviceable Events Manager window
	Events Manager for Call Home	Events Manager for Call Home window
	Service Management	Create Serviceable Event
		Manage Remote Connections
		Manage Remote Support Requests
		Manage Dumps
		Transmit Service Information
		Schedule Service Information
		Format Media
		Perform Management Console Trace
		View Management Console Logs
		View Component Logs
		IBM Electronic Service Agent™ Setup Wizard
		Authorize User
		Enable Electronic Service Agent
		Manage Outbound Connectivity
		Manage Inbound Connectivity
		Manage Customer Information
		Manage Serviceable Event Notification
		Manage Connection Monitoring

6.2 Session handling

Learn about session limitations in the HMC Enhanced+ interface.

6.2.1 Session limitations

The HMC Enhanced+ interface does not support disconnected sessions like the HMC Classic interface. In the HMC Enhanced+ interface, a session logoff and a session disconnect are both considered as a session logoff. This means that you cannot reconnect to the same session to resume your task or tasks that were initiated from a previous session. Every login through the HMC Enhanced+ interface creates a new session.

If you initiate long-running tasks from the HMC Enhanced+ interface and then log off from the session, the long-running tasks continue to run in the background. However, when you log in again, a new session is created and the task progress panels (which help track the progress of the previous tasks) are no longer available. In this scenario, if you want to check the progress of the tasks that were initiated from a previous session, you can run the respective command-line interface (CLI) commands, check the state of the managed resource, or check the console event logs.

> **Note:** You can use the HMC Classic interface to perform long-running tasks to avoid these limitations. Examples of long-running tasks include the following tasks:
>
> - System management for servers:
>   - Deploy system plan
>   - Code update
>   - Hardware - Prepare for hot repair or upgrade
> - System management for partitions:
>   - DLPAR memory in large units in the order of terabytes
>   - Live Partition Mobility (LPM)
>   - Suspend or resume
> - HMC management:
>   - Backup management console data
>   - Restore management console data
>   - Save upgrade data

If you fail to reauthenticate within the time that is specified in the verify timeout settings, you are automatically logged off from the current session.

The idle timeout user property task is not functional in the HMC Enhanced+ interface. The HMC Enhanced+ interface uses the default value of 0 (zero) for the idle timeout setting. If you set a different value, it is ignored.

> **Note:** Session, idle, and verify timeout properties are set for a user and can be different for different users on the same HMC.

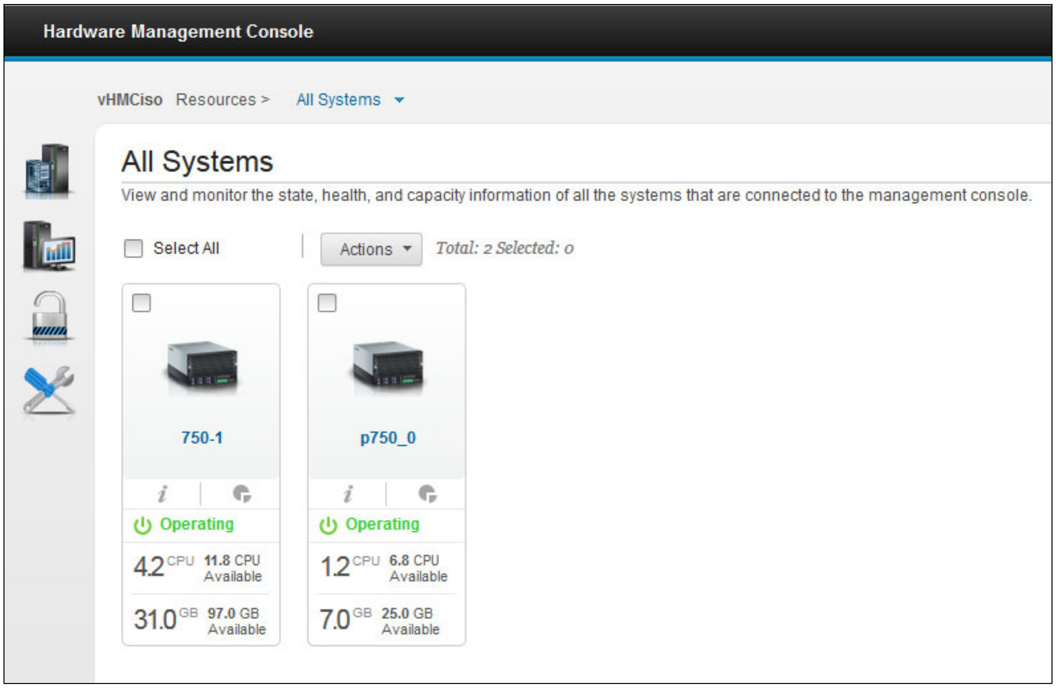
6.3 Serviceability

Problem Analysis on the HMC automatically detects error conditions and then reports to you any problem that requires your attention.

These problems are reported to you as serviceable events. Use the Serviceable Events Manager task to view specific events for selected systems. However, if you notice a problem occurred or you suspect a problem is affecting the system but Problem Analysis did not report it to you, use the Create Serviceable Event task to report the problem to your service provider.

To open the serviceability tasks that are available for your system, complete these steps:

1. In the navigation area, click the **Resources** icon, and then select **All Systems**. The All Systems pane opens (Figure 6-1).



Hardware Management Console
vHMCiso Resources > All Systems
All Systems

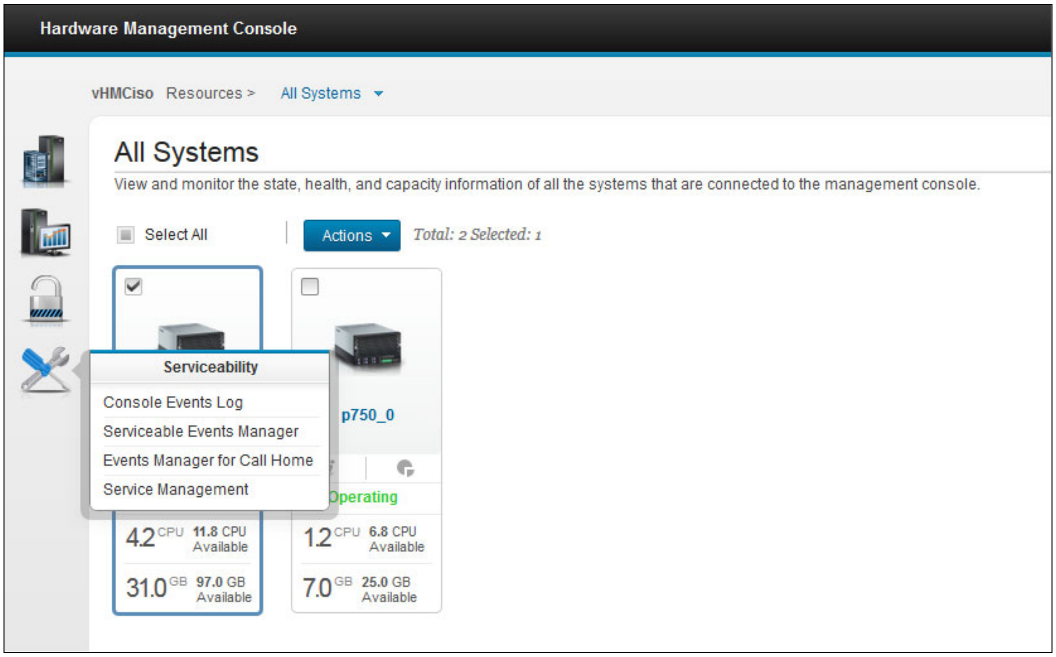
View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

□ Select All
Actions
Total: 2 Selected: 0
750-1
Operating
4.2 CPU 11.8 CPU Available
31.0 GB 97.0 GB Available
p750_0
Operating
1.2 CPU 6.8 CPU Available
7.0 GB 25.0 GB Available

Figure 6-1 HMC Hardware Resources Menu

2. Select the server for which you want to manage serviceability tasks.

3. Select **Actions** → **Serviceability** → **Serviceable Events Manager** (Figure 6-2).



Hardware Management Console
vHMCiso Resources > All Systems
All Systems

View and monitor the state, health, and capacity information of all the systems that are connected to the management console.

Select All
Actions
Total: 2 Selected: 1
Serviceability
Console Events Log
Serviceable Events Manager
Events Manager for Call Home
Service Management
p750_0
Operating
4.2 CPU 11.8 CPU Available
31.0 GB 97.0 GB Available
1.2 CPU 6.8 CPU Available
7.0 GB 25.0 GB Available

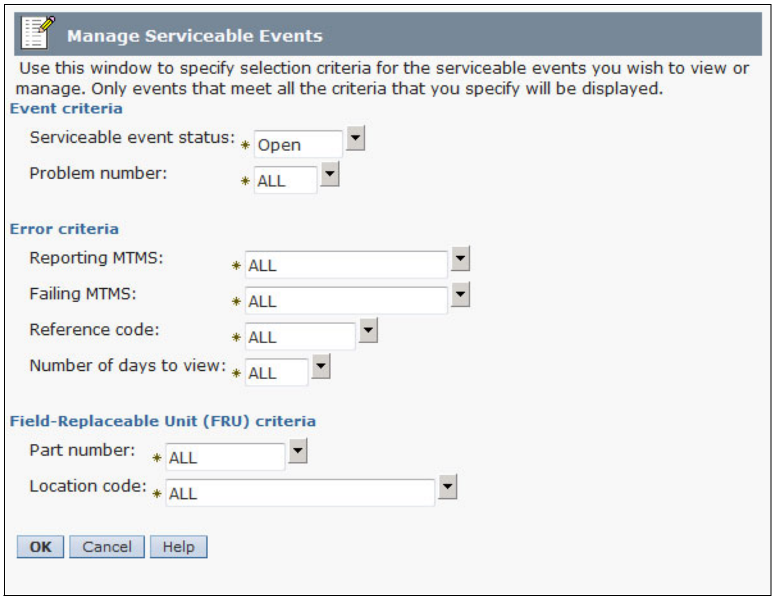
Figure 6-2 HMC Serviceability Menu

6.3.1 Serviceable Events Manager

Problems on your managed system are reported to the HMC as serviceable events. You can view the problem, manage problem data, use call home for the event to your service provider, or repair the problem.

To set the criteria for the serviceable events, complete these steps:

1. In the navigation area, click the **Resources** icon, and then select **All Systems**.
2. Select the server for which you want to manage serviceable events.
3. In the menu pod, expand **Serviceability** and then click **Serviceability**.
4. Click **Serviceable Events Manager**.
5. The Manage Serviceable Events window opens (Figure 6-3).



Manage Serviceable Events

Use this window to specify selection criteria for the serviceable events you wish to view or manage. Only events that meet all the criteria that you specify will be displayed.

Event criteria

Serviceable event status: * Open

Problem number: * ALL

Error criteria

Reporting MTMS: * ALL

Failing MTMS: * ALL

Reference code: * ALL

Number of days to view: * ALL

Field-Replaceable Unit (FRU) criteria

Part number: * ALL

Location code: * ALL

Figure 6-3 Manage Serviceable Events

6. Provide event criteria, error criteria, and FRU criteria. If you do not want the results filtered, select **ALL**.
7. Click **OK**.

Figure 6-4 on page 428 shows the Serviceable Event Overview window, which lists all events that match your criteria. The information displayed in the compact table view includes these items:

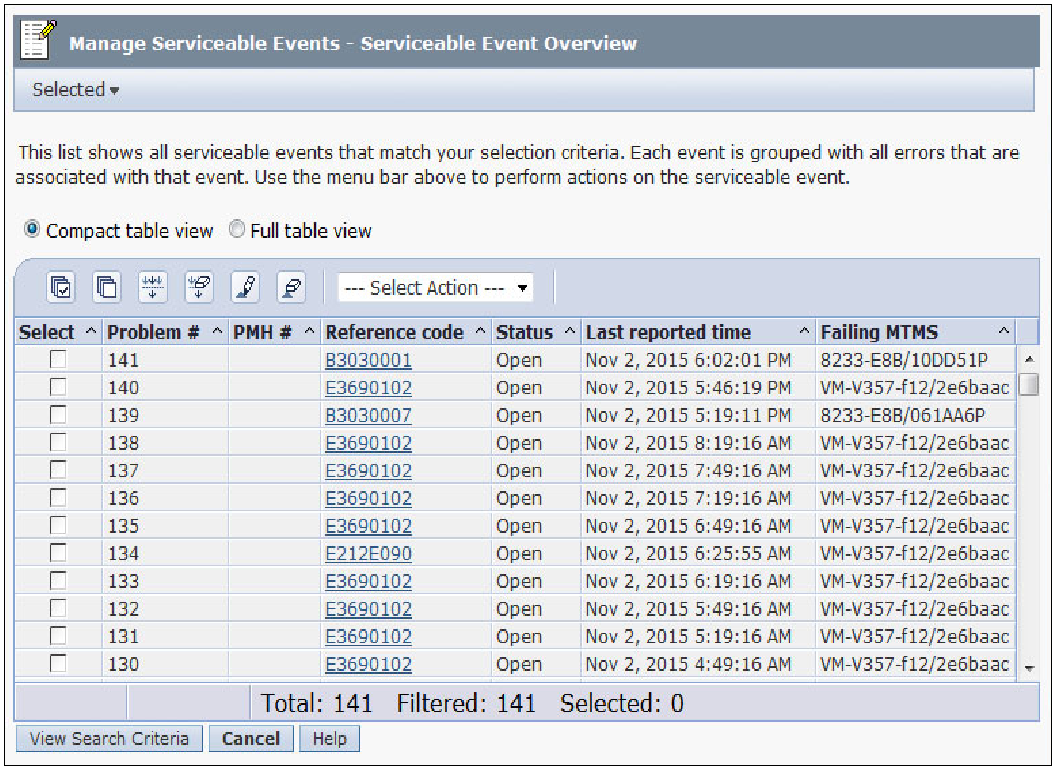
- Select

  Select a serviceable event if you want to perform actions on it.

- Problem number (#)
- Problem Management Hardware number (PMH #)
- Reference code

  Click a link in the Reference code column to display a description of the problem reported and actions that you can do to correct the problem.

- Status of the problem
- Last reported time of the problem
- Failing machine serial label (MTMS) of the problem



This list shows all serviceable events that match your selection criteria. Each event is grouped with all errors that are associated with that event. Use the menu bar above to perform actions on the serviceable event.

● Compact table view ○ Full table view

Select	Problem #	PMH #	Reference code	Status	Last reported time	Failing MTMS
□	141		B3030001	Open	Nov 2, 2015 6:02:01 PM	8233-E8B/10DD51P
□	140		E3690102	Open	Nov 2, 2015 5:46:19 PM	VM-V357-f12/2e6baac
□	139		B3030007	Open	Nov 2, 2015 5:19:11 PM	8233-E8B/061AA6P
□	138		E3690102	Open	Nov 2, 2015 8:19:16 AM	VM-V357-f12/2e6baac
□	137		E3690102	Open	Nov 2, 2015 7:49:16 AM	VM-V357-f12/2e6baac
□	136		E3690102	Open	Nov 2, 2015 7:19:16 AM	VM-V357-f12/2e6baac
□	135		E3690102	Open	Nov 2, 2015 6:49:16 AM	VM-V357-f12/2e6baac
□	134		E212E090	Open	Nov 2, 2015 6:25:55 AM	VM-V357-f12/2e6baac
□	133		E3690102	Open	Nov 2, 2015 6:19:16 AM	VM-V357-f12/2e6baac
□	132		E3690102	Open	Nov 2, 2015 5:49:16 AM	VM-V357-f12/2e6baac
□	131		E3690102	Open	Nov 2, 2015 5:19:16 AM	VM-V357-f12/2e6baac
□	130		E3690102	Open	Nov 2, 2015 4:49:16 AM	VM-V357-f12/2e6baac

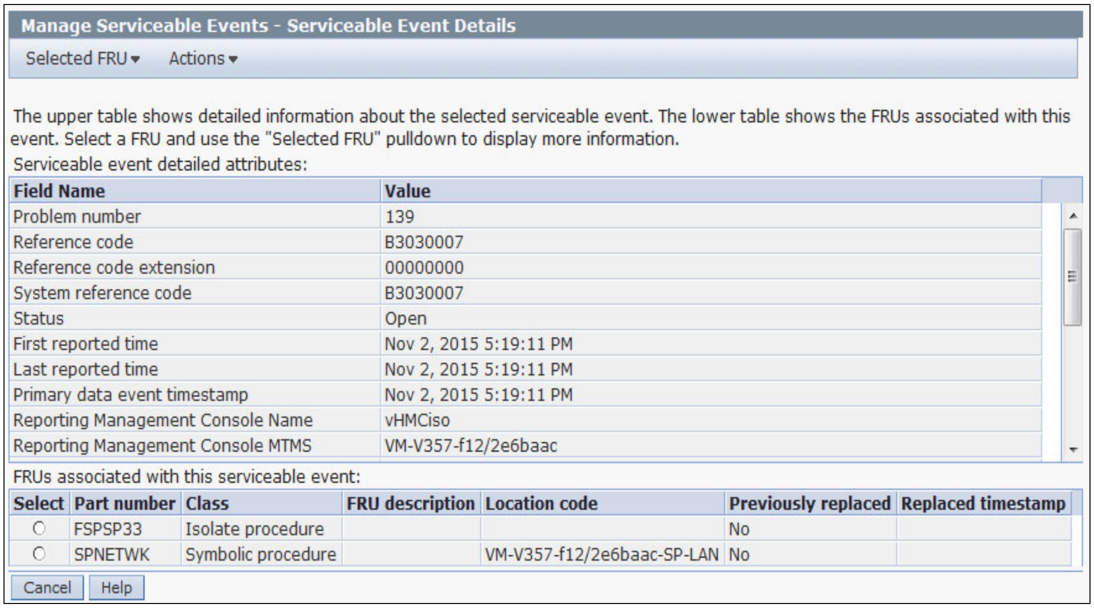
Total: 141 Filtered: 141 Selected: 0

Figure 6-4 Serviceable Events Overview menu

The full table view includes more detailed information, including reporting MTMS, first reported time, and serviceable event text.

Select a serviceable event, click **Select Action**, and then select one of the following actions:

- **View event details**: See details about the event and about field-replaceable units (FRUs) associated with this event and their descriptions (Figure 6-5).



The upper table shows detailed information about the selected serviceable event. The lower table shows the FRUs associated with this event. Select a FRU and use the "Selected FRU" pulldown to display more information.

Serviceable event detailed attributes:

Field Name	Value
Problem number	139
Reference code	B3030007
Reference code extension	00000000
System reference code	B3030007
Status	Open
First reported time	Nov 2, 2015 5:19:11 PM
Last reported time	Nov 2, 2015 5:19:11 PM
Primary data event timestamp	Nov 2, 2015 5:19:11 PM
Reporting Management Console Name	vHMCiso
Reporting Management Console MTMS	VM-V357-f12/2e6baac

FRUs associated with this serviceable event:

Select	Part number	Class	FRU description	Location code	Previously replaced	Replaced timestamp
○	FSPSP33	Isolate procedure			No	
○	SPNETWK	Symbolic procedure		VM-V357-f12/2e6baac-SP-LAN	No	

Figure 6-5 Serviceable event details

- **Repair the event:** Launch a guided repair procedure, if available.
- **Call home the event:** Report the event to your service provider.
- **Manage event problem data:** View, call home, or offload to media the data and logs that are associated with this event.
- **Close the event:** After the problem is solved, add comments and close the event.

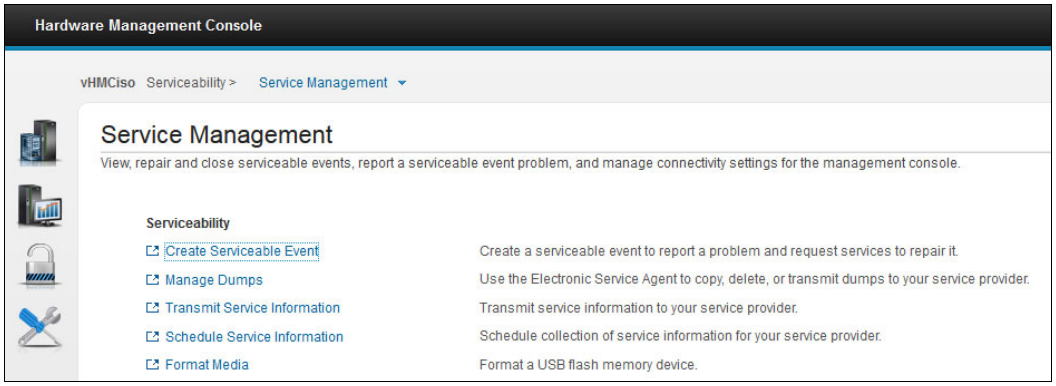
6.3.2 Create Serviceable Event

Use this task to report problems that occurred on your Hardware Management Console (HMC) to the service provider (for example, the mouse does not work); also use to test problem reporting.

Submitting a problem depends upon whether you have customized this HMC to use the Remote Support Facility (RSF) and if it is authorized to automatically call for service.

To report a problem about your HMC, complete the following steps:

1. In the navigation area, click the **Serviceability** icon, and then select **Service Management**. The Service Management area opens (Figure 6-6).


Hardware Management Console
vHMCiso Serviceability > Service Management

Service Management

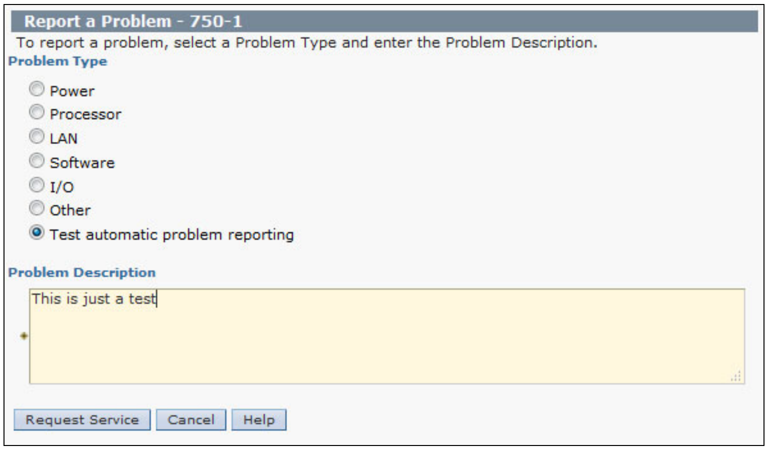
View, repair and close serviceable events, report a serviceable event problem, and manage connectivity settings for the management console.

Serviceability

Create Serviceable Event	Create a serviceable event to report a problem and request services to repair it.
Manage Dumps	Use the Electronic Service Agent to copy, delete, or transmit dumps to your service provider.
Transmit Service Information	Transmit service information to your service provider.
Schedule Service Information	Schedule collection of service information for your service provider.
Format Media	Format a USB flash memory device.

Figure 6-6 Service Management menu

2. Under Serviceability, click **Create Serviceable Event**.
3. In the next window (Figure 6-7), select a problem type from the Problem Type list, enter a brief description of the problem in the Problem Description input field, and click **Request Service**.


Report a Problem - 750-1

To report a problem, select a Problem Type and enter the Problem Description.

Problem Type

○ Power
○ Processor
○ LAN
○ Software
○ I/O
○ Other
● Test automatic problem reporting

Problem Description

This is just a test

Figure 6-7 Create serviceable event window

To test problem reporting from the Report a Problem window, complete these steps:

1. Select **Test automatic problem reporting** and enter a text such as “This is just a test” in the Problem Description input field.
2. Click **Request Service**. The problems are reported to the service provider for the Hardware Management Console. Reporting a problem sends to the service provider the information you provide in the Report a Problem window, and machine information that identifies the console.

If this is a real problem (not a test), then under Problem Description, provide as much information as possible about the problem that you encountered, including the hardware that is involved and references to any error logs or reports that are associated with the event.

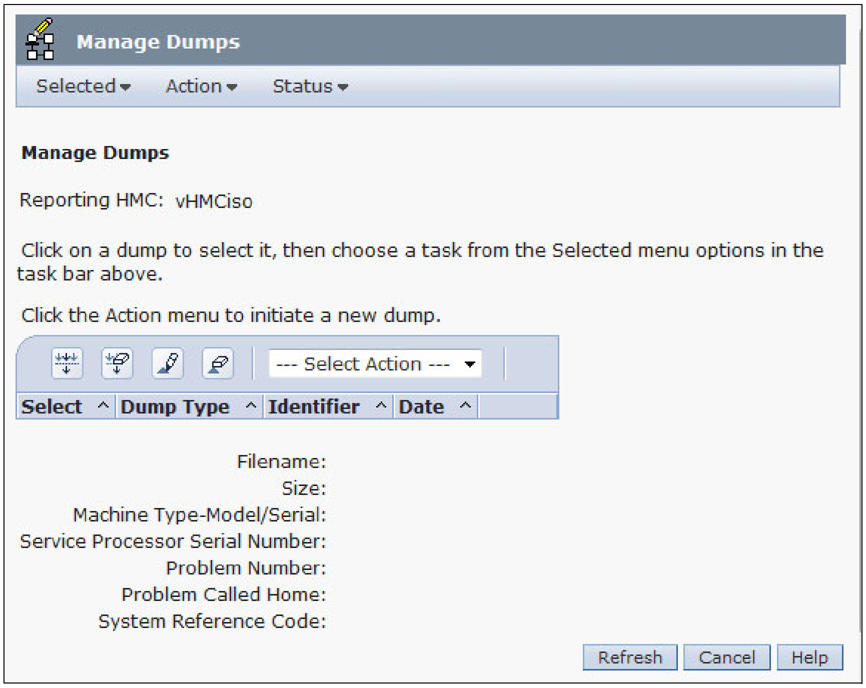
The options that can be performed in the top half of the service management area mostly pertain to service events, formatting and using removable media, and sending in service reports to IBM. There are also troubleshooting tools available in this area of the HMC that pertain to troubleshooting not only with managed servers but also with the HMC itself.

After you click **Request Service**, if your connectivity to IBM is set up properly (as described in 6.4, “Connectivity” on page 434), the error report is sent to IBM.

6.3.3 Manage Dumps

Use this task to manage system, service processor, and power subsystem dumps for systems that are managed by the HMC.

Figure 6-8 shows Manage Dumps window.



Manage Dumps

Reporting HMC: vHMCiso

Click on a dump to select it, then choose a task from the Selected menu options in the task bar above.

Click the Action menu to initiate a new dump.

Select	Dump Type	Identifier	Date

Filename:
Size:
Machine Type-Model/Serial:
Service Processor Serial Number:
Problem Number:
Problem Called Home:
System Reference Code:

Figure 6-8 Manage Dumps

Use the Manage Dumps task to do the following actions:

- Initiate a system dump, a service processor dump, or a power subsystem dump.
- Modify the dump capability parameters for a dump type before initiating a dump.
- Delete a dump.
- Copy a dump to media.
- Copy a dump to another system using FTP.
- View the offload status of a dump as it progresses.
- Use the Call Home feature to transmit the dump to your service provider, for example IBM Remote Support, for further analysis.

System dump

This type is a collection of data from server hardware and firmware, either after a system failure or a manual request. Perform a system dump only under the direction of your next level of support or your service provider.

> **Note:** Do a system dump only for the problem determination procedure because it forces a shutdown on every logical partition (LPAR) in the selected managed system.

Service processor dump

This type is a collection of data from a service processor either after a failure, external reset, or manual request.

Power subsystem dump

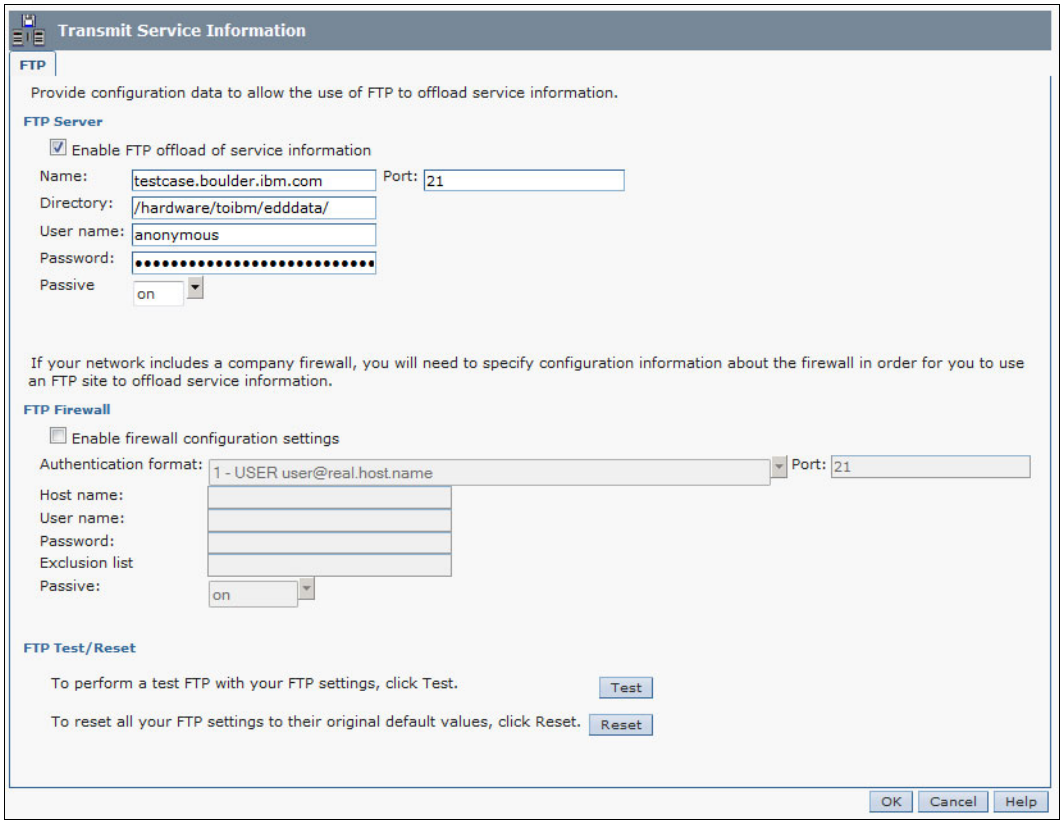
This type is a collection of data from the Bulk Power Control service processor. This is applicable to only certain models of managed systems.

6.3.4 Transmit Service Information

To transmit service information, complete the following steps:

1. In the navigation area, click the **Serviceability** icon, and select **Service Management**.
2. In the content pane, click **Transmit Service Information**.

   The Transmit Service Information section is displayed (Figure 6-9 on page 432).



Transmit Service Information

FTP

Provide configuration data to allow the use of FTP to offload service information.

FTP Server

☑ Enable FTP offload of service information

Name: testcase.boulder.ibm.com Port: 21

Directory: /hardware/toibm/edddata/

User name: anonymous

Password: ••••••••••••••••••••••••••

Passive on

If your network includes a company firewall, you will need to specify configuration information about the firewall in order for you to use an FTP site to offload service information.

FTP Firewall

☐ Enable firewall configuration settings

Authentication format: 1 - USER user@real.host.name Port: 21

Host name:

User name:

Password:

Exclusion list

Passive: on

FTP Test/Reset

To perform a test FTP with your FTP settings, click Test.

To reset all your FTP settings to their original default values, click Reset.

Figure 6-9 Transmit Service Information

3. Click one of the following tabs, provide the necessary information, and then click **OK**:

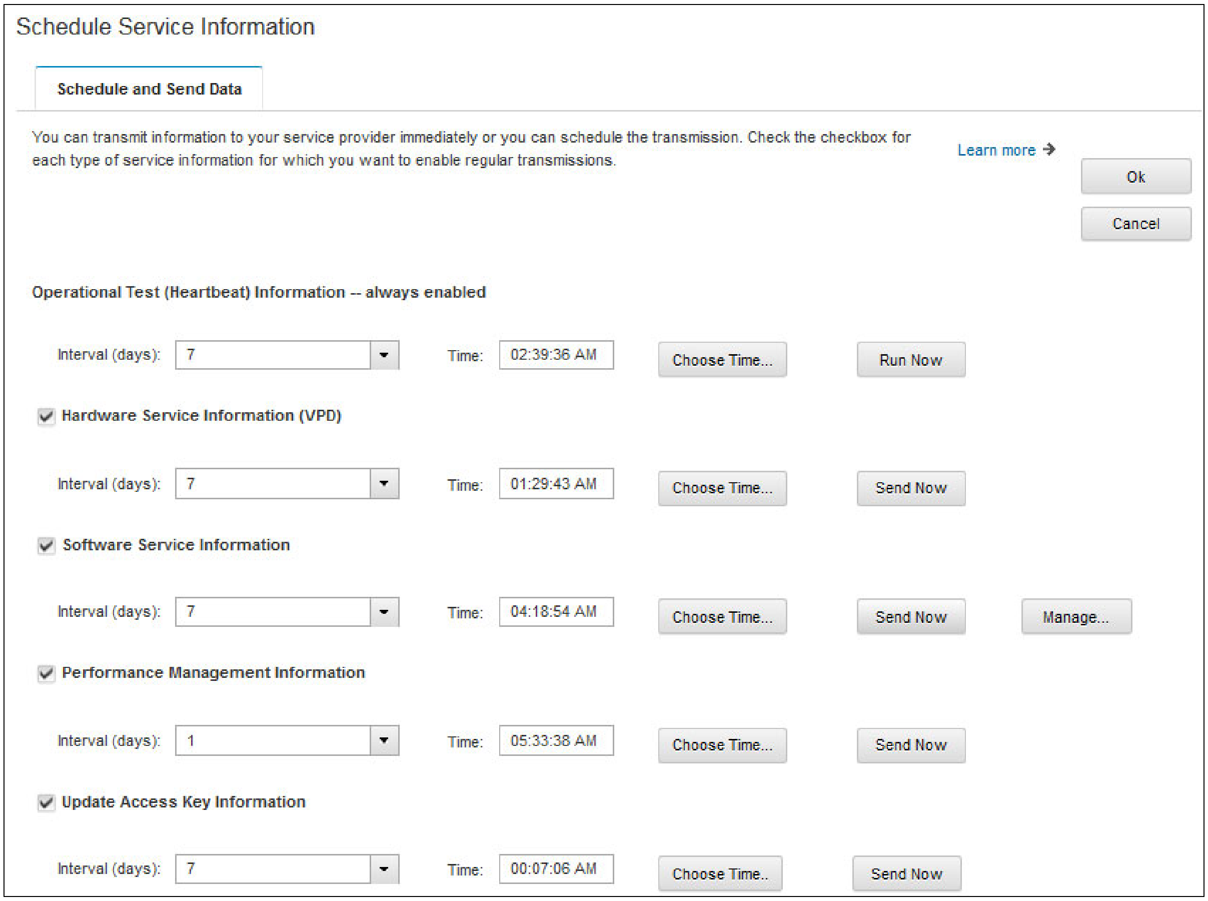
> **Tabs:** When Figure 6-9 was created for this book, FTP was the only available tab.

- **Transmit**. Use this page to schedule when to transmit service data to your service provider (specifying frequency in days and time of day) and how you want to transmit the service and performance management information.
- **FTP**. Use this page to configure the File Transfer Protocol (FTP) information for the FTP server, with or without a firewall, for off loading service information. This service information is extended error data, consisting of problem-related data about problems opened on the HMC for the HMC or managed system.
- **Transmit Service Data to IBM**. Use this page to provide the ability to send information that is stored on the HMC hard disk that can be used for problem determination. The data may be traces, logs, or dumps and the destination for the data may be the IBM Service Support System, a diskette, USB flash memory drive, or a DVD-RAM. Before you can send information to the IBM Service Support System, Phone Server and Remote Service must be enabled.

6.3.5 Schedule Service Information

To schedule service information, complete the following steps:

1. In the navigation area, click the **Serviceability** icon, and then select **Service Management**.
2. In the content pane, click **Schedule Service Information**.
3. In the Schedule and Send Data page of the Schedule Service Information area (Figure 6-10), select the interval (in days) and the time to schedule repeating transmissions. Then, click **OK**.



Schedule Service Information

Schedule and Send Data

You can transmit information to your service provider immediately or you can schedule the transmission. Check the checkbox for each type of service information for which you want to enable regular transmissions.

Operational Test (Heartbeat) Information -- always enabled

Interval (days): 7 Time: 02:39:36 AM

☑ Hardware Service Information (VPD)

Interval (days): 7 Time: 01:29:43 AM

☑ Software Service Information

Interval (days): 7 Time: 04:18:54 AM

☑ Performance Management Information

Interval (days): 1 Time: 05:33:38 AM

☑ Update Access Key Information

Interval (days): 7 Time: 00:07:06 AM

Figure 6-10 Schedule Service Information window

6.3.6 Format Media

This task formats a diskette or USB 2.0 Flash Drive Memory Key. You can format a diskette by supplying a user-specified label.

To format a diskette or USB 2.0 Flash Drive Memory Key, do the following:

1. In the navigation area, click the **HMC Management** icon, and then select **Console Managment**.
2. In the content pane, click **Format Media**.
3. From the Format Media window, select the type of media you want to format, and then click **OK**.

4. Make sure your media has been correctly inserted, then click **Format**.

   The Format Media progress window opens. After the media is formatted, the Format Media Completed window opens.

5. Click **OK** and then click **Close** to end the task.

6.4 Connectivity

To see the following connectivity options, select **Service Management** in the HMC workplace window:

- Enable Electronic Service Agent

  Use the call home function to allow the HMC to dial in to the IBM network through a modem or to the Internet to report the following information:

  – Serviceable events
  – CoD usage (On/Off, Reserve Capacity, and Utility Capacity)
  – Hardware failures

- Outbound Connectivity

  Configure the HMC modem or Ethernet connectivity to the outside Ethernet.

- Inbound Connectivity

  Allow your service provider temporary access to your HMC or partitions of a managed system.

- Customer Information

  Specify administrator, system, and account information.

- Authorize User

  Register a client user ID with the eService website.

- Serviceable Event Notification

  Define information to enable client notification when service events occur.

- Connection Monitoring

  Configure timers to detect outages and monitor connections for selected computers.

- Electronic Service Agent Setup wizard

  Set up the electronic service agent through a guided setup wizard.

6.4.1 Enable Electronic Service Agent option

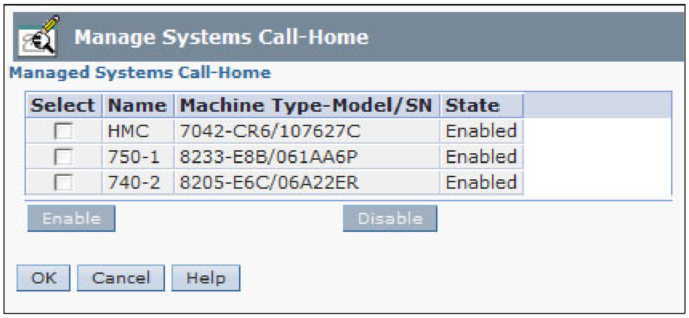
Use this task to enable or disable the call-home state for managed systems.

Note: If Customizable Data Replication is Enabled on this HMC (by using the Manage Data Replication task), the data specified in this task may change depending on automatic replication from other HMCs configured on your network. For more information about data replication, see 5.3.9, “Manage Data Replication” on page 324.

By enabling the call-home state for a managed system, the console automatically contacts a service center when a serviceable event occurs. When a managed system is disabled, your service representative is not informed of serviceable events.

To manage call home for the systems, complete the following steps:

1. In the navigation area, click the **Serviceability** icon, and then select **Service Management.**
2. In the content pane, click **Enable Electronic Service Agent**.
3. From the next window, select a system or systems for which you want to enable or disable the call-home state, and then click **Enable** or **Disable** (Figure 6-11).
4. Click **OK** after making your selections.


Manage Systems Call-Home

Managed Systems Call-Home

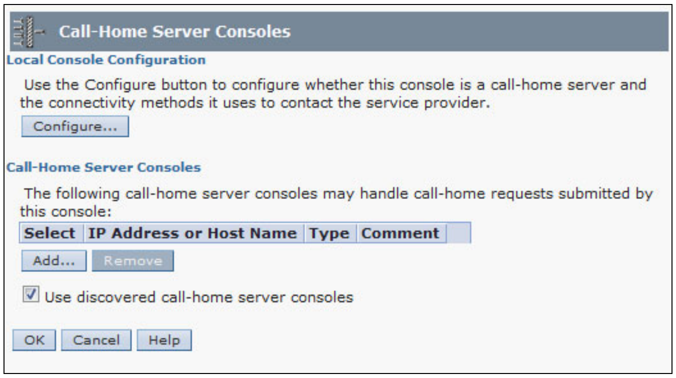
Select	Name	Machine Type-Model/SN	State
□	HMC	7042-CR6/107627C	Enabled
□	750-1	8233-E8B/061AA6P	Enabled
□	740-2	8205-E6C/06A22ER	Enabled

Figure 6-11 The call home feature

Along with enabling your HMC or managed servers for the call-home feature, configure and test your outbound connectivity to ensure that your reports can get to IBM.

6.4.2 Manage Outbound Connectivity task.

You can achieve outbound connectivity either through a modem on the HMC or through Internet connectivity. First, click the **Serviceability** icon and then select **Service Management** → **Manage Outbound Connectivity** → **Enable local server as call-home server**. The next window opens (Figure 6-12).


Call-Home Server Consoles

Local Console Configuration

Use the Configure button to configure whether this console is a call-home server and the connectivity methods it uses to contact the service provider.

Call-Home Server Consoles

The following call-home server consoles may handle call-home requests submitted by this console:

Select	IP Address or Host Name	Type	Comment

☑ Use discovered call-home server consoles

Figure 6-12 Call-Home Server Consoles

This allows the local HMC to connect to your service providers remote support facility for call-home requests.

> **Note:** Before the window opens, you must first accept the terms described about the information you provided in this task.

The dial information window displays the following tabs for providing input:

- Local Modem

  To allow connectivity over a modem, use the following steps:

  a. Click the **Local Modem** tab, then select **Allow local modem dialing for service**.

  b. If your location requires a prefix to be dialed in order to reach an outside line, click **Modem Configuration** and enter the Dial prefix (required by your location) in the Customize Modem Settings window. Click **OK** to accept the setting.

  c. Click **Add** to add a telephone number. When local modem dialing is allowed, there must be at least one telephone number configured.

- Internet

  If you want to allow connectivity over the Internet, click the **Internet** tab, and select **Allow an existing Internet connection for service**.

- Internet VPN

  If you want to configure the use of a VPN over an existing Internet connection to connect from the local HMC to your service provider's remote support facility, click the **Internet VPN** tab.

- Pass-Through Systems

  If you want to allow the HMC to use the pass-through systems as configured by the TCP/IP address or host name, click the **Pass-Through Systems** tab.

When you complete all the necessary fields, click **OK** to save your changes.

6.4.3 Manage Inbound Connectivity

To manage inbound connectivity, complete the following steps:

1. In the navigation area, click the **Serviceability** icon, and then select **Service Management**.
2. In the content pane, click **Manage Inbound Connectivity**.
3. From the Manage Inbound Connectivity settings window, use the following tabs:

   a. The **Remote Service** tab to provide the information necessary to start an attended remote service session.

   b. The **Call Answer** tab to provide the information necessary to accept incoming calls from your service provider to start an unattended remote service session.
4. Click **OK** to proceed with your selections.

6.4.4 Manage Customer Information

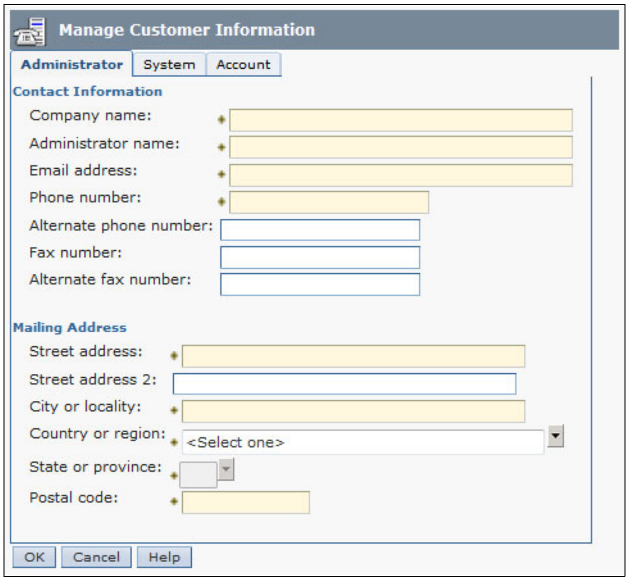
Use this task to customize the customer information for the HMC.

> **Note:** If Customizable Data Replication is Enabled on this HMC (using the Manage Data Replication task), the data specified in this task may change depending on automatic replication from other HMCs configured on your network.

To customize your customer information, complete the following steps:

1. In the navigation area, click the **Serviceability** icon, and then select **Service Management**.
2. In the content pane, click **Manage Customer Information**.

   The Manage Customer Information window opens (Figure 6-13).



Manage Customer Information

Contact Information

Company name: *

Administrator name: *

Email address: *

Phone number: *

Alternate phone number:

Fax number:

Alternate fax number:

Mailing Address

Street address: *

Street address 2:

City or locality: *

Country or region: * <Select one>

State or province: *

Postal code: *

Figure 6-13 Manage Customer Information window

3. Provide information for the fields on the following tabs and then click **OK** when done:
   - Administrator
   - System
   - Account

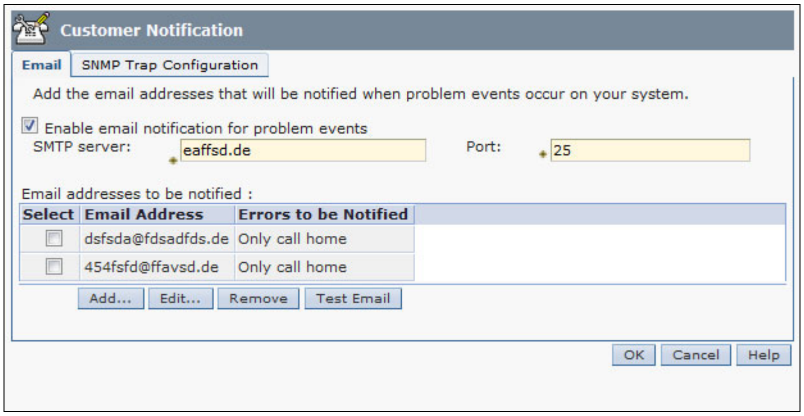
   > **Note:** Information is required for fields with an asterisk (*).

6.4.5 Manage Serviceable Event Notification

Use this task to add email addresses that notify you when problem events occur on your system and configure how you want to receive notification of system events from the Electronic Service Agent.

To set up notification, complete the following steps:

1. In the navigation area, click the **Serviceability** icon, and then select **Service Management**.
2. In the content pane, click **Manage Serviceable Event Notification**.
3. From the next window (Figure 6-14 on page 438), you can do the following tasks:
   - Click the **Email** tab and then add email addresses that will be notified when problem events occur on your system.
   - Click the **SNMP Trap Configuration** tab and then specify locations for sending Simple Network Management Protocol (SNMP) trap messages for HMC API events.
4. Click **OK**.



Add the email addresses that will be notified when problem events occur on your system.

☑ Enable email notification for problem events

SMTP server: eaffsd.de

Port: 25

Email addresses to be notified :

Select	Email Address	Errors to be Notified
☐	dsfsda@fdsadfds.de	Only call home
☐	454fsfd@ffavsd.de	Only call home

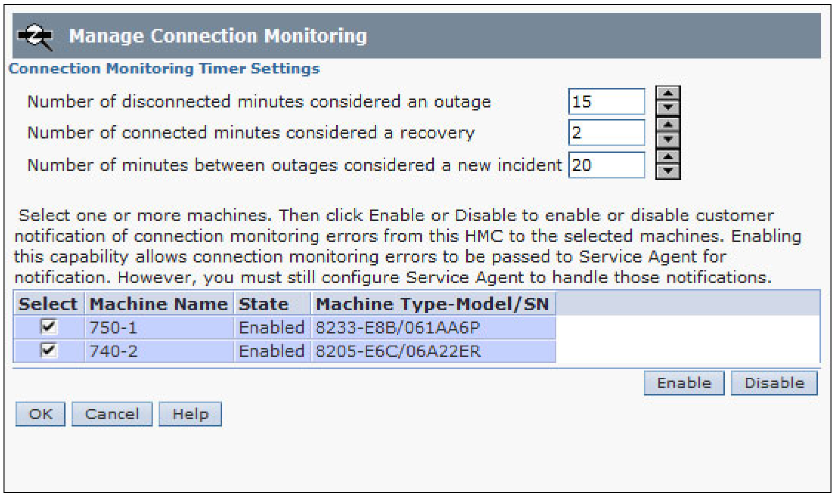
Figure 6-14 Customer Notification window

6.4.6 Manage Connection Monitoring

You can view and, if authorized, change connection monitoring settings by machine. Connection monitoring generates serviceable events when communication problems are detected between the HMC and managed systems. If you disable connection monitoring, no serviceable events are generated for networking problems between the selected machine and this HMC.

To monitor the connections, complete the following steps:

1. In the navigation area, click the **Serviceability** icon, and then select **Service Management**.
2. In the content pane, click **Manage Connection Monitoring**.
3. From the Manage Connection Monitoring window (Figure 6-15), adjust the timer settings, if necessary, and enable or disable the server.
4. Click **OK**.



Connection Monitoring Timer Settings

Number of disconnected minutes considered an outage 15

Number of connected minutes considered a recovery 2

Number of minutes between outages considered a new incident 20

Select one or more machines. Then click Enable or Disable to enable or disable customer notification of connection monitoring errors from this HMC to the selected machines. Enabling this capability allows connection monitoring errors to be passed to Service Agent for notification. However, you must still configure Service Agent to handle those notifications.

Select	Machine Name	State	Machine Type-Model/SN
☑	750-1	Enabled	8233-E8B/061AA6P
☑	740-2	Enabled	8205-E6C/06A22ER

Figure 6-15 Manage Connection Monitoring

6.5 Hardware operations

Add, exchange, or remove hardware from the managed system. Display a list of installed field-replaceable units (FRUs) or enclosures and their locations. Select the FRU or enclosure and launch a guided procedure to add, exchange, or remove the unit.

To open the hardware tasks that are available for your system, complete the following steps:

1. In the navigation area, click the **Resources** icon, and then select **All Systems**.
2. Select the server for which you want to manage hardware tasks.
3. In the menu, expand **Serviceability** and then click **Serviceability**.
4. From the list of tasks, select the hardware task that you want to do.

6.5.1 Power On/Off IO Unit

Use the Power On/Off IO Unit task to power on or off an IO unit, see Figure 6-16.

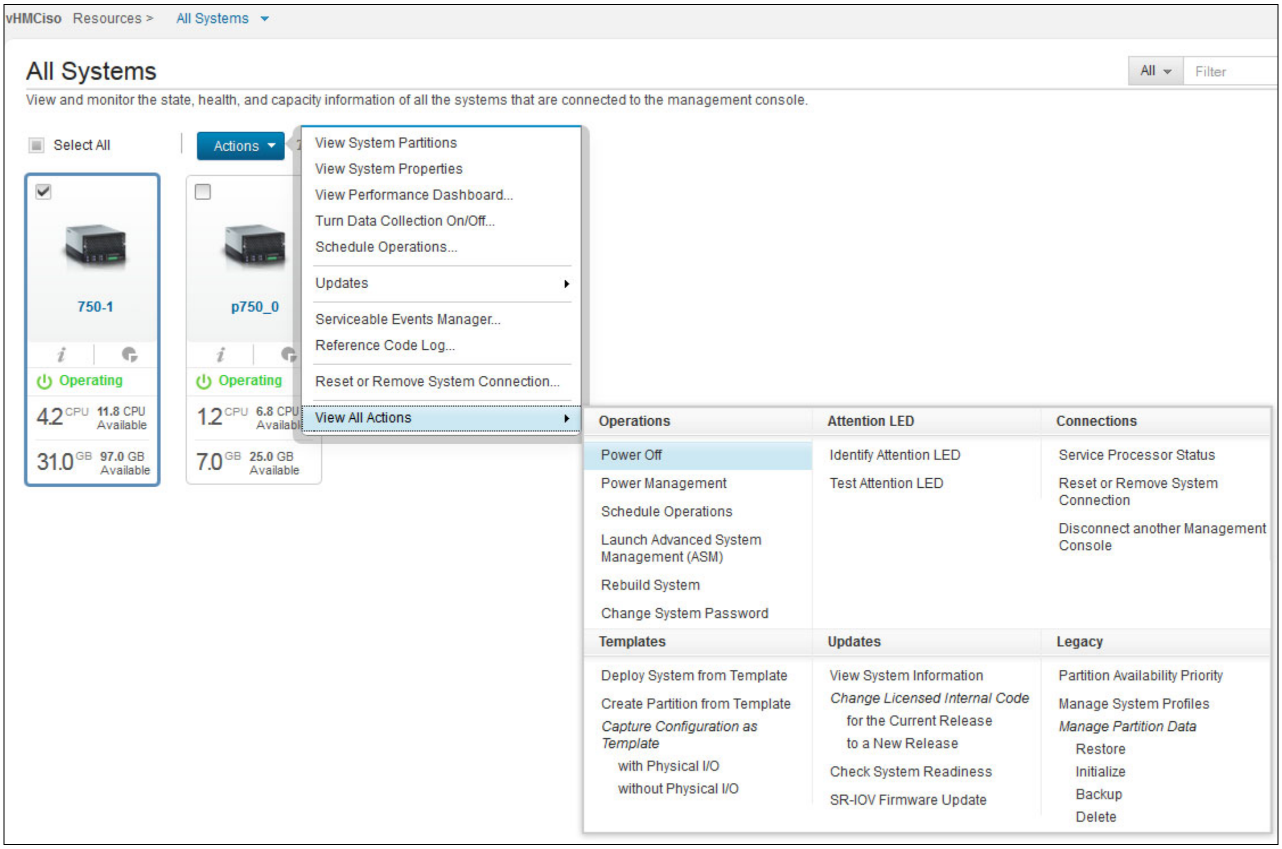

vHMCiso Resources > All Systems
All Systems
View and monitor the state, health, and capacity information of all the systems that are connected to the management console.
All
Filter
Select All
Actions
750-1
p750_0
Operating
Operating
4.2 CPU 11.8 CPU Available
31.0 GB 97.0 GB Available
1.2 CPU 6.8 CPU Available
7.0 GB 25.0 GB Available
View System Partitions
View System Properties
View Performance Dashboard...
Turn Data Collection On/Off...
Schedule Operations...
Updates
Serviceable Events Manager...
Reference Code Log...
Reset or Remove System Connection...
View All Actions
Operations
Power Off
Power Management
Schedule Operations
Launch Advanced System Management (ASM)
Rebuild System
Change System Password
Attention LED
Identify Attention LED
Test Attention LED
Connections
Service Processor Status
Reset or Remove System Connection
Disconnect another Management Console
Templates
Deploy System from Template
Create Partition from Template
Capture Configuration as Template
with Physical I/O
without Physical I/O
Updates
View System Information
Change Licensed Internal Code
for the Current Release
to a New Release
Check System Readiness
SR-IOV Firmware Update
Legacy
Partition Availability Priority
Manage System Profiles
Manage Partition Data
Restore
Initialize
Backup
Delete

Figure 6-16 Power ON/OFF menu

Only units or slots that reside in a power domain can be powered on or off. The corresponding power on/off buttons are disabled for location codes that are not controllable by the HMC.

6.5.2 Add FRU

Use the Add FRU task to locate and add a field-replaceable unit (FRU).

Figure 6-17 highlights the Add FRU, Exchange FRU, and Remove FRU tasks.

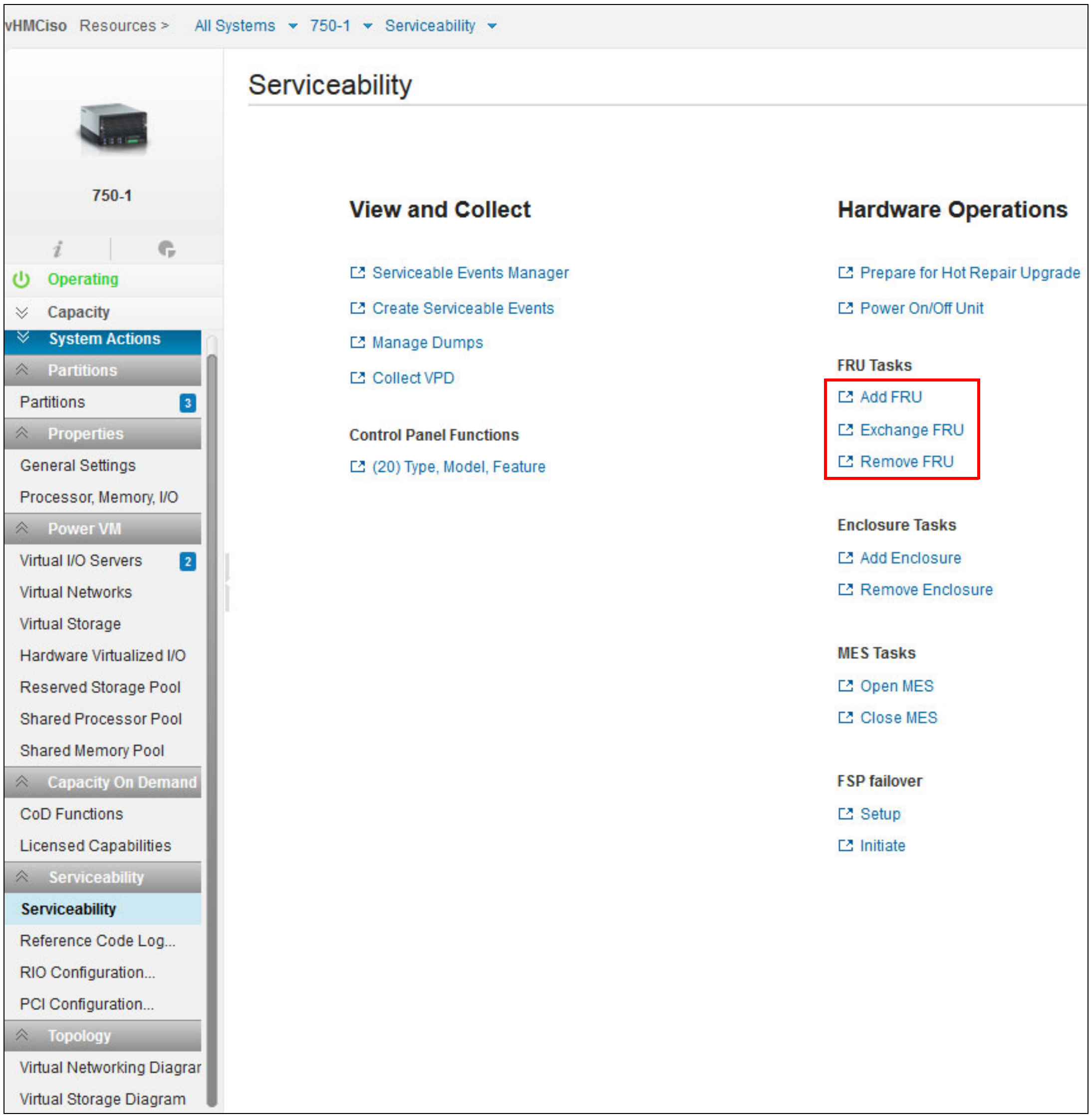


Figure 6-17 Exchanging FRU parts

To add a field-replaceable unit, complete the following tasks:

1. Select an enclosure type from the drop down list.
2. Select an FRU type from the list.
3. Click **Next.**
4. Select a location code from the displayed list.
5. Click **Add**.
6. Click **Launch Procedure**.
7. After the FRU installation process completes, click **Finish**.

6.5.3 Exchange FRU

Use the Exchange FRU task to exchange one FRU with another. See Figure 6-17 on page 440.

To exchange a field-replaceable unit, complete the following steps:

1. Select an installed enclosure type from the list.
2. From the displayed list of FRU types for this enclosure, select an FRU type.
3. Click **Next** to display a list of locations for the FRU type.
4. Select a location code for a specific FRU.
5. Click **Add** to add the FRU location to **Pending Actions**.
6. Select **Launch Procedure** to begin replacing the FRUs listed in **Pending Actions**.
7. Click **Finish** after you complete the installation.

6.5.4 Remove FRU

Use the Remove FRU task to remove an FRU from your managed system. See Figure 6-17 on page 440.

To remove a field-replaceable unit, complete the following steps:

1. Select an enclosure from the drop down list to display a list FRU types currently installed in the selected enclosure.
2. From the displayed list of FRU types for this enclosure, select an FRU type.
3. Click **Next** to display a list of locations for the FRU type.
4. Select a location code for a specific FRU.
5. Click **Add** to add the FRU location to **Pending Actions**.
6. Select **Launch Procedure** to begin removing the FRUs listed in **Pending Actions**.
7. Click **Finish** after the removal procedure completes.

6.5.5 Add Enclosure

Use the Add Enclosure task to exchange one enclosure for another.

Figure 6-18 highlights the Add Enclosure and Remove Enclosure tasks.

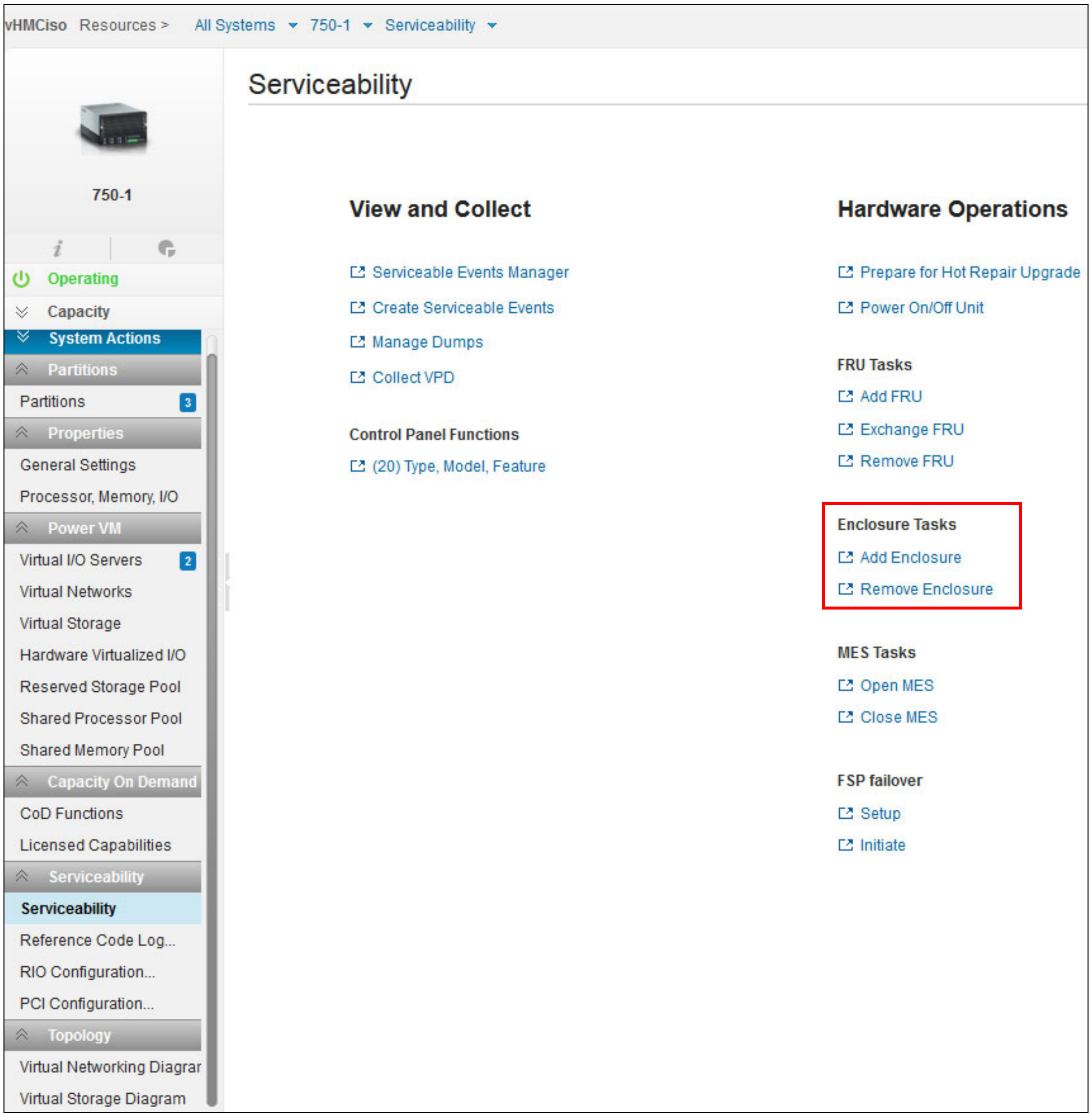
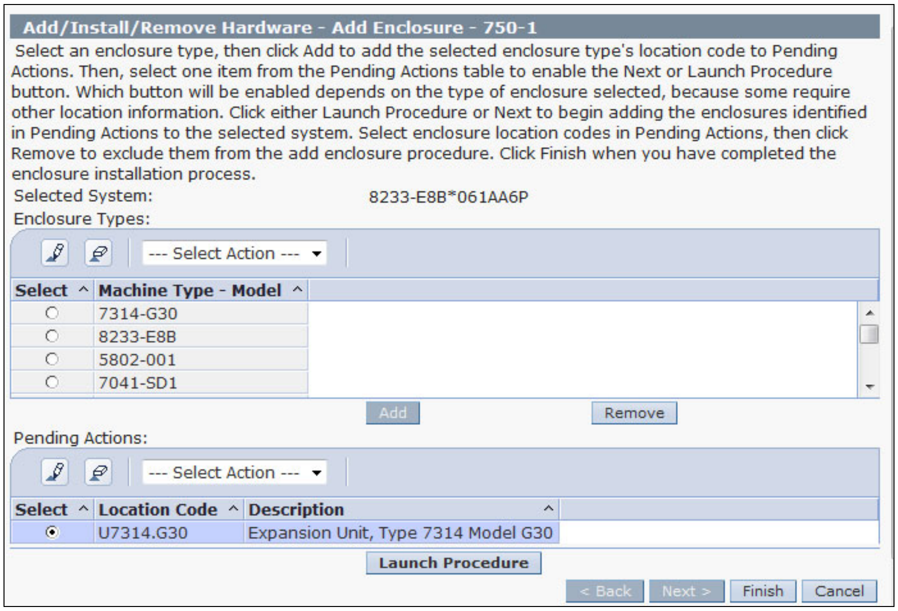


Figure 6-18 Add/ Remove Enclosure menu

To add an enclosure, complete the following steps, as shown in Figure 6-19 on page 443:

1. Select an enclosure type, then click **Add**.
2. Click **Launch Procedure**.
3. After you complete the enclosure installation process, click **Finish**.



Add/Install/Remove Hardware - Add Enclosure - 750-1

Select an enclosure type, then click Add to add the selected enclosure type's location code to Pending Actions. Then, select one item from the Pending Actions table to enable the Next or Launch Procedure button. Which button will be enabled depends on the type of enclosure selected, because some require other location information. Click either Launch Procedure or Next to begin adding the enclosures identified in Pending Actions to the selected system. Select enclosure location codes in Pending Actions, then click Remove to exclude them from the add enclosure procedure. Click Finish when you have completed the enclosure installation process.

Selected System: 8233-E8B*061AA6P

Enclosure Types:

Select	Machine Type - Model
○	7314-G30
○	8233-E8B
○	5802-001
○	7041-SD1

Pending Actions:

Select	Location Code	Description
●	U7314.G30	Expansion Unit, Type 7314 Model G30

Figure 6-19 Add/Install/Remove Hardware window

6.5.6 Remove Enclosure

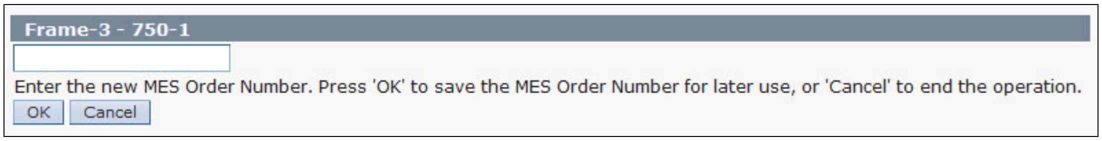
Use the Remove Enclosure task to remove an enclosure. See Figure 6-18 on page 442.

To remove an enclosure, complete the following steps and see Figure 6-19:

1. Select an enclosure type, then click **Remove** to remove the selected enclosure type's location code to **Pending Actions**.
2. Click **Launch Procedure** to begin removing the enclosures identified in **Pending Actions** from the selected system.
3. Click **Finish** after you complete the enclosure removal process.

6.5.7 Open MES

View MES order numbers and their states, for any MES operations that are active or inactive for the HMC (Figure 6-20).



Frame-3 - 750-1

Enter the new MES Order Number. Press 'OK' to save the MES Order Number for later use, or 'Cancel' to end the operation.

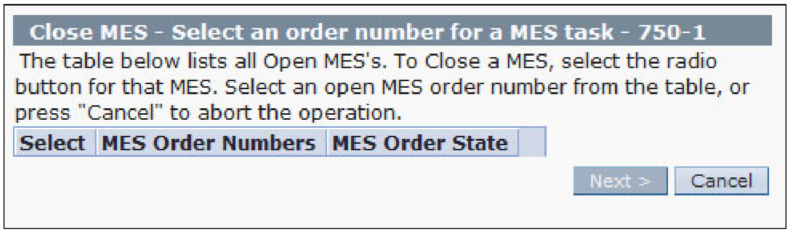
Figure 6-20 Add MES Order Number window

Use Add MES Order Number to add a new number to the list as follows:

1. Click **Add MES Order Number**.
2. Enter new MES Order number.
3. Click **OK**.

6.5.8 Close MES

View all open MES order numbers and their states (Figure 6-21).



Close MES - Select an order number for a MES task - 750-1

The table below lists all Open MES's. To Close a MES, select the radio button for that MES. Select an open MES order number from the table, or press "Cancel" to abort the operation.

Select	MES Order Numbers	MES Order State

Figure 6-21 Close MES window

Use Close MES Order Number to close an MES as follows:

1. Select an open MES order number from the table.
2. Click **OK**.

6.5.9 Set up service processor failover

Set up a secondary service processor if your managed system's primary service processor fails. If a redundant service processor is supported for the current system configuration, set up service processor failover.

Service processor failover is designed to reduce customer outages due to service processor hardware failures.

Figure 6-22 on page 445 highlights the Setup and Initiate service processor failover tasks.

Complete the following steps to set up service processor failover for the selected managed system:

1. In the content pane, click the **Setup** service processor failover task.
2. Click **OK** to enable automatic failover for the selected system.

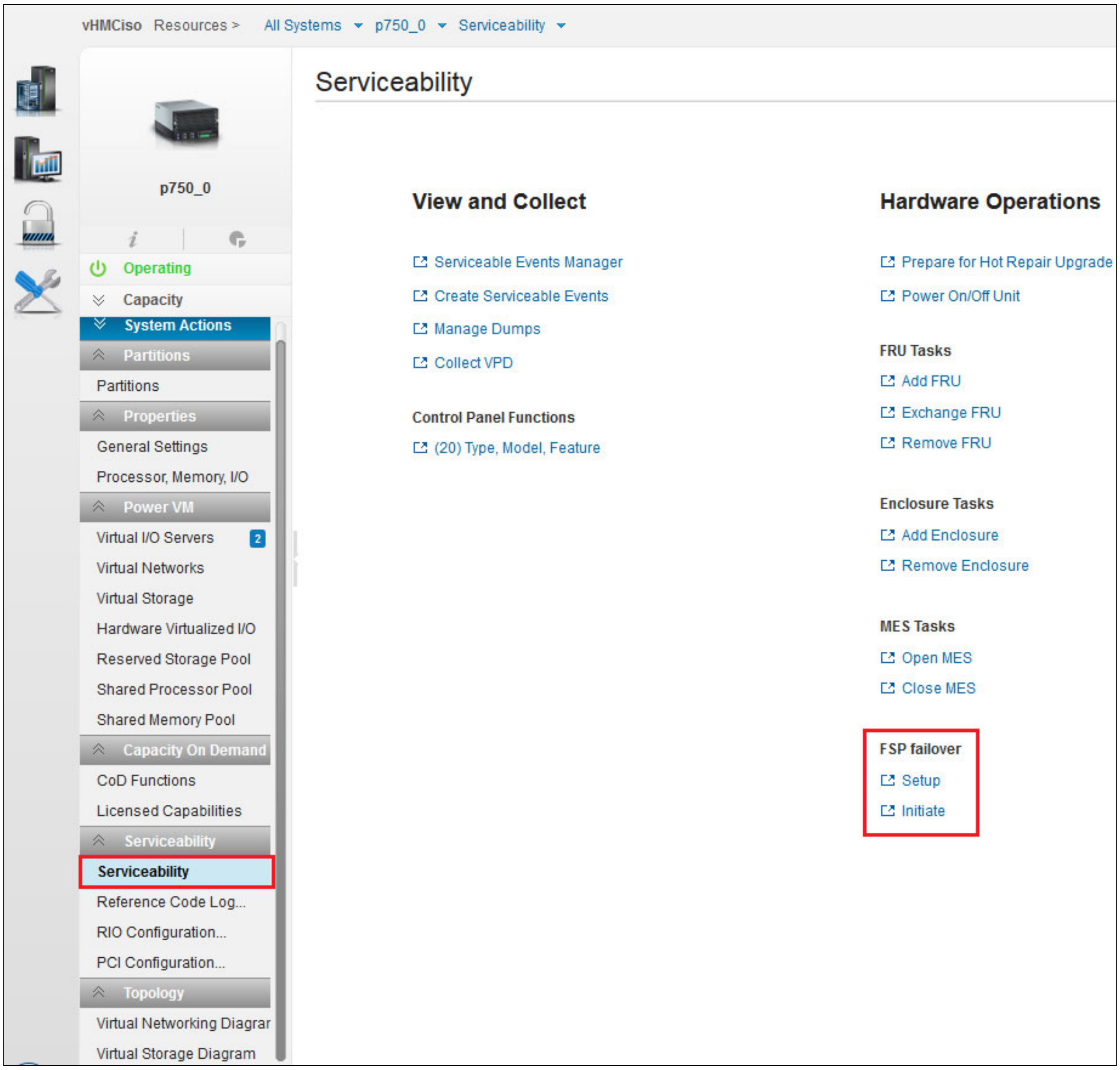


Figure 6-22 Service processor (FSP) failover tab view

6.5.10 Initiate service processor failover

Initiate a secondary service processor if your managed system’s primary service processor fails.

Service processor failover is designed to reduce customer outages due to service processor hardware failures.

Figure 6-22 highlights the Setup and Initiate service processor failover tasks.

Complete these steps to initiate service processor failover for the selected managed system:

1. In the content pane under **FSP failover**, click **Initiate**.
2. Click **OK** to initiate the automatic failover for the selected system.

6.6 Software maintenance introduction

Various options are available for maintaining both HMC and managed system firmware levels.

The following information is described:

- The main firmware update options; examples are also provided.
- The various methods of updating the HMC to a new software level and installing individual fix packs.
- The temporary and permanent side of the firmware on a POWER8.
- The various options available to POWER8 system’s firmware, either through the HMC or through an AIX service partition.

6.7 HMC Data backup

Before you begin any firmware upgrade, be sure you maintain a current HMC Data backup or Critical Console Data (CCD) backup. This back up can be useful in recovering the HMC in the event of the loss of a disk drive.

When you move to a new version level of HMC or use a Recovery CD to update the HMC, you must create an HMC Data backup immediately following the installation. If you update HMC code between releases by using the Corrective Service files downloadable from the web and then create new HMC Data backups after the update, you can use those HMC Data backups and the last-used recovery CD to rebuild the HMC to the level in use when the disk drive was lost.

Another example where an HMC Data backup can be useful is when replacing a service processor or Bulk Power Controller (BPC) on a Power6, Power7, and Power8 processor-based server. You must make a fresh HMC Data backup *before* starting the replacement to preserve the DHCP lease file on the HMC that lists the starting service processor and BPC IP addresses. If for some reason, operations do not work after you replace the service processor or BPC, you can use the backup to restore the original information. If the replacement is successful, a new IP address is assigned to the new component, and the lease file is updated. A new HMC Data backup is created that captures the freshly updated DHCP lease file.

With the HMC, you can back up the following important data:

- User-preference files
- User information
- HMC platform-configuration files
- HMC log files
- HMC updates through Install Corrective Service

Use the archived data only with a reinstallation of the HMC from the product CDs.

Note: You cannot restore the HMC Data backup on different versions of HMC software.

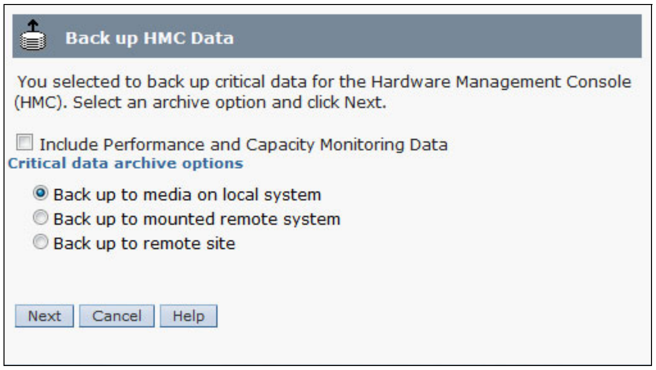
Manual backup of HMC Data

To back up the HMC, you must be a member of one of the following roles:

- Super administrator
- Operator
- Service representative

You must format the DVD in the DVD-RAM format *before* you can save data to the DVD. To format a DVD, select **HMC Management** → **Format Media** from the HMC workplace window (Figure 6-23).

To back up HMC Data, click **HMC Management** → **Backup HMC Data**.



Back up HMC Data

You selected to back up critical data for the Hardware Management Console (HMC). Select an archive option and click Next.

□ Include Performance and Capacity Monitoring Data

Critical data archive options

● Back up to media on local system
○ Back up to mounted remote system
○ Back up to remote site

Figure 6-23 Back up HMC Data menu

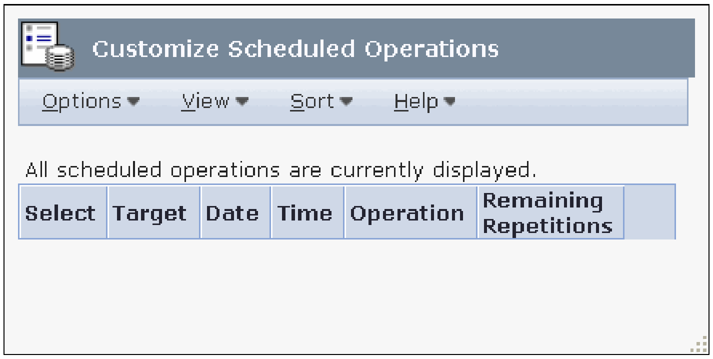
Then, select an archive option. You can back up to a local media (DVD or USB flash memory device) on the HMC, back up to a remote system mounted to the HMC file system or a remote site through FTP. After you select an option, click **Next** and follow the instructions to back up the data.

Scheduled HMC Data backup

Back up the HMC Data up at least once each week. Also keep two copies of the HMC Data backup: one copy from the upgrade or any changes to the HMC, and one backup HMC Data to store in a safe place. For information about how to make a backup, see the beginning of this section (6.7, “HMC Data backup” on page 446).

To schedule a backup, select **HMC Management** → **Schedule Operations** from the HMC workplace window. Then, follow these steps:

1. In the Customize Scheduled Operations window (Figure 6-24), select **Options** → **New**.



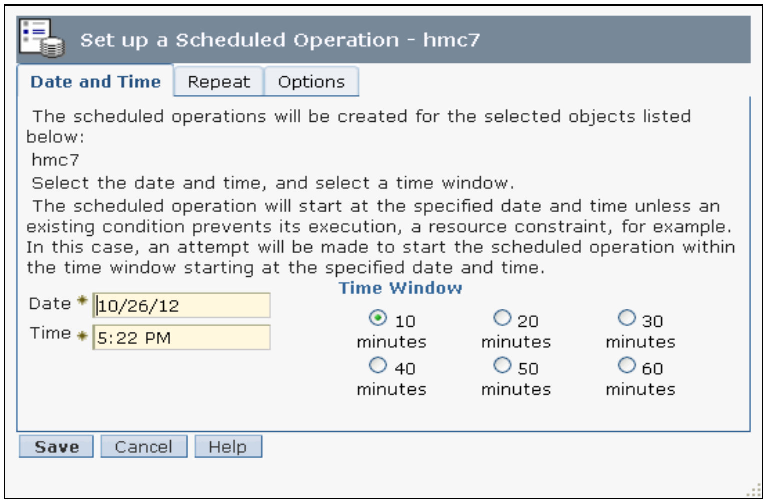
Customize Scheduled Operations

All scheduled operations are currently displayed.

Select	Target	Date	Time	Operation	Remaining Repetitions

Figure 6-24 Customize Scheduled Operations window

2. In the Add a Scheduled Operation window, select **OK**.
3. On the Date and Time tab (Figure 6-25), select the date and time, and time window for the first backup. The scheduled operation starts at that *time window*.



Set up a Scheduled Operation - hmc7

Date and Time | Repeat | Options

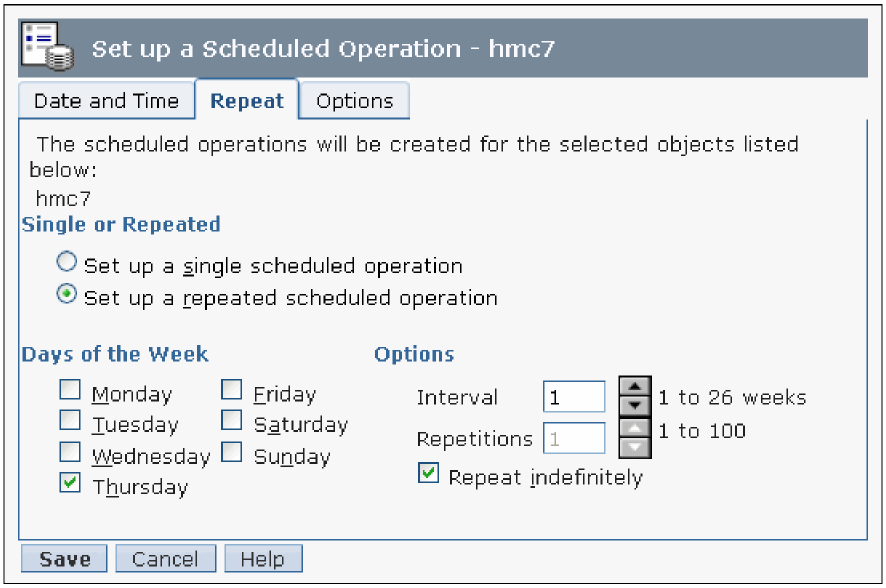
The scheduled operations will be created for the selected objects listed below:
hmc7
Select the date and time, and select a time window.
The scheduled operation will start at the specified date and time unless an existing condition prevents its execution, a resource constraint, for example. In this case, an attempt will be made to start the scheduled operation within the time window starting at the specified date and time.

Date * 10/26/12
Time * 5:22 PM

Time Window
● 10 minutes ○ 20 minutes ○ 30 minutes
○ 40 minutes ○ 50 minutes ○ 60 minutes

Figure 6-25 Set up a Scheduled Operation window on the Date and Time tab

4. On the Repeat tab (Figure 6-26), select the repeat options for the backup.



Set up a Scheduled Operation - hmc7

Date and Time | Repeat | Options

The scheduled operations will be created for the selected objects listed below:
hmc7

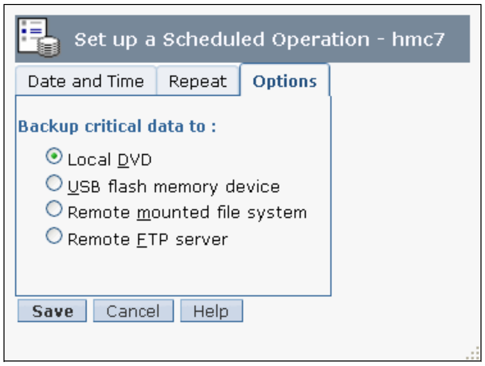
Single or Repeated
○ Set up a single scheduled operation
● Set up a repeated scheduled operation

Days of the Week
□ Monday □ Friday
□ Tuesday □ Saturday
□ Wednesday □ Sunday
☑ Thursday

Options
Interval 1 1 to 26 weeks
Repetitions 1 1 to 100
☑ Repeat indefinitely

Figure 6-26 Scheduled backup HMC Data Repeat tab

5. On the Options tab (Figure 6-27), select locations of where you want to back up the data.



Set up a Scheduled Operation - hmc7

Backup critical data to :

● Local DVD
○ USB flash memory device
○ Remote mounted file system
○ Remote FTP server

Figure 6-27 Scheduled HMC Data backup storage Options tab

6. Click **Save**. Then, click **OK**.
7. After you save the scheduled operations, you can view the operations by selecting **HMC management** → **Schedule Operations**. Select the backup scheduled operation and then click **View**.

6.8 Restoring HMC data

Various ways are available for restoring HMC Data, depending on the option that you use to back up the data. These options are described next.

Restoring data from removable media

Restore HMC Data from the menu that is displayed at the end of the HMC reinstallation. You can choose one removable media type: a DVD backup, or USB flash memory device backup.

- To restore from DVD, insert the DVD that contains the archived HMC data and select the DVD option.
- To restore from a USB flash memory device, insert the USB flash memory device in one of the HMC USB ports, and select **Restore** from USB flash memory device.

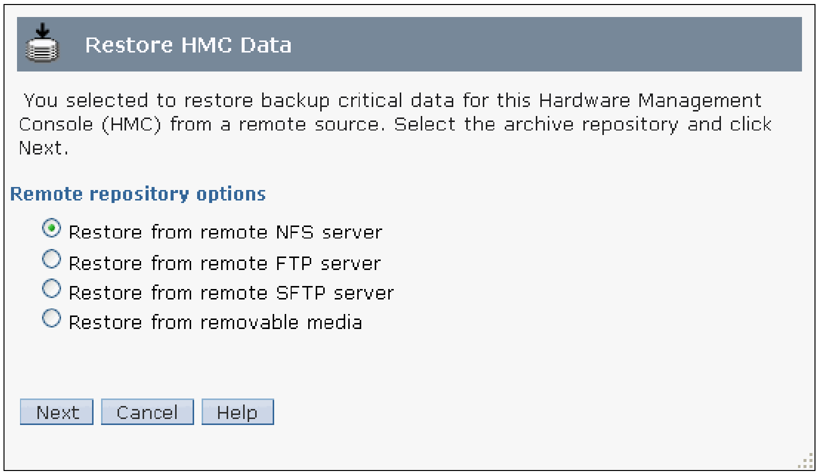
On the first start of the newly installed HMC, the data is restored automatically. This option also works after the installation of the HMC is done.

Restoring data from FTP, SFTP, NFS, or removable media

If the critical console data was archived remotely either on an FTP server or remote file system, follow these steps (and see Figure 6-28 on page 450):

1. Manually reconfigure network settings to enable access to the remote server after the HMC is installed. For information about configuring network settings, see 4.1, “Network configuration” on page 260.
2. In the HMC workplace window, select **HMC Management** → **Restore HMC Data**. Then, select the type of restoration and click **Next**.

3. Follow the directions to restore the HMC Data. The data restores automatically from the remote server when the system restarts.



Restore HMC Data

You selected to restore backup critical data for this Hardware Management Console (HMC) from a remote source. Select the archive repository and click Next.

Remote repository options

● Restore from remote NFS server
○ Restore from remote FTP server
○ Restore from remote SFTP server
○ Restore from removable media

Figure 6-28 Restore HMC Data menu from HMC management

6.9 Updating, upgrading, and migrating your HMC machine code

Updates and upgrades are periodically released for the HMC to add new functionality and to improve existing features. Migrating moves the data to another version. Learn more about the differences between updating, upgrading, and migrating your HMC machine code. Also learn how to perform an HMC machine code update, upgrade, or migration.

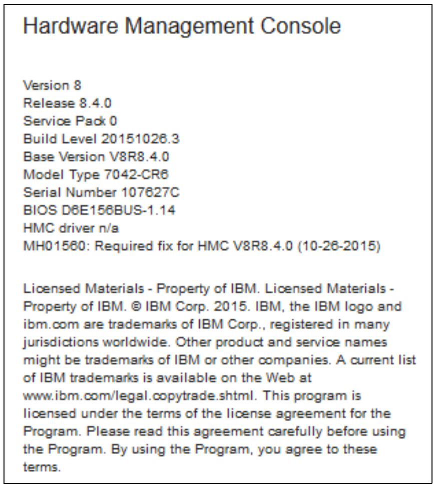
When you are finished with each of these tasks, the HMC reboots but the partitions do not:

- Updating HMC code:
  - Applies maintenance to an existing HMC level.
  - Does not require that you perform the Save upgrade data task.
- Upgrading HMC code:
  - Replaces HMC software with a new release or fix level of the same program.
  - Requires that you boot from recovery media.
- Migrating HMC code:
  - Moves HMC data from one HMC version to another.
  - Is a type of upgrade.

6.9.1 Determining your HMC machine code version and release

The level of machine code on the HMC will determine the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

To determine the HMC machine code version and release, click the **Help** icon (in the navigation area) and select the **About** tab. You see the version view (Figure 6-29).



Hardware Management Console

Version 8
Release 8.4.0
Service Pack 0
Build Level 20151026.3
Base Version V8R8.4.0
Model Type 7042-CR6
Serial Number 107627C
BIOS D6E156BUS-1.14
HMC driver n/a
MH01560: Required fix for HMC V8R8.4.0 (10-26-2015)

Licensed Materials - Property of IBM. Licensed Materials - Property of IBM. © IBM Corp. 2015. IBM, the IBM logo and ibm.com are trademarks of IBM Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal.copytrade.shtml. This program is licensed under the terms of the license agreement for the Program. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.

Figure 6-29 HMC version view

6.9.2 Applying machine code updates for the HMC with an Internet connection

The five steps described in this section are as follows:

- Step 1. Ensure that you have an Internet connection
- Step 2. Determine your existing HMC machine code level and release
- Step 3. View the available HMC machine code levels
- Step 4. Apply the HMC machine code update
- Step 5. Verify that the HMC machine code update installed successfully

Step 1. Ensure that you have an Internet connection

To download updates from the service and support system or website to your HMC or server, you must have one of the following prerequisites:

- SSL connectivity with or without a SSL proxy
- Internet VPN

Ensure that you have an Internet connection, as follows:

1. In the navigation area, click **Service Management**.
2. Select **Manage Outbound Connectivity**.
3. Click **Configure** to confirm outbound connectivity.

> **Note:** If a connection to service and support does not exist, set up the service connection before proceeding with this procedure. For instructions to set up a connection to service and support, see 6.3.4, “Transmit Service Information” on page 431.

4. Click **Test**.

5. Verify that the test completes successfully. If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on DVD.
6. Continue with Step 2. Determine your existing HMC machine code level and release.

Step 2. Determine your existing HMC machine code level and release

Determine the HMC machine code version and release, as follows:

1. In the navigation area, click the **HMC Management** icon, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that is listed under the Current HMC Driver Information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Continue with Step 3. View the available HMC machine code levels.

Step 3. View the available HMC machine code levels

View the available HMC machine code levels, as follows:

1. From a computer or server with an Internet connection, go to IBM Fix Central:

   `http://www.ibm.com/support/fixcentral/`
2. Select the appropriate product in the product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console page is displayed.
5. Scroll to your HMC Version level to view available HMC levels.

   Note: If you prefer, you can contact service and support.
6. Continue with Step 4. Apply the HMC machine code update.

Step 4. Apply the HMC machine code update

Apply the HMC machine code update, as follows:

1. Before you install updates to the HMC machine code, back up critical console information on your HMC. Then continue with the next step.
2. In the navigation area, click the **HMC Management** icon, and then select **Console Management.**
3. In the content pane, click **Update the Hardware Management Console**. The Install Corrective Service Wizard opens.
4. Follow the instructions in the wizard to install the update.
5. Shut down and then restart the HMC for the update to take effect.
6. Click **Log on** and launch the Hardware Management Console web application.
7. Log in to the HMC interface.
8. Continue with Step 5. Verify that the HMC machine code update installed successfully.

Step 5. Verify that the HMC machine code update installed successfully

Verify that the HMC machine code update installed correctly, as follows:

1. In the navigation area, click the **HMC Management** icon, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that is listed under the Current HMC Driver Information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code displayed is not the level that you installed, do the following steps:
   a. Select the network connection on the HMC.
   b. Retry the firmware update using a different repository.
   c. If the problem persists, contact your next level of support.

6.9.3 Applying machine code updates for the HMC using a DVD or FTP server

The five steps described in this section are as follows:

- Step 1. Determine your existing HMC machine code level and release
- Step 2. View the available HMC machine code levels
- Step 3. Obtain the HMC machine code update
- Step 4. Apply the HMC machine code update
- Step 5. Verify that the HMC machine code update installed successfully

Step 1. Determine your existing HMC machine code level and release

Determine your existing HMC machine code level, as follows:

1. In the navigation area, click the **HMC Management** icon, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Continue with Step 2. View the available HMC machine code levels.

Step 2. View the available HMC machine code levels

View the available HMC machine code levels, as follows:

1. From a computer or server with an Internet connection, go to the Fix Central website:

   `http://www.ibm.com/support/fixcentral/`

2. Scroll to your HMC Version level to view available HMC levels.

   > **Note:** If you prefer, you can contact IBM service and support.

3. Continue with Step 3. Obtain the HMC machine code update.

Step 3. Obtain the HMC machine code update

You can order the HMC machine code update through the Fix Central website, download it to an FTP server, or contact service and support.

Order the HMC machine code update through Fix Central

Use these steps to order the HMC machine code update from the Fix Central website:

1. From a computer or server with an Internet connection, go to the Fix Central website:

   `http://www.ibm.com/support/fixcentral/`

2. Under Supported HMC products, select the latest HMC level.
3. Scroll to the **File name(s) / Package** area and locate the update you want to order.
4. In the Order column, select **Go**.
5. Click **Continue** to sign in with your IBM ID.
6. Follow the prompts to submit your order.
7. Continue with Step 4. Apply the HMC machine code update.

Download the HMC machine code update to removable media

Use these steps to download the HMC machine code update to removable media:

1. From a computer or server with an Internet connection, go to the Fix Central website:

   `http://www.ibm.com/support/fixcentral/`

2. Under Supported HMC products, select the latest HMC level.
3. Scroll to the **File name(s) / Package** area and locate the update you want to download.
4. Click the update you want to download.
5. Accept the license agreement, and save the update to your removable media.
6. Continue with Step 4. Apply the HMC machine code update.

Step 4. Apply the HMC machine code update

Apply the HMC machine code update, as follows:

1. Before you install updates to the HMC machine code, follow these prerequisites:
   - Back up HMC data. If you obtained or created the update on DVD-RAM, insert it into the DVD drive on the HMC. If you obtained or created the update on a USB memory device, insert the memory device.
   - Back up critical console information on your HMC. Then continue with the next step.
2. In the navigation area, click the **HMC Management** icon, and then select **Console Management**.
3. In the content pane, click **Update the Hardware Management Console**. The Install Corrective Service Wizard opens.
4. Follow the instructions in the wizard to install the update.
5. Shut down, restart, and log in again to the HMC for the update to take effect.
6. Continue with Step 5. Verify that the HMC machine code update installed successfully.

Step 5. Verify that the HMC machine code update installed successfully

Verify that the HMC machine code update installed successfully, as follows:

1. In the navigation area, click the **HMC Management** icon, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.
3. In the new window, view and record the information that appears under the Current HMC Driver Information heading, including the HMC version, release, maintenance level, build level, and base versions.
4. Verify that the version and release match the update that you installed.
5. If the level of code displayed is not the level that you installed, do the following steps:
   a. Retry the machine code update. If you created a DVD for this procedure, use a new media.
   b. If the problem persists, contact your next level of support.

6.9.4 HMC software maintenance

The HMC is independent from the server. The server and all partitions can remain active while maintenance is done on the HMC, allowing you to easily keep your HMC at the latest maintenance level.

The HMC software level must be maintained the same as managed system firmware. HMC firmware is packaged as a full recovery DVD set or as a corrective service pack or fix image. The HMC recovery DVDs are bootable images and can be used to perform a complete recovery of the HMC (scratch installation) or an update to an existing HMC version.

A corrective fix updates the minor version level of code on the HMC. The HMC update packages are available on CDs or as downloadable, compressed files. The downloadable, compressed files have different naming formats depending on whether they are individual fixes or complete update packages:

- Individual HMC fixes:

  `MHxxxxx.zip`

  Where *xxxxx* is the HMC fix number.

- HMC update packages:

  `HMC_Update_VxRyMz_n.zip`

  Where *x* is the version number, *y* is the release number, *z* is the modification number, and *n* is the image number (if there are multiple images).

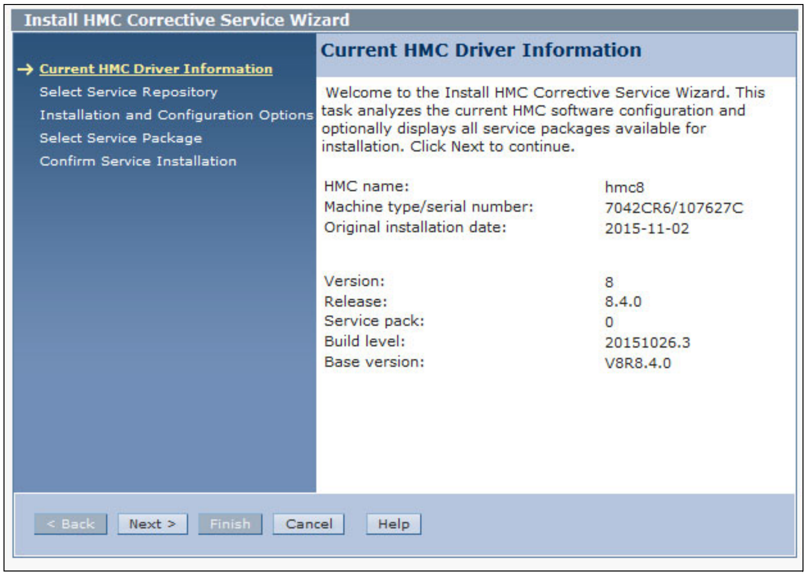
How to detect the HMC software version

The level of machine code on the HMC determines the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

To detect the HMC software version, follow these steps:

1. Click **HMC Management** icon in the HMC navigation area, and then select **Console Management**.
2. In the content pane, click **Update the Hardware Management Console**.

3. In the next window (Figure 6-30), view and record the information that is listed under the Current HMC Driver Information heading, including the HMC version, release, maintenance level, build level, and base versions.


Install HMC Corrective Service Wizard
→ Current HMC Driver Information
Select Service Repository
Installation and Configuration Options
Select Service Package
Confirm Service Installation
< Back
Next >
Finish
Cancel
Help

Current HMC Driver Information

Welcome to the Install HMC Corrective Service Wizard. This task analyzes the current HMC software configuration and optionally displays all service packages available for installation. Click Next to continue.

HMC name:	hmc8
Machine type/serial number:	7042CR6/107627C
Original installation date:	2015-11-02
Version:	8
Release:	8.4.0
Service pack:	0
Build level:	20151026.3
Base version:	V8R8.4.0

Figure 6-30 Shows the version number of HMC in Enhanced+ interface

6.9.5 Determining which firmware or fix level is correct for your system

One of the most important tasks is to determine the correct level of firmware or fix level for your system. IBM has an online tool, which is called the *Fix Level Recommendation Tool* (FLRT). The FLRT assists system administrators in formulating a maintenance plan for IBM Power Systems servers.

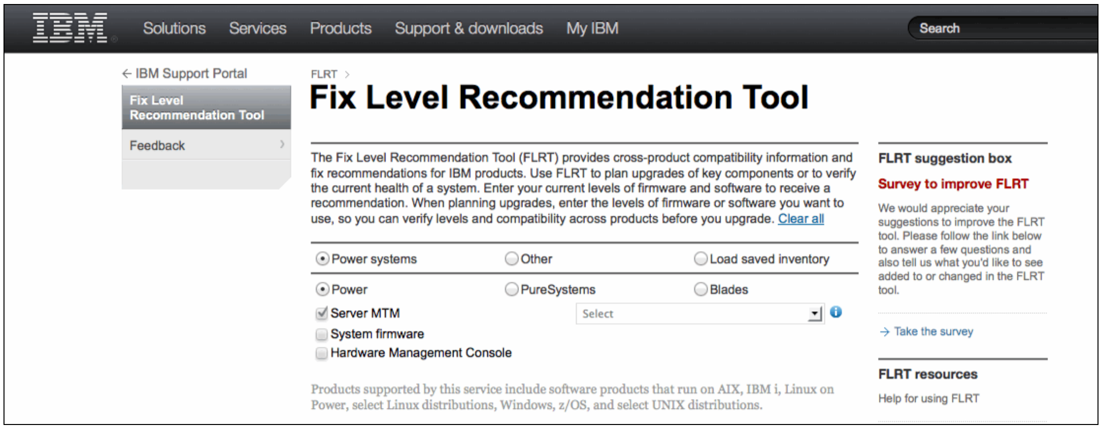
For each hardware model that you select, the tool displays fix-level information in a report for the following components:

- HMC
- System Firmware (SF)
- AIX
- Virtual I/O Server (VIOS)
- High Availability Cluster Multi-Processing (IBM HACMP™)
- General Parallel File System (IBM GPFS™)
- Cluster Systems Management (CSM)
- IBM PowerHA® SystemMirror®
- IBM Software Component: Information Management, IBM Lotus®, IBM Rational®, IBM Tivoli® software, and IBM WebSphere®

See the FLRT website:

https://www.ibm.com/support/customercare/flrt/

Figure 6-31 shows the Fix Level Recommendation Tool main page.



Fix Level Recommendation Tool

The Fix Level Recommendation Tool (FLRT) provides cross-product compatibility information and fix recommendations for IBM products. Use FLRT to plan upgrades of key components or to verify the current health of a system. Enter your current levels of firmware and software to receive a recommendation. When planning upgrades, enter the levels of firmware or software you want to use, so you can verify levels and compatibility across products before you upgrade. Clear all

● Power systems ○ Other ○ Load saved inventory

● Power ○ PureSystems ○ Blades

☑ Server MTM Select

□ System firmware

□ Hardware Management Console

Products supported by this service include software products that run on AIX, IBM i, Linux on Power, select Linux distributions, Windows, z/OS, and select UNIX distributions.

FLRT suggestion box

Survey to improve FLRT

We would appreciate your suggestions to improve the FLRT tool. Please follow the link below to answer a few questions and also tell us what you'd like to see added to or changed in the FLRT tool.

→ Take the survey

FLRT resources

Help for using FLRT

Figure 6-31 Fix Level Recommendation Tool website

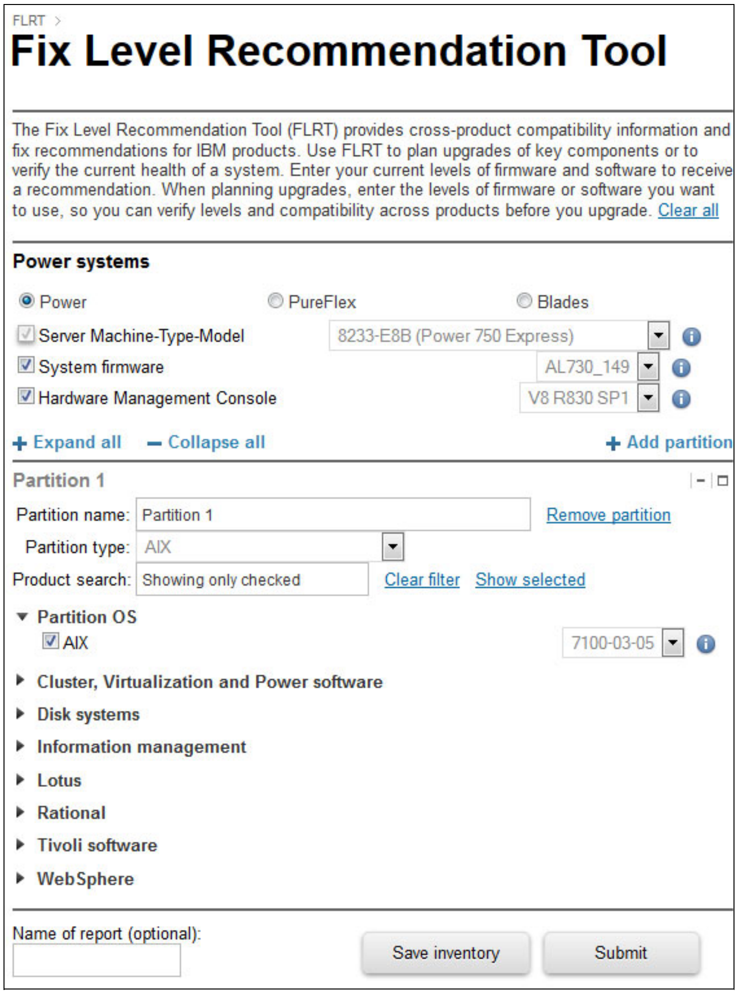
Only the products that you select on the Fix Level Recommendation Tool entry page are listed on the *inventory* page. The Fix Level Recommendation Tool is most useful for querying the combination of two or more products to ensure that they are at the recommended level and that any interdependencies are met. For example, specific system firmware levels are required for some HMC releases, and Virtual I/O Server virtualizes only a system with AIX 7.1 and later or IBM i V7R1 and later.

The report that the FLRT produces includes two sections:

- Your selected level
- The recommended minimum fix level

Selecting products for an FLRT report

On the main page of the FLRT (Figure 6-32), select the products for which you want to check recommended levels and click **Submit**.



FLRT >

Fix Level Recommendation Tool

The Fix Level Recommendation Tool (FLRT) provides cross-product compatibility information and fix recommendations for IBM products. Use FLRT to plan upgrades of key components or to verify the current health of a system. Enter your current levels of firmware and software to receive a recommendation. When planning upgrades, enter the levels of firmware or software you want to use, so you can verify levels and compatibility across products before you upgrade. Clear all

Power systems

● Power ○ PureFlex ○ Blades

☑ Server Machine-Type-Model: 8233-E8B (Power 750 Express)

☑ System firmware: AL730_149

☑ Hardware Management Console: V8 R830 SP1

Partition 1

Partition name: Partition 1

Partition type: AIX

Product search: Showing only checked

Partition OS

☑ AIX: 7100-03-05

Name of report (optional):

Figure 6-32 Fix Level Recommendation Tool product options window

FLRT product selection page

The FLRT landing page initially lists operating systems. Other products become available after an operating system is selected.

Operating system family

From this section, select the operating system running on your server, or in one of the LPARs on your server. After you choose an operating system, FLRT displays selections for Platform and Server.

Platform

From this section, choose either Power Systems or BladeCenter (POWER based processors). FLRT supports blade servers that are based on POWER technology.

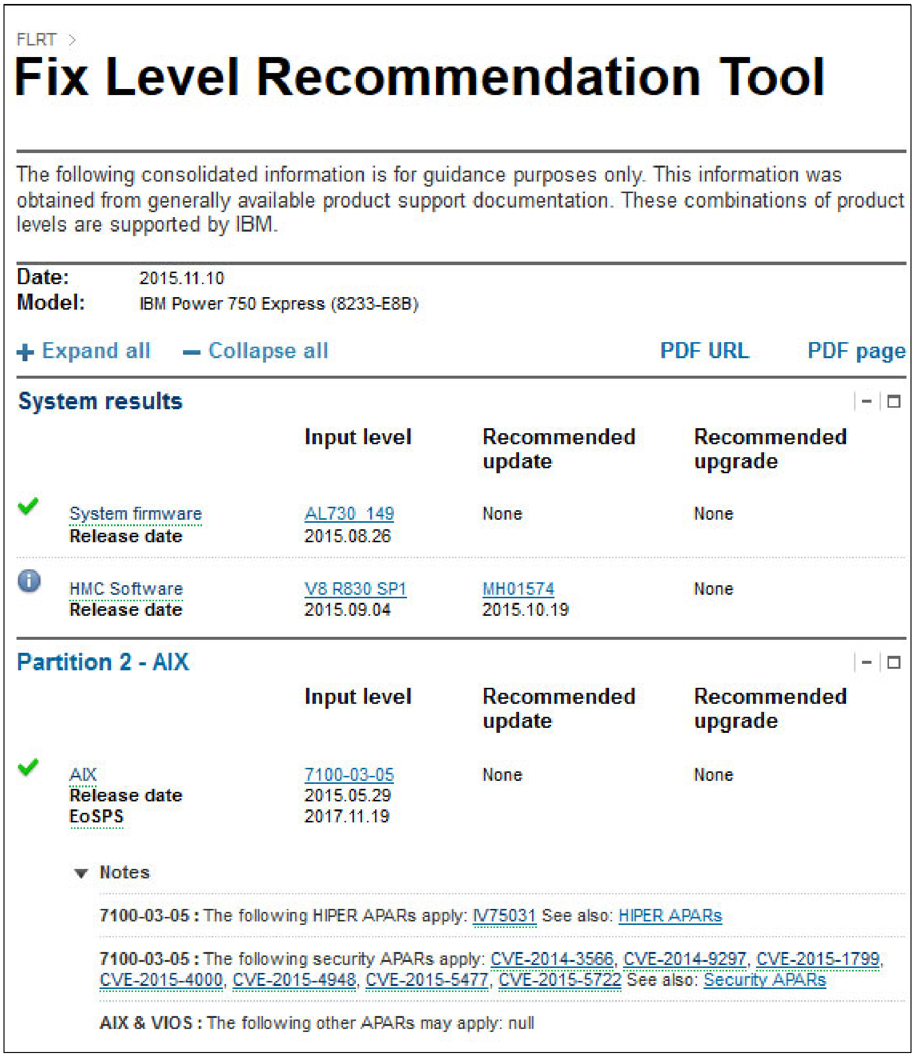
Server

Use the drop-down menu in this section to select the machine type and model (MTM) for your server and the clock speed (GHz). If only one clock speed is available for the selected server, FLRT displays that clock speed.

Enter the current details from your system. To find the current fix level of the HMC and managed system, see “How to detect the HMC software version” on page 455. Select **Submit**.

Reviewing the report

The Fix Level Recommendation Tool displays the report (Figure 6-33).



FLRT >

Fix Level Recommendation Tool

The following consolidated information is for guidance purposes only. This information was obtained from generally available product support documentation. These combinations of product levels are supported by IBM.

Date: 2015.11.10
Model: IBM Power 750 Express (8233-E8B)

+ Expand all — Collapse all PDF URL PDF page

System results

		Input level	Recommended update	Recommended upgrade
✓	System firmware **Release date**	AL730_149 2015.08.26	None	None
ⓘ	HMC Software **Release date**	V8 R830 SP1 2015.09.04	MH01574 2015.10.19	None

Partition 2 - AIX

		Input level	Recommended update	Recommended upgrade
✓	AIX **Release date** **EoSPS**	7100-03-05 2015.05.29 2017.11.19	None	None

▼ Notes

7100-03-05 : The following HIPER APARs apply: IV75031 See also: HIPER APARs

7100-03-05 : The following security APARs apply: CVE-2014-3566, CVE-2014-9297, CVE-2015-1799, CVE-2015-4000, CVE-2015-4948, CVE-2015-5477, CVE-2015-5722 See also: Security APARs

AIX & VIOS : The following other APARs may apply: null

Figure 6-33 Fix Level Recommendation Tool recommendation window

Report heading

The heading of the report lists the date and name of the report (if you entered a name). It also lists the server that you selected and the clock speed. The heading also includes a link to a page that shows you the latest firmware for the devices that are supported by your machine. You can download device firmware from that same page.

Detailed results

Product compatibility, detailed results, and fix recommendations are displayed. FLRT uses several icons to indicate the type of information that is displayed in the report (Table 6-2). More information is supplied in the report, depending on the type of result indicated.

Table 6-2 Several icons indicate the type of information in the FLRT report

✓	Ok Green check mark: Displayed when the level that you input is supported for longer than six months and the input level is the currently recommended update or latest level.
ℹ	Blue “i” (information) circle: Displayed when the input level is supported for longer than six months but there is also a recommended update available.
⚠	Yellow caution triangle: Displayed when the input level has less than six months that are left for service and there is also a recommended upgrade available. If the input level no longer has updates available, the yellow caution triangle is displayed, if there is an upgrade option.
❗	Red alert exclamation: Displayed for incompatibilities. If end of service pack support (EoSPS) is reached and no upgrade recommendation is reported, the red alert sign is also displayed.

Obtaining HMC updates and recovery software

You can order Recovery DVDs or download packages that contain the files you can save (burn) to your own Recovery DVD. The files that you use to create DVDs have an `.iso` file extension. The CDs created from these packages are bootable. You can download updates to the HMC code and emergency fixes, and you can order CDs containing the updates and fixes. The CDs containing updates and fixes are *not* bootable.

Important: If you are not sure which code level is correct for your machine, read 6.9.5, “Determining which firmware or fix level is correct for your system” on page 456.

Download the latest HMC software from the following location:

`http://www.ibm.com/support/fixcentral/options`

Upgrading the HMC machine code

To upgrade the HMC machine code, follow these steps:

1. Determine the HMC machine code level that is required for your system. See 6.9.5, “Determining which firmware or fix level is correct for your system” on page 456.
2. Obtain the recovery image. See “Obtaining HMC updates and recovery software” on page 460.
3. Back up the profile data of the managed system. In the HMC workplace window, select **System Management** → **Servers**. Then, select the server and ensure that the state is `Operating` or `Standby`.

   Under Tasks, select **Configuration** → **Manage Partition Data** → **Backup**. Enter a backup file name and record this information. Then, click **OK**.
4. Back up critical console data as described in 6.7, “HMC Data backup” on page 446.

   Back up the HMC Data: It is absolutely necessary to back up the HMC Data.

5. Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information as follows:
   a. In the HMC workplace window, select **HMC Management**. Then, in the tasks list, select **Schedule Operations**. The Scheduled Operations window displays a list of all managed systems.
   b. Select the HMC that you plan to upgrade and click **OK**. All scheduled operations for the HMC are displayed.

      Tip: If you do not have any scheduled operations, skip to step 6.

   c. Select **Sort** → **By Object**. Select each object and record the following details:
      - Object Name
      - Scheduled date
      - Operation Time (displayed in 24-hour format)
      - Repetitive

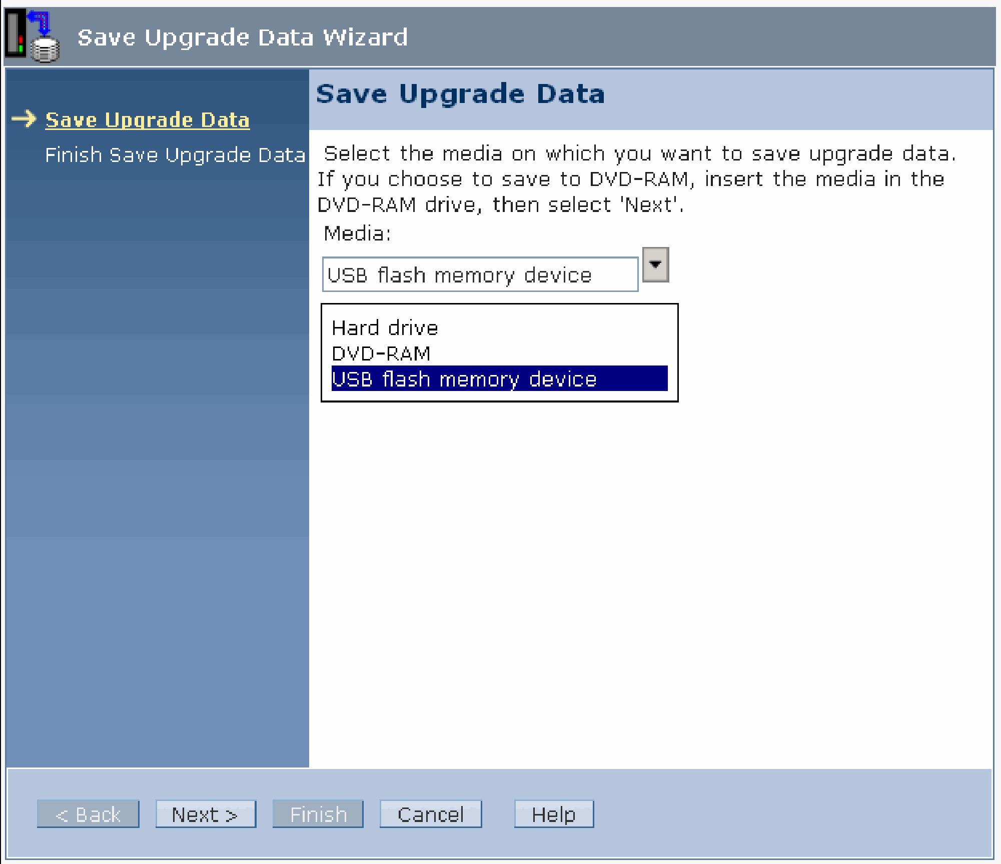
        If Yes, select **View** → **Schedule Details**. Then, record the interval information and close the scheduled operations window. Repeat for each scheduled operation.
   d. Close the Customize Scheduled Operations window.
6. Record the remote command status:
   a. In the navigation area, select **HMC Management**. Then, in the tasks list, click **Remote Command Execution**.
   b. Record whether the Enable remote command execution using the **ssh** facility check box is selected.
   c. Click **Cancel**.
7. Repeat these steps for each managed system.

Saving upgrade data

You can save the current HMC configuration in a designated disk partition on the HMC. Save upgrade data only immediately before upgrading your HMC software to a new release. Use this action in order to restore HMC configuration settings after upgrading.

Only one level of backup data is allowed: Each time that you save upgrade data, the previous level is overwritten.

HMC Version 8 also gives an option to save upgrade data on hard disk, DVD, or USB flash memory device (Figure 6-34). A strong suggestion is to save a copy on a USB flash memory device also.


Save Upgrade Data Wizard

Save Upgrade Data

Select the media on which you want to save upgrade data. If you choose to save to DVD-RAM, insert the media in the DVD-RAM drive, then select 'Next'.

Media: USB flash memory device

Figure 6-34 Save Upgrade Data wizard

To save upgrade data, complete these steps:

1. In the HMC workplace window, select **HMC Management** → **Console Management**. Then, in the tasks list, select **Save Upgrade Data**. Select **Hard drive**.

   Repeat this step, but this time select **USB flash memory device** option.
2. Click **Next**.
3. Click **Finish**.
4. Wait for the task to complete. If the Save Upgrade Data task fails, contact your next level of support before proceeding.

   > **Important:** If the save upgrade data task fails, do not continue the upgrade process.
5. Click **OK**. Then, click **Close**.

To upgrade the HMC software, complete these steps:

1. Restart the HMC with the Recovery DVD-RAM in the DVD-RAM drive by inserting the HMC Recovery DVD-RAM into the DVD-RAM drive.
2. In the navigation area, select **HMC Management** → **Console Management** → **Shutdown or Restart**. Then, select **Restart the HMC** and click **OK**.
3. The HMC restarts and boots from the bootable recovery DVD. The window shows the following options:
   - Install
   - Upgrade

   Select **Upgrade** and click **Next**.
4. When the warning displays, choose one of the following options:
   - If you saved upgrade data during the previous task, continue with the next step.
   - If you did not save upgrade data previously in this procedure, save the upgrade data now before you continue.
5. Select **Upgrade** from media and click **Next**. Confirm the settings and click **Finish**.
6. Follow the prompts as they display.

   > **If window is blank, press Spacebar:** If the window goes blank, press the Spacebar to view the information. The first DVD can take approximately 20 minutes to install.

7. Select option **1. Install additional software from media** and press Enter. Press any key to confirm the installation. The HMC displays status messages as it installs the packages.
8. When the second media installation is complete, remove the media from the drive and close the media drawer.
9. Select option **2. Finish the installation** and press Enter. The HMC completes the booting process.
10. At the login prompt, log in using your user ID and password.
11. Accept the license agreement for machine code twice. The HMC code installation is complete.
12. Verify that the HMC machine code upgrade installed successfully. See “How to detect the HMC software version” on page 455.

You completed upgrading the HMC machine code procedure.

Upgrading HMC from Version 7 to Version 8

You can upgrade your HMC Version 7.7.8 or later to HMC Version 8 while you maintain your configuration data.

> **Important:** You must be at a minimum of version 7.7.8 to upgrade to the POWER8 HMC machine code level, which is Version 8 Release 8.1.0.

Prerequisite steps

Complete the following prerequisites:

1. Verify that the HMC does not manage any POWER5 server.

   > **Note:** POWER5 servers are not supported at HMC Version 8.

   To determine if a managed system is POWER5, use the following steps:

   a. On HMC GUI, select **Updates** in left panel.

   b. In the right panel, find the System Code Levels section, which lists each system managed by this HMC.

   c. For each managed system, check the EC Number. Any system with an EC number of 01SFxxx is a POWER5.

   If an attempt is made to connect a HMC V8.8.1 or later to a POWER5 server, the state will show `Version Mismatch` with connection error `Connection not allowed`:

   ```
   resource_type=sys,type_model_serial_num=9406-520*103E8FE,sp=primary,sp_phys_loc
   =unavailable,ipaddr=9.5.66.29,alt_ipaddr=unavailable,state=Version
   Mismatch,connection_error_code=Connection not allowed 0009-0008-00000000
   ```

2. Verify HMC model is compatible with HMC V8.

   HMC V8 is supported on rack-mount models CR5, CR6, CR7,CR8, and CR9, and on desktop model C08. These listed models meet or exceed the V8 minimum memory requirement of 2 GB, however 4 GB is suggested.

3. Upgrading to HMC Version 8 requires a minimum level of 7.7.8 + MH01402, 7.7.8.0.1, or later; or 7.7.9 + mandatory fix MH01406 or later:

   – For HMC version *7.7.9*, SP1 or later is suggested. To update 7.7.9 HMC to the latest fixes, see updates for HMC 7.7.9:

     `http://www-912.ibm.com/s_dir/slkbase.NSF/DocNumber/703105966`

   – For HMC version *7.7.8*, SP1 or later is suggested. To update 7.7.8 to the latest fixes see support document updates for HMC 7.7.8:

     `http://www-912.ibm.com/s_dir/slkbase.NSF/DocNumber/690069604`

   – For HMC version *7.7.7* and earlier, use one of the following options:

     - Upgrade to 7.7.9 first, then upgrade to Version 8.
     - Do a scratch-install of Version 8, then reconfigure the HMC.

   To upgrade an HMC to 7.7.9, see support document *Upgrading the HMC from Version 7.7.x to Version 7.7.9*:

   `http://www-912.ibm.com/s_dir/slkbase.NSF/DocNumber/703169924`

4. Confirm machine type/model and serial number are correct.

   Use one of the following methods to verify that the Machine Type/Model and Serial Number (MTMS) match the information on the tag at the front of the physical HMC. If they do not match, do not attempt the upgrade. To resolve the problem, contact IBM Support and request a BIOS flash to correct the MTMS:

   a. On the HMC GUI interface, select **Updates** in the left navigation panel. Find the Model Type and Serial number in the HMC Code Level section of the right panel.

   b. From a restricted shell command line, type the following command and press Enter:

      ```
      lshmc -v
      ```

      The command returns TM type model and SE serial number.

5. Reboot the HMC.

   If the HMC has not been restarted recently, restart before you begin the upgrade. To reboot, use either the GUI task or command line:

   – GUI task: Select **HMC Management** → **Shutdown or Restart** → **Restart HMC**, and then click **OK**.

   – Command line:

     ```
     hmcshutdown -r -t now
     ```

6. Remove any USB used for HMC backup.

   Remove any USB flash drive that contains HMC Backup Management Console Data prior to performing a network upgrade. Failure to remove the drive will result in failed network upgrade.

7. Verify Server Firmware is compatible.

   For a complete list of supported combinations of HMC V7 and V8 code levels and server firmware levels, see the following web page:

   `https://ibm.biz/BdRJnK`

While the HMC can perform basic management tasks and upgrades on downlevel servers, servers below the supported level should be updated soon after the HMC upgrade is complete.

The upgrade steps

To upgrade from Version 7 to Version 8, complete the following steps:

1. Determine the HMC machine code level that is required for your system. See 6.9.5, “Determining which firmware or fix level is correct for your system” on page 456.

2. Obtain the recovery CD or DVD as described in “Obtaining HMC updates and recovery software” on page 460.

3. Back up the profile data of the managed system. In the HMC workplace window, select **System Management** → **Servers**. Select the server and ensure that the state is `Operating` or `Standby`.

   Under Tasks, select **Configuration** → **Manage Partition Data** → **Backup**. Enter a backup file name and record this information. Then, click **OK**.

   Repeat these steps for each managed system.

4. Backup Critical Console Data (CCD), HMC Data in HMC 7 Version, as described in 6.7, “HMC Data backup” on page 446.

   > **Back up:** You must back up the CCD.

5. Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information as follows:

   a. In the Navigation area, select **HMC Management** → **Console Management**. Then, in the tasks list, select **Schedule Operations**. The **Scheduled Operations** window displays with a list of all managed systems.

   b. Select the HMC that you plan to upgrade and click **OK**. All scheduled operations for the HMC are displayed.

   > **Tip:** If you do not have any scheduled operations, skip to step 6. Otherwise, continue with step c.

c. Select **Sort** → **By Object**.

d. Select each object and record the following details:

- Object Name
- Scheduled date
- Operation Time (displayed in 24-hour format)
- Repetitive

  If Yes, select **View** → **Schedule Details**. Then, record the interval information. Close the scheduled operations window. Repeat for each scheduled operation.

e. Close the Customize Scheduled Operations window.

6. Record remote command status:

   a. In the navigation area, select **HMC Management**. Then, in the tasks list click **Remote Command Execution**.

   b. Record whether the Enable remote command execution using the ssh facility check box is selected.

   c. Click **Cancel**.

7. Save the upgrade data as described in “Saving upgrade data” on page 461.

> **Attention:** If this step is not followed properly, you lose all your partition information.

8. Upgrade the HMC Software from Version 7 to Version 8.

> **Note:** You can upgrade only your HMC from Version 7 to Version 8. If you have an HMC Version 6, you need to upgrade it to Version 7 first. You need to have a recovery DVD from step 2 in this procedure.

   a. Insert the Version 8 recovery DVD in the DVD drive.

   b. In the navigation area, select **HMC Management** → **Shutdown or Restart**. Then, select **Restart the HMC** and click **OK**.

   c. The HMC restarts and boots from the bootable recovery DVD. The window shows the following options:

   - Install
   - Upgrade

   d. Select **Upgrade** and click **Next**.

   e. When the warning displays, choose one of the following options:

   - If you saved upgrade data during the previous task, continue with the next step.
   - If you did not save upgrade data previously in this procedure, you must save the upgrade data now before you continue. See previous step.

   f. Select **Upgrade** from media and click **Next**. Confirm the settings and click **Finish**. Follow the prompts as they display.

> **If blank window, press the Spacebar:** If the window is blank, press the Spacebar to view the information. Installing the first DVD takes approximately 20 minutes.

g. Select option **1. Install additional software from media** and press Enter. Press any key to confirm the installation. The HMC displays status messages as it installs the packages. When the second media installation is complete, remove the media from the drive and close the media drawer.

h. Select Option **2. Finish the installation** and press Enter. The HMC completes the booting process.

i. At the login prompt, log in using your user ID and password.

j. Accept the License Agreement for Machine Code twice. The HMC code installation is complete.

k. Verify that the HMC machine code upgrade installed successfully. See "How to detect the HMC software version" on page 455.

6.9.6 Managed system firmware updates

This section describes available options for installing system firmware. The system firmware is also referred to as *licensed internal code*. It is on the service processor.

> **Important:** The HMC machine code needs to be equal to or greater than the managed system firmware level. Also, if an HMC manages multiple servers at different firmware release levels, the HMC machine code level must be equal to or higher than the system firmware level on the server that is at the latest release level.

Firmware overview

Depending on your system model and service environment, you can download, install, and manage your server firmware updates by using different methods. The default firmware update policy for a partitioned system is through the HMC. If you do not have a HMC attached to your system, see your operating system documentation to upload the code by using the operating system.

System firmware is delivered as a *release level or a service pack*. Release levels support the general availability (GA) of new function or features and new machine types or models. Upgrading to a later release level can be disruptive to client operations. Thus, IBM intends to introduce no more than two new release levels per year. These release levels are supported by service packs. Service packs are intended to contain only firmware fixes and are not intended to introduce new functionality. A service pack is an update to an existing release level.

> **Upgrading and updating your firmware:** Installing a release level is also referred to as *upgrading* your firmware. Installing a service pack is referred to as *updating* your firmware.

The file naming convention for system firmware is as follows:

- POWER6

  EM*xxx_yyy_zzz*

  Where:

  – *xxx* is the release level
  – *yyy* is the service pack level
  – *zzz* is the last disruptive service pack level

  For example, System Firmware 01EM310_026, as displayed on the Firmware Download page, is Release Level 310, Service Pack 026.

- POWER7

  `AM`*`xxx_yyy_zzz`*

  Where:

  – *xxx* is the release level
  – *yyy* is the service pack level
  – *zzz* is the last disruptive service pack level

  For example, System Firmware 01QAM730_095, as displayed on the Firmware Download page, is Release Level 730, Service Pack 095.

- POWER8

  `SV`*`xxx_yyy_zzz`*

  Where:

  – *xxx* is the release level
  – *yyy* is the service pack level
  – *zzz* is the last disruptive service pack level

  For example, System Firmware SV830_048, as displayed on the Firmware Download page, is Release Level 830, Service Pack 048.

The service pack maintains two copies of the server firmware. One copy is held in the t-side repository (temporary) and the other copy is held in the p-side repository (permanent):

- Temporary side

  Apply new firmware updates to the t-side first and test before they are permanently applied. When you install server firmware updates on the t-side, the existing contents of the t-side should be permanently installed on the p-side first.

  A suggestion is that, under normal operations, the managed system run on the t-side version of the system firmware.

- Permanent side

  The permanent side holds the last firmware release that was running on the temporary side. You know that this firmware was running for a while on the temporary side and is stable. This method is also a good way to hold a backup firmware on the system. If for any reason your temporary firmware gets corrupted, you can start from the permanent side and recover your system.

Before you update your system firmware, move current firmware that is on the temporary side to the permanent side.

We suggest that under normal operations the managed system runs on the t-side version of the system firmware.

When you install changes to your firmware, three options are available:

- Concurrent installation and activate: Fixes can be applied without interrupting running partitions and restarting managed system.
- Concurrent installation with deferred disruptive activate: Fixes can be applied as delayed and activated the next time that the managed system is restarted.
- Disruptive installation with activate: Fixes can be applied only by turning off the managed system.

Choose the option that fits the status of the server that you are updating. For example, do not use a disruptive installation option on a production server. However, on a test server, this option might not be an issue.

Check compatibility: Always check the compatibility between HMC software and managed system firmware at the following web page:

`http://www.ibm.com/support/fixcentral/firmware/supportedCombinations`

For more details about installation instructions of firmware see the IBM Knowledge Center:

`https://www.ibm.com/support/knowledgecenter/8247-21L/p8eh6/p8eh6_updates_sys.htm?lang=en`

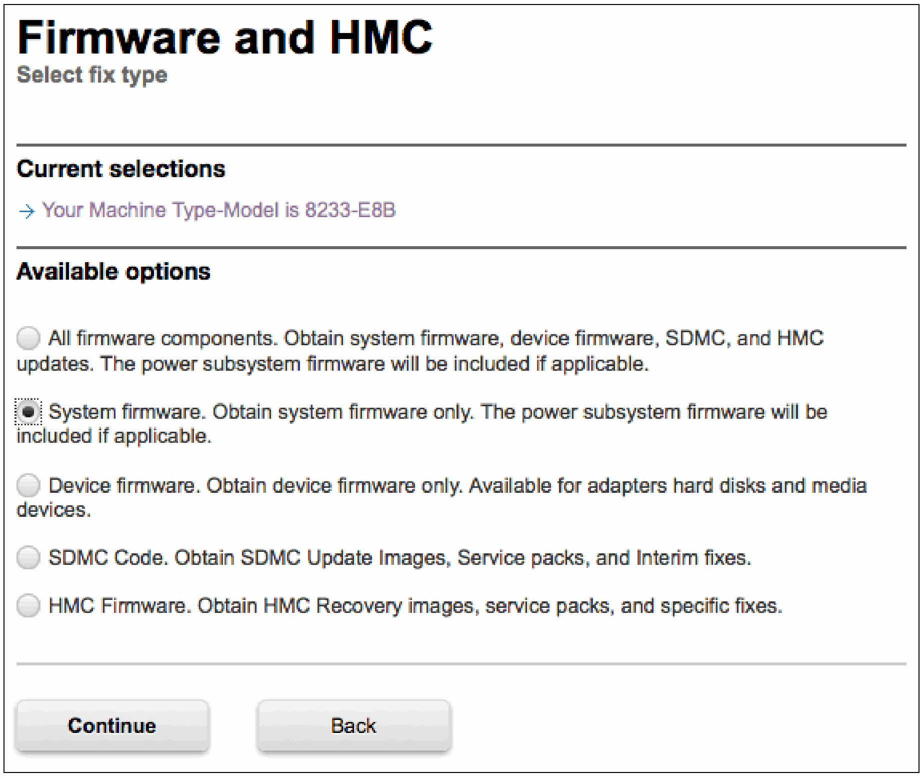
Obtaining system firmware

This section describes how to view or to download the firmware fix. Download the fix to your computer with an Internet connection and then create a fix CD that you apply on the server. If necessary, contact service and support to order the fix on CD.

You can download fixes from the following web page:

`http://www.ibm.com/support/fixcentral/options`

Repeat the same process of "Obtaining HMC updates and recovery software" on page 460 until you arrive at the HMC firmware type, and then select **System firmware** (Figure 6-35).



Firmware and HMC

Select fix type

Current selections

→ Your Machine Type-Model is 8233-E8B

Available options

○ All firmware components. Obtain system firmware, device firmware, SDMC, and HMC updates. The power subsystem firmware will be included if applicable.

● System firmware. Obtain system firmware only. The power subsystem firmware will be included if applicable.

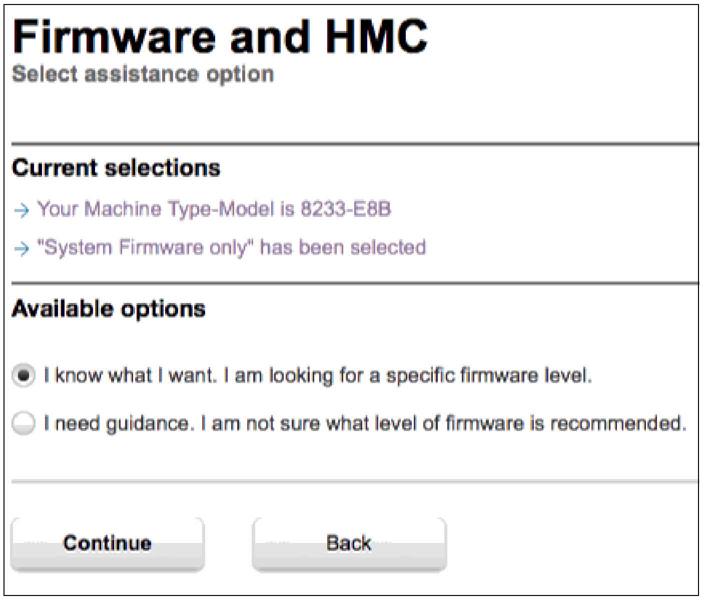
○ Device firmware. Obtain device firmware only. Available for adapters hard disks and media devices.

○ SDMC Code. Obtain SDMC Update Images, Service packs, and Interim fixes.

○ HMC Firmware. Obtain HMC Recovery images, service packs, and specific fixes.

Figure 6-35 Firmware and HMC select fix type: System firmware

Decide what version of the firmware is correct for your system, as described in 6.9.5, “Determining which firmware or fix level is correct for your system” on page 456. Use the Fix Level Recommendation Tool to decide the level of firmware that you require for your system and check the compatibility website, then select **I know what I want** (Figure 6-36). The Fix Central website provides guidance if you are unsure which firmware is recommended.



Firmware and HMC

Select assistance option

Current selections

→ Your Machine Type-Model is 8233-E8B

→ "System Firmware only" has been selected

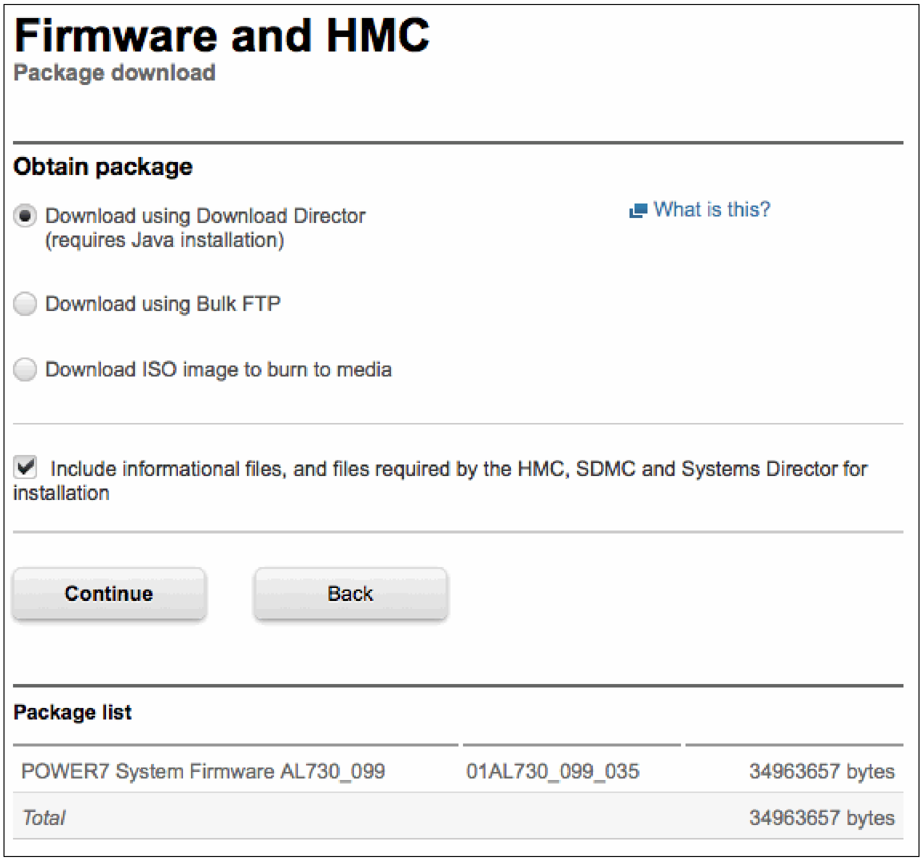
Available options

● I know what I want. I am looking for a specific firmware level.

○ I need guidance. I am not sure what level of firmware is recommended.

Figure 6-36 Firmware and HMC assistance option

Select the version of the system firmware that is applicable to your system. Then, accept the user license agreement and click **Continue** to download directly to your workstation or to use FTP (Figure 6-37).



Firmware and HMC

Package download

Obtain package

● Download using Download Director (requires Java installation)

○ Download using Bulk FTP

○ Download ISO image to burn to media

☑ Include informational files, and files required by the HMC, SDMC and Systems Director for installation

Package list

POWER7 System Firmware AL730_099	01AL730_099_035	34963657 bytes
Total		34963657 bytes

Figure 6-37 System firmware download selection

6.10 Advanced System Management Interface

This section describes how to set up and use the Advanced System Management Interface (ASMI). The ASMI provides a terminal interface through a standard web browser to the service processor. Use it to do general and administrator level service tasks, service functions, and various system management functions.

6.10.1 What is new in managing the ASMI

Read about new or significantly changed information in managing the Advanced System Management Interface (ASMI) since the previous update of this topic collection. At the time of writing, the items in this section were the most recent updates to ASMI.

For more details about new features of ASMI see the IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter/8247-21L/p8hby/p8hby_whatsnew.htm?lang=en

October 2015

The following topics were added:

- Certificate management
- Soft reset of the service processor
- Setting the system brand name
- Configuring the call-home policy

June 2015

The following topics were added:

- Configuring firmware
- Selecting console type
- DVD device driver
- Controlling server power consumption
- Viewing resources deconfigured using the guard function

October 2014

The following topics were added:

- Initiating a service processor failover
- Setting the predictive memory deallocation
- Viewing estimated corrosion rates
- Preparing the RTC battery
- Updated the Changing the processor unit configuration topic.

June 2014

- Added information for IBM Power Systems servers that contain the POWER8 processor.

6.10.2 Connecting to ASMI

The three methods to connect to the ASMI are as follows:

- Access through the HMC
- Access through a web browser
- Access through ASCII terminal

Connection to ASMI by using the HMC

If you have an HMC attached to your managed system, connecting the ASMI by using the HMC is the simplest way to connect. If this is a new system, see 5.5.1, “Add a server” on page 340 for information about how to connect your managed system to the HMC.

To connect to ASMI by using the HMC, complete the following steps:

1. In the HMC workplace window, select **Resources** → **All Systems**.
2. In the contents area, select the server to which you want to connect the ASMI.

3. From the lower panel of the HMC menu, select **Actions** → **View All Actions** → **Launch Advanced System Management (ASM)** as shown in Figure 6-38.

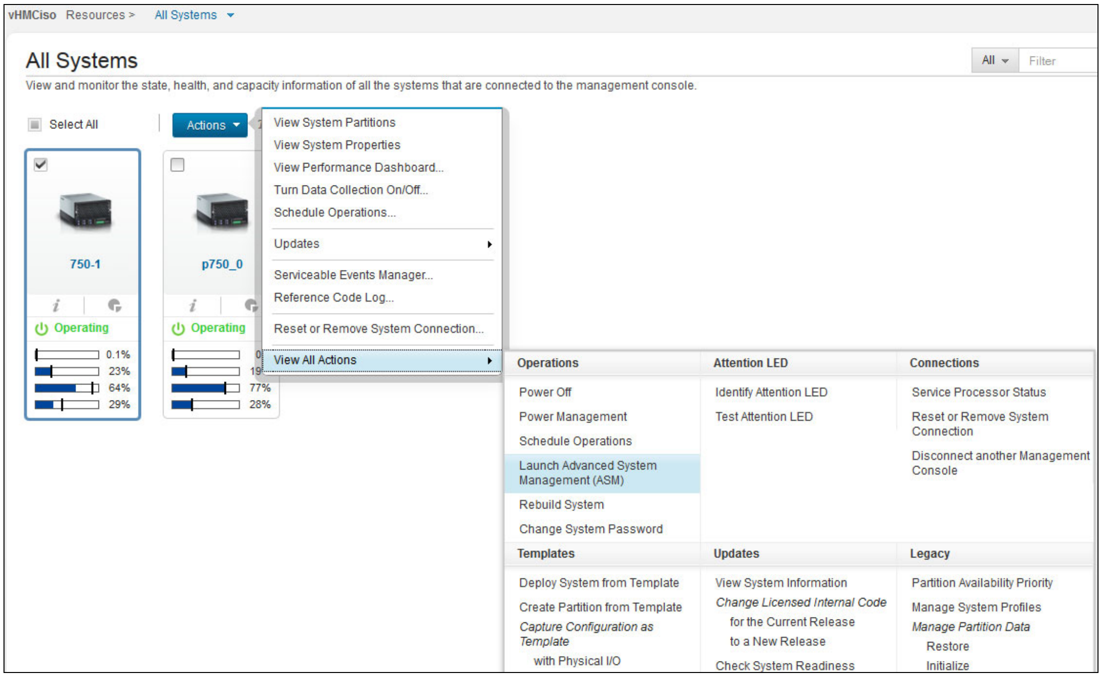


Figure 6-38 Launch ASMI from HMC

Connecting to ASMI through a web browser

The web interface to the ASMI is accessible through Microsoft Internet Explorer 7.0, Netscape 9.0.0.4, or Opera 9.24 and Mozilla Firefox 2.0.0.11 or later versions, running on a PC or notebook that is connected to the service processor. The web interface is available during all phases of system operation, including the initial program load (IPL) and run time. However, several menu options in the web interface are unavailable during IPL or run time to prevent usage or ownership conflicts if the system resources are in use during that phase.

To set up the web browser for direct or remote access to the ASMI, complete these tasks:

1. Connect the power cord from the server to a power source, and wait for the control panel to display `01`.
2. Select a PC or a notebook that has Microsoft Internet Explorer 7.0, Netscape 9.0.0.4, or Opera 9.24 and Mozilla Firefox 2.0.0.11 to connect to your server. You can use this PC or notebook temporarily or permanently to access ASMI.
3. Connect an Ethernet cable from the PC or notebook to the Ethernet port labeled HMC1 on the back of the managed system. If HMC1 is occupied, connect an Ethernet cable from the PC or notebook to the Ethernet port labeled HMC2 on the back of the managed system. You can use cross-over cable or standard Ethernet cable, both are supported.

4. Configure the Ethernet interface on the PC or notebook to an IP address and subnet mask within the same subnet as the server so that your PC or notebook can communicate with the server. Use Table 6-3 to help you determine these values.

   If you are not sure how to configure your PCs IP settings, then consult your network administrator.

Table 6-3 Default IP address for server connectors HMC1 and HMC2

Power System	Server connector	Subnet mask	IP address of service processor	Example of your PC IP address
Service processor A	HMC1	255.255.255.0	169.254.2.147	169.254.2.140
	HMC2	255.255.255.0	169.254.3.147	169.254.3.140
Service processor B (if Installed)	HMC1	255.255.255.0	169.254.2.147	169.254.2.140
	HMC2	255.255.255.0	169.254.3.147	169.254.3.140

5. Use Table 6-3 to determine the IP address of the Ethernet port to which your PC or notebook is connected, and enter the IP address in the address field of the web browser of your PC or notebook.

   For example, if you connected your PC or notebook to HMC1, enter the following address in the web browser of your PC or notebook:

   ```
   https://169.254.2.147
   ```

Accessing the ASMI by using an ASCII terminal

The ASCII interface to the ASMI provides a subset of the web interface functions. The ASCII terminal is available only when the system is in the platform standby state. It is not available during the IPL or run time. The ASMI on an ASCII terminal is not available during the other phases of system operation, including the IPL and run time.

To set up the ASCII terminal for direct or remote access to the ASMI, complete the following tasks:

1. Use a null modem cable to connect the ASCII terminal to system connector S1 on the back of the server or to system port S1 on the control panel by using an RJ-45 connector.

   > **System port connections:** Both system port 1 connections are not available simultaneously; when one is connected, the other is deactivated.

2. Connect the power cord from the server to a power source.

   Wait for the control panel to display `01`.

3. Ensure that your ASCII terminal is set to the following general attributes. These attributes are the default settings for the diagnostic programs:

   ```
   Line Speed-19200,word length-8,parity- none,stop bit-1
   ```

4. Press a key on the ASCII terminal to allow the service processor to confirm the presence of the ASCII terminal.

   The ASMI login window opens.

6.10.3 Log in to ASMI

To connect successfully to the ASMI, the ASMI requires password authentication:

- The ASMI provides a Secure Sockets Layer (SSL) web connection to the service processor. To establish an SSL connection, open your browser by using the following format:

  ```
  https://[Your flexible processor IP address]
  ```

- The browser-based ASMI is available during all phases of the system operation, including IPL and run time. Some menu options are not available during the system IPL or run time to prevent usage or ownership conflicts if corresponding resources are in use during that phase.
- The ASMI that is accessed on a terminal is available only if the system is at platform standby.

After you connect to the ASMI (as described in 6.10.2, “Connecting to ASMI” on page 472), the login display opens. Enter one of the default user IDs and passwords listed in Table 6-4.

Table 6-4 Default login user ID and password

User ID	Default password	Authority level
general	general	general user
admin	admin	administrator
celogin	contact IBM for password	authorized service provider
celogin1	not set, default user disabled	authorized service provider
celogin2	not set, default user disabled	authorized service provider
dev	contact IBM for password	developer user, service only

celogin: The celogin1 and celogin2 IDs can be enabled on POWER6 System and later.

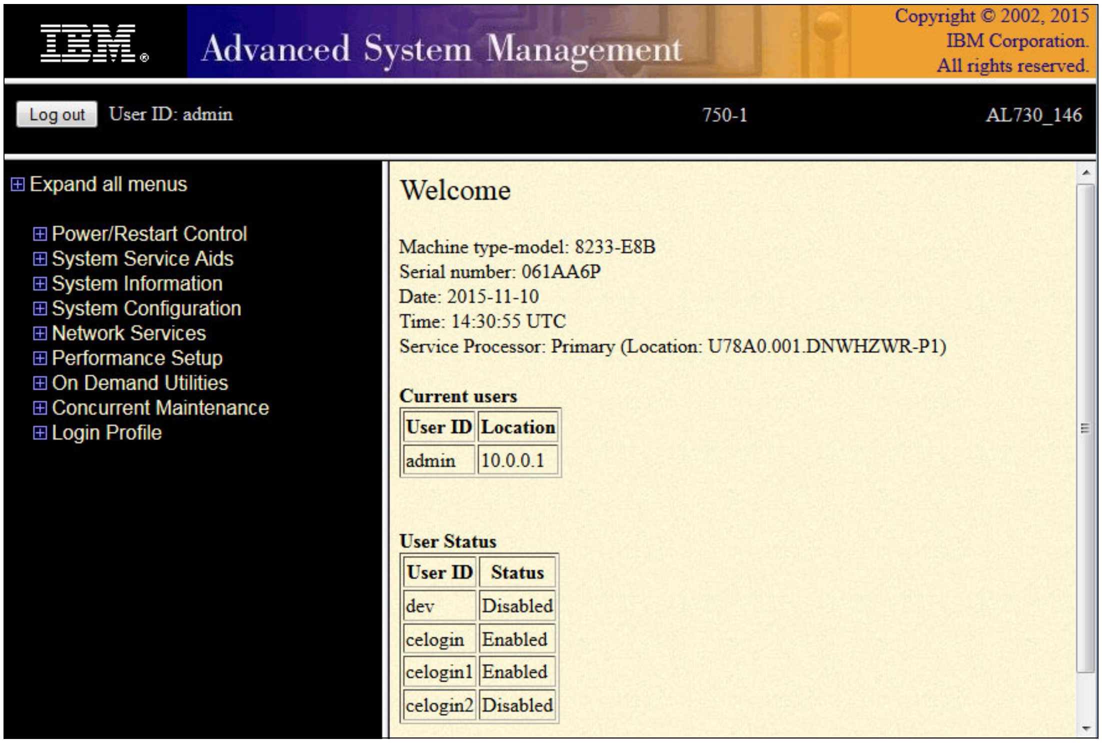
When you log in to ASMI, you are asked to change the default password. You are unable to proceed until you change the password.

ASMI login restrictions

The following restrictions apply to ASMI users:

- Only three users can log in at any one time.
- If you are logged in and inactive for 15 minutes, your session expires and you have to log in again.
- If you make five invalid login attempts, your user ID is locked out for five minutes.

The ASMI window opens (Figure 6-39) after a successful login.



Welcome

Machine type-model: 8233-E8B
Serial number: 061AA6P
Date: 2015-11-10
Time: 14:30:55 UTC
Service Processor: Primary (Location: U78A0.001.DNWHZWR-P1)

Current users

User ID	Location
admin	10.0.0.1

User Status

User ID	Status
dev	Disabled
celogin	Enabled
celogin1	Enabled
celogin2	Disabled

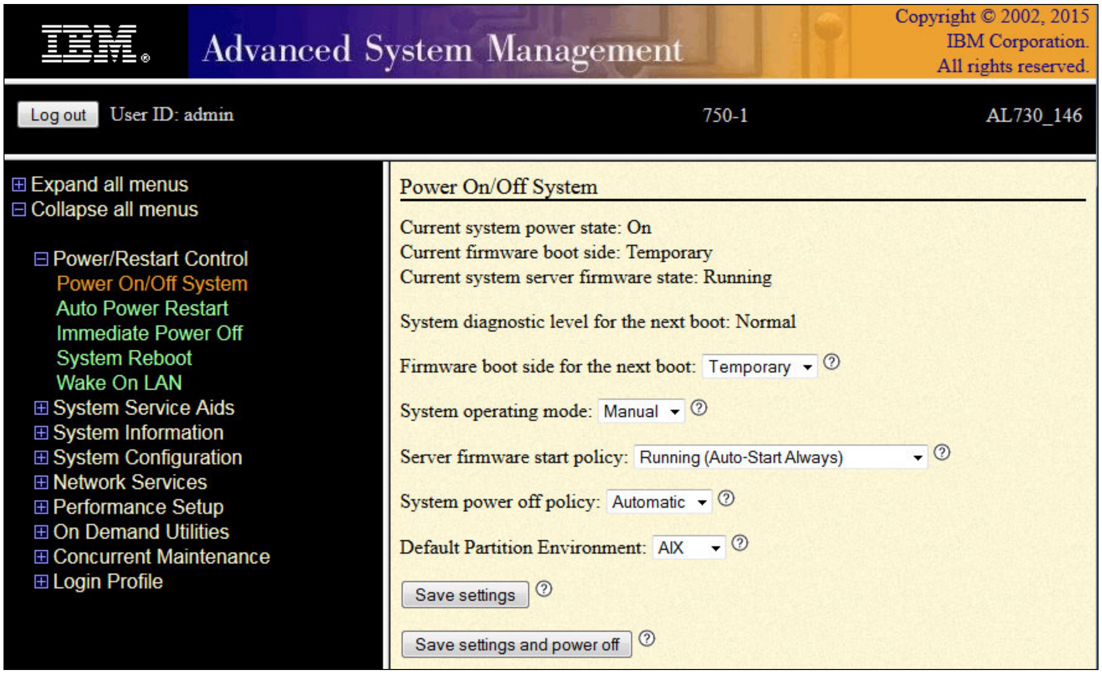
Figure 6-39 Advanced System Management main menu

6.10.4 Power and restart control

You can use the power and restart control feature to control the system power manually and automatically. This section also describes available options for turning on the system. See Figure 6-40 on page 477, which shows the Power On/Off System option.

The following options are described:

- Fast and slow boot
- Temporary and permanent boot side
- Normal and permanent operating mode



User ID: admin

750-1

AL730_146

Power On/Off System

Current system power state: On
Current firmware boot side: Temporary
Current system server firmware state: Running

System diagnostic level for the next boot: Normal

Firmware boot side for the next boot: Temporary

System operating mode: Manual

Server firmware start policy: Running (Auto-Start Always)

System power off policy: Automatic

Default Partition Environment: AIX

Figure 6-40 System power on and off options

Power On/Off System function

When you select this function, the right side of the menu displays the current system power state, current firmware boot side, and system server firmware state.

Set the following boot values:

- System boot speed

  Select the speed for the next boot (Fast or Slow). A fast boot results in some diagnostic tests being skipped, and shorter memory tests being run during the boot. A slow boot goes through all diagnostic tests and memory tests. Normally, you take this option if you are experiencing some system errors or when you made some system changes, for example CPU and memory upgrades.

- Firmware boot side

  Select the side from which the firmware boots (Permanent or Temporary). When you upgrade your system firmware, typically, firmware updates are tested on the temporary side before they are applied to the permanent side. Therefore, the temporary side should always have the latest firmware. The permanent side has the previous version.

- System operating mode

  Select the operating mode (Manual or Normal). Manual mode overrides various automatic power-on functions, such as auto-power restart, and enables the power button, which allows you to select power options from the control panel. You can also set this option from the control panel.

- Server firmware start policy

  Select the state for the server firmware: Standby or Running. When the server is in the server firmware standby state, partitions can be set up and activated. The running option restarts your partitions automatically.

- System power off policy

  Select the system power off policy. This policy is a system parameter that controls the behavior of the system when the last partition (or the only partition in the case of a system that is not managed by an HMC) is powered off. The choices are as follows:

  - Power off: When the last partition is powered down, the system turns off.
  - Stay on: When the last system is powered down, the system stays on.
  - Automatic: This is the default setting. If the system is not partitioned, the system is turned off. If the system is partitioned, it stays on.

Make your selections and select **Save settings and power on**.

Auto Power Restart function

You can set your system to restart automatically. This function is useful when power is restored after an unexpected power line disturbance causes the system to shut down unexpectedly. Select **Enable** or **Disable**. By default, the auto power restart value is set to *Disable*. In many cases, you might not want the system to restart automatically, unless you are reasonably certain that the power problem is resolved.

Immediate Power Off function

You can power off the system quickly by using the Immediate Power Off function. Typically, this option is used when an emergency power off is needed. The operating system is not notified before the system is powered off.

> **Attention:** To avoid experiencing data loss and a longer IPL the next time the system or logical partitions are booted, shut down the operating system before doing an immediate power off.

System Reboot function

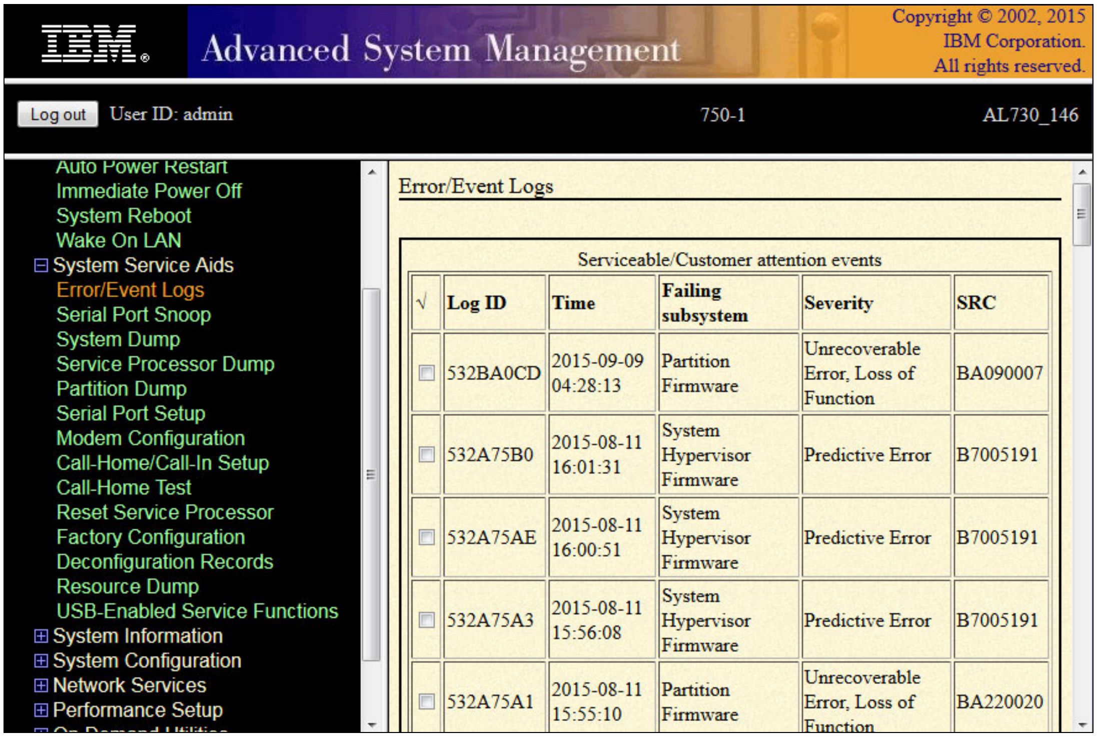
You can reboot the system quickly by using the System Reboot function. The operating system is not notified before the system is rebooted.

> **Attention:** Rebooting the system shuts down all partitions immediately. To avoid experiencing data loss and a longer IPL the next time the system or logical partitions are booted, shut down the operating system before doing a reboot.

6.10.5 System Service Aids menu options

Figure 6-41 shows the System Service Aids menu. From this menu, you can do the following functions, among others:

- Display system error, event logs.
- Initiate a system dump.
- Initiate a service processor dump.
- Reset the service processor.
- Reset your system to the factory-shipped configuration settings.



Error/Event Logs

Serviceable/Customer attention events

√	Log ID	Time	Failing subsystem	Severity	SRC
□	532BA0CD	2015-09-09 04:28:13	Partition Firmware	Unrecoverable Error, Loss of Function	BA090007
□	532A75B0	2015-08-11 16:01:31	System Hypervisor Firmware	Predictive Error	B7005191
□	532A75AE	2015-08-11 16:00:51	System Hypervisor Firmware	Predictive Error	B7005191
□	532A75A3	2015-08-11 15:56:08	System Hypervisor Firmware	Predictive Error	B7005191
□	532A75A1	2015-08-11 15:55:10	Partition Firmware	Unrecoverable Error, Loss of Function	BA220020

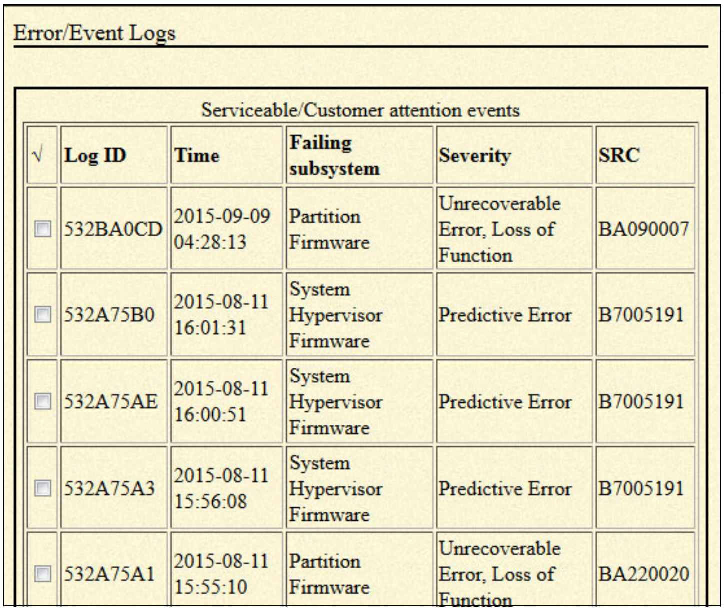
Figure 6-41 System Service Aids menu

The following features are not available when your system is connected to the HMC. These features are part of the Service Management on the HMC:

- Serial port snoop
- Partition dump
- Serial port setup
- Modem configuration
- Call home/call in setup
- Call home test
- Reset Service Processor

Error/Event Logs option

From the System Service Aids menu, select **Error/Event Logs**. The Error/Event Logs selection panel opens (Figure 6-42). Use it to view error and event logs that are generated by various service processor firmware components. The content of these logs can be useful in solving hardware or server firmware issues.



Error/Event Logs

Serviceable/Customer attention events

√	Log ID	Time	Failing subsystem	Severity	SRC
□	532BA0CD	2015-09-09 04:28:13	Partition Firmware	Unrecoverable Error, Loss of Function	BA090007
□	532A75B0	2015-08-11 16:01:31	System Hypervisor Firmware	Predictive Error	B7005191
□	532A75AE	2015-08-11 16:00:51	System Hypervisor Firmware	Predictive Error	B7005191
□	532A75A3	2015-08-11 15:56:08	System Hypervisor Firmware	Predictive Error	B7005191
□	532A75A1	2015-08-11 15:55:10	Partition Firmware	Unrecoverable Error, Loss of Function	BA220020

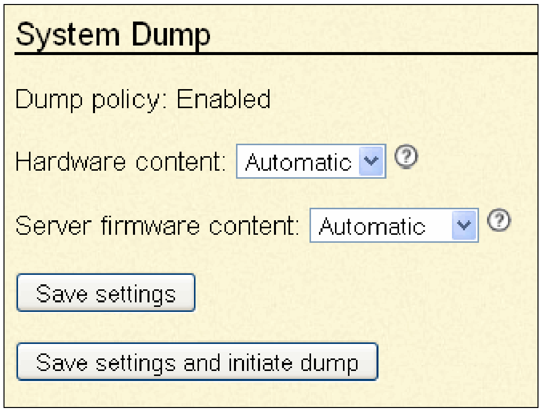
Figure 6-42 Error and event logs

Select the event log that you want to view and scroll to the bottom of the window to select **Show details**. The details provide the description of the system reference code (SRC).

System Dump procedure

Use the System Dump procedure only under the direction of your service provider. You can initiate a system dump to capture overall system information, system processor state, hardware scan rings, caches, and other information. This information can be used to resolve a hardware or server firmware issue. A system dump can also be initiated automatically after a system malfunction, such as a check stop or hang.

Select **System Dump**. The System Dump window opens (Figure 6-43).



System Dump

Dump policy: Enabled

Hardware content: Automatic

Server firmware content: Automatic

Figure 6-43 Capturing overall system information with System Dump procedure

Use this window to set the following information:

- Dump policy

  Select the policy to determine when system dump data is collected.

  The default is `Enabled`.

- Hardware content

  Select the policy to determine how much hardware data is collected for a system dump.

  - If you select **Automatic** (default), the SP collects the hardware data that it determines is necessary, depending on the particular failure.
  - If you select **Maximum**, the SP collects the maximum amount of hardware data. If you choose this selection, the collection of hardware data can be quite time consuming, especially for systems with many processors.

- Server firmware content

  Select the policy to determine how much server firmware data is collected for a system dump:

  - If you select **Automatic**, the SP collects the minimum amount of data necessary to debug server firmware failures. Automatic is the default policy. In some cases, your support engineer might want you to override the default policy.
  - If you select **Physical I/O**, the SP collects the minimum firmware data plus the firmware data that is associated with physical I/O operations.
  - If you select **Virtual I/O**, the SP collects the minimum firmware data plus the firmware data that is associated with I/O operations that do not involve physical I/O devices.
  - If you select **High performance switch HPS Cluster**, the SP collects the minimum firmware data plus the firmware data that is associated with high performance switch operations between this server and other servers in the cluster.
  - If you select **HCA I/O**, the SP collects the minimum firmware data plus the firmware data associated with the host channel adapter I/O operations.
  - If you select **Maximum**, the SP collects the maximum amount of server firmware data.

Make your selections and click **Save settings**.

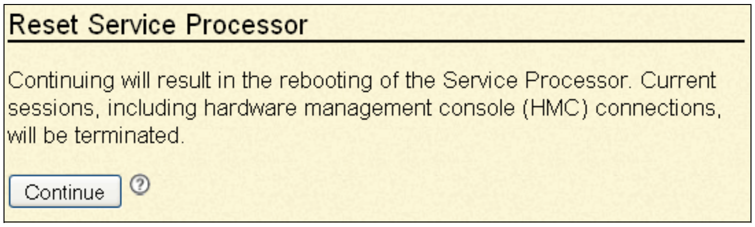
Service Processor Dump option

You use the Service Process Dump option to enable or disable the service processor dump function. The default value is *Enabled*. A service processor dump captures error data after a service processor failure, or upon user request. User request for service processor dump is not available when this policy is set to disabled.

The save settings and initiate dump button is visible only when an SP dump is allowed (that is, when SP dumps are enabled and the previous SP dump data is retrieved). Click this button to initiate an SP dump.

Reset Service Processor option

Typically, rebooting of the SP is done only when instructed by IBM service personnel (Figure 6-44).



Reset Service Processor

Continuing will result in the rebooting of the Service Processor. Current sessions, including hardware management console (HMC) connections, will be terminated.

Figure 6-44 Reset service processor

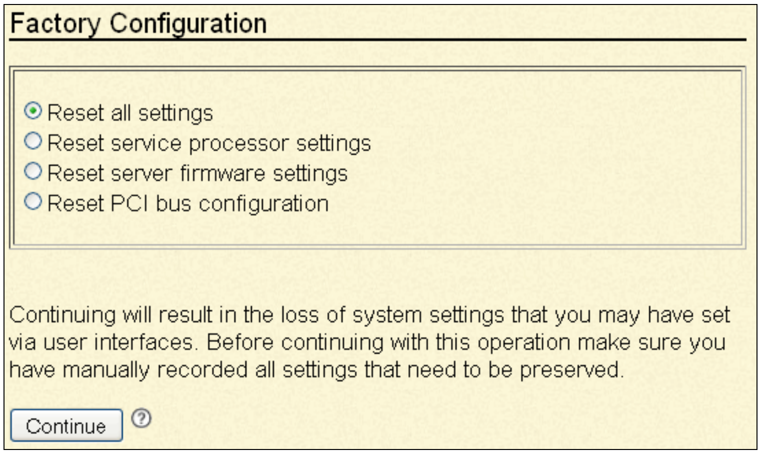
This function is not available if your system is on. Clicking **Continue** causes the service processor to reboot. Because the service processor reboots, your ASMI session is dropped, and you must reconnect your session to continue.

Factory Configuration option

Use this procedure (Figure 6-45) only under the direction of your IBM service personnel.

In critical systems situations, you can restore your system to the factory default settings. Doing so results in the loss of all system settings (such as the HMC access and ASMI passwords, time of day, network configuration, and hardware deconfiguration policies) that you have to set again through the service processor interfaces. Also, you lose the system error logs and partition-related information.

> **Manually record all settings:** Before you continue with this operation, ensure that you manually recorded all settings that must be preserved.



Factory Configuration

● Reset all settings
○ Reset service processor settings
○ Reset server firmware settings
○ Reset PCI bus configuration

Continuing will result in the loss of system settings that you may have set via user interfaces. Before continuing with this operation make sure you have manually recorded all settings that need to be preserved.

Figure 6-45 Factory configuration reset

This window has the following options:

- Reset all settings

  Resets a combination of all the other options. To complete this operation, the system is powered on and then off, and the service processor is reset.
- Reset service processor settings

  Resets the settings of the service processor that include passwords, network addresses, time of day, hardware configuration policies, and so forth. Any sessions that are currently active in the network interfaces are disconnected, and the service processor is reset.
- Reset server firmware settings

  Resets the firmware settings only. Partition data is lost.
- Reset Peripheral Component Interconnect (PCI) bus configuration

  Resets the PCI bus and the firmware settings. To complete this operation, the system is turned on and then off.

Make the appropriate selection and then select **Continue**.

6.10.6 System Information menu options

Use the System Information menu (Figure 6-46) to do these tasks:

- Display vital product data.
- Perform system power control network (SPCN) trace and display the results.
- Display the previous boot indicator.
- Display the progress indicator history.
- Display the real-time progress Indicator.

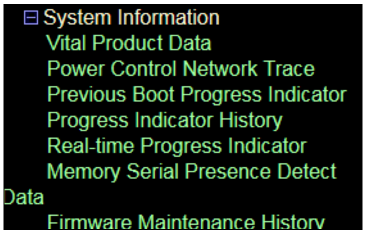
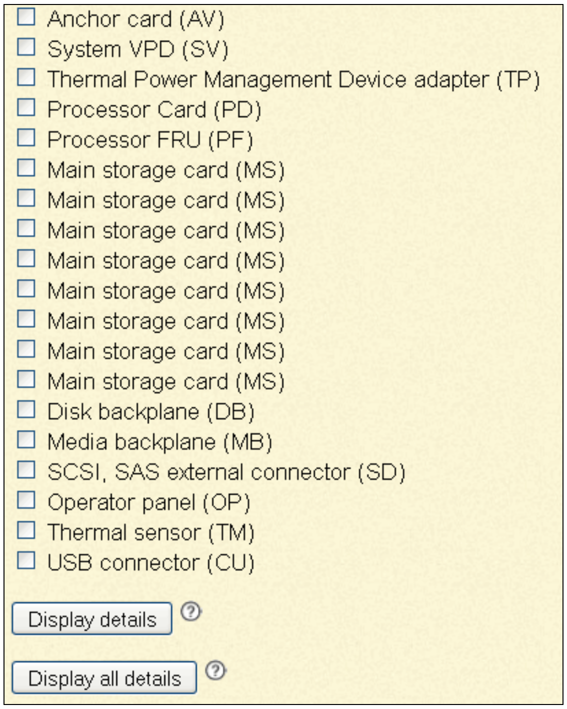

⊟ System Information
Vital Product Data
Power Control Network Trace
Previous Boot Progress Indicator
Progress Indicator History
Real-time Progress Indicator
Memory Serial Presence Detect Data
Firmware Maintenance History

Figure 6-46 System Information menu

Vital Product Data option

Select **Vital Product Data** to view manufacturer's vital product data (VPD) that is stored from the system boot before the one in progress now (Figure 6-47).

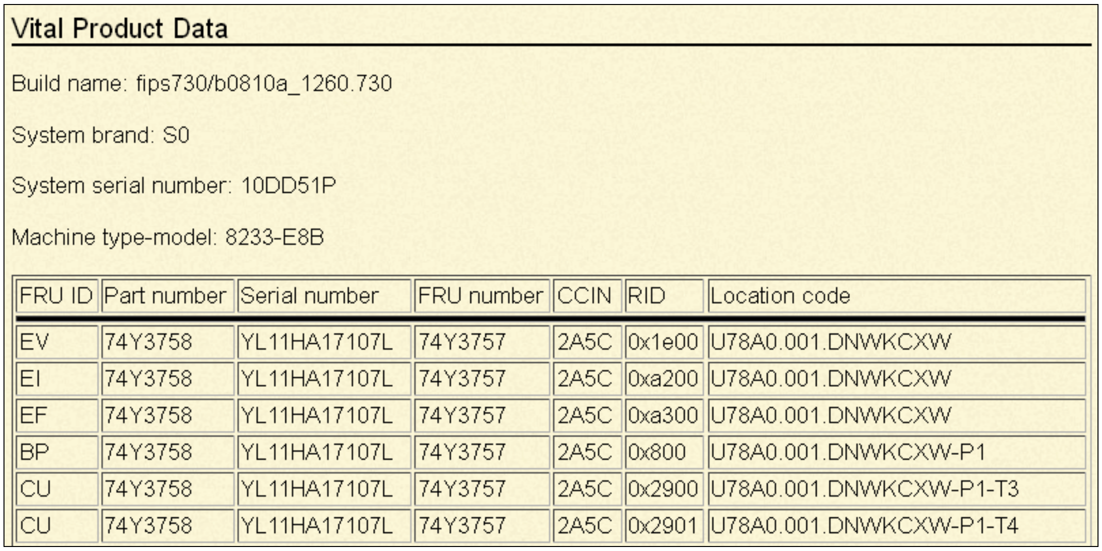


□ Anchor card (AV)
□ System VPD (SV)
□ Thermal Power Management Device adapter (TP)
□ Processor Card (PD)
□ Processor FRU (PF)
□ Main storage card (MS)
□ Main storage card (MS)
□ Main storage card (MS)
□ Main storage card (MS)
□ Main storage card (MS)
□ Main storage card (MS)
□ Main storage card (MS)
□ Main storage card (MS)
□ Disk backplane (DB)
□ Media backplane (MB)
□ SCSI, SAS external connector (SD)
□ Operator panel (OP)
□ Thermal sensor (TM)
□ USB connector (CU)

Figure 6-47 Display details of VPD

If you want to view only selected manufacturer's VPD, such as serial numbers and part numbers, select the feature that you want to view and click **Display details**.

To view details of all the features, click **Display all details**. The Vital Product Data window opens (Figure 6-48).



Vital Product Data

Build name: fips730/b0810a_1260.730

System brand: S0

System serial number: 10DD51P

Machine type-model: 8233-E8B

FRU ID	Part number	Serial number	FRU number	CCIN	RID	Location code
EV	74Y3758	YL11HA17107L	74Y3757	2A5C	0x1e00	U78A0.001.DNWKCXW
EI	74Y3758	YL11HA17107L	74Y3757	2A5C	0xa200	U78A0.001.DNWKCXW
EF	74Y3758	YL11HA17107L	74Y3757	2A5C	0xa300	U78A0.001.DNWKCXW
BP	74Y3758	YL11HA17107L	74Y3757	2A5C	0x800	U78A0.001.DNWKCXW-P1
CU	74Y3758	YL11HA17107L	74Y3757	2A5C	0x2900	U78A0.001.DNWKCXW-P1-T3
CU	74Y3758	YL11HA17107L	74Y3757	2A5C	0x2901	U78A0.001.DNWKCXW-P1-T4

Figure 6-48 Displays all VPD detail

Power control network trace

You can perform an SPCN trace and display the results. This information is gathered to provide extra debug information when you work with your hardware service provider.

> **Note:** Producing a trace can take an extended amount of time, based on your system type and configuration. This process is a normal delay because of the amount of time the system requires to query the data.

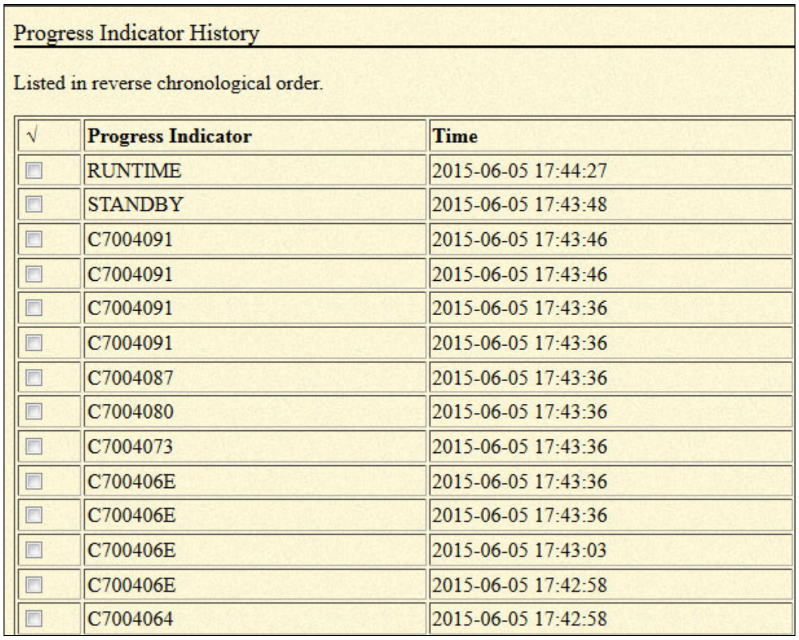
Previous boot progress indicator

You can display the previous boot progress indicator that was displayed in the control panel during the previous failed boot by selecting this option. During a successful boot, the previous progress indicator is cleared. If this option is selected after a successful boot, nothing is displayed.

The progress indicator information is stored in nonvolatile memory. If the system is powered off using the power-on button on the control panel, this information is retained. If the alternating current (ac) power is disconnected from the system, this information is lost.

Progress Indicator History option

With this option, you can review the progress of codes that displays in the control panel during the previous boot. The codes are listed in reverse chronological order (Figure 6-49): The first entry is the most recent entry. This information is gathered to provide extra debug information when you work with your hardware service provider. Select a code to display and select show details.



Progress Indicator History

Listed in reverse chronological order.

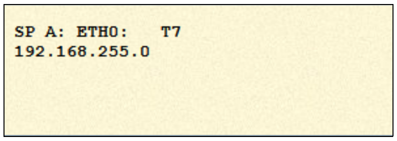
√	Progress Indicator	Time
□	RUNTIME	2015-06-05 17:44:27
□	STANDBY	2015-06-05 17:43:48
□	C7004091	2015-06-05 17:43:46
□	C7004091	2015-06-05 17:43:46
□	C7004091	2015-06-05 17:43:36
□	C7004091	2015-06-05 17:43:36
□	C7004087	2015-06-05 17:43:36
□	C7004080	2015-06-05 17:43:36
□	C7004073	2015-06-05 17:43:36
□	C700406E	2015-06-05 17:43:36
□	C700406E	2015-06-05 17:43:36
□	C700406E	2015-06-05 17:43:03
□	C700406E	2015-06-05 17:42:58
□	C7004064	2015-06-05 17:42:58

Figure 6-49 Progress Indicator History option

You can view the progress and error codes that currently display on the control panel. Viewing progress and error codes is useful when you diagnose boot-related issues. To perform this operation, your authority level must be one of the following possibilities:

- General
- Administrator
- Authorized service provider

Select this option to open the window that shows the real-time progress of the system and displays what you have on the system display (Figure 6-50).



```
SP A: ETH0:   T7
192.168.255.0
```

Figure 6-50 Real-time progress indicator

6.10.7 System Configuration menu options

Figure 6-51 shows the expanded System Configuration menu. This section describes some of the tasks that are listed. You can use this menu to do the following tasks, among others:

- Change the system name.
- Configure I/O enclosures.
- Change the time of day.
- Establish the firmware update policy.
- Establish the detailed PCI error injection policies.
- Change the interposer plug count.
- Enable I/O adapter enlarged capacity.
- View Hardware Management Console connections.
- Change floating point unit commutation test values.

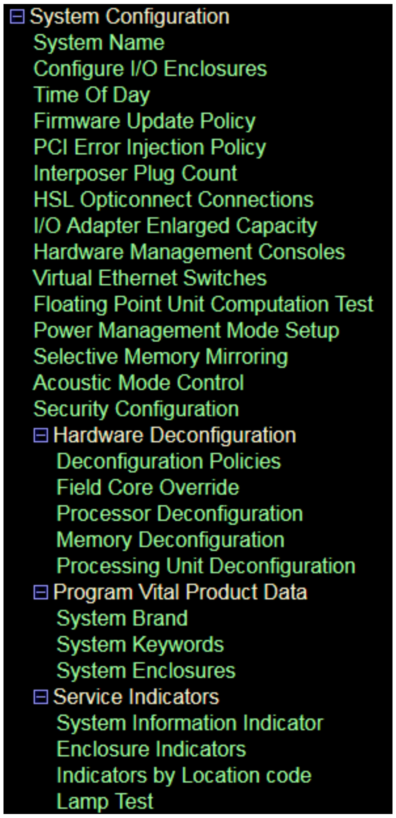
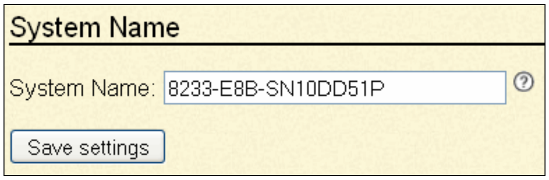

⊟ System Configuration
System Name
Configure I/O Enclosures
Time Of Day
Firmware Update Policy
PCI Error Injection Policy
Interposer Plug Count
HSL Opticonnect Connections
I/O Adapter Enlarged Capacity
Hardware Management Consoles
Virtual Ethernet Switches
Floating Point Unit Computation Test
Power Management Mode Setup
Selective Memory Mirroring
Acoustic Mode Control
Security Configuration
⊟ Hardware Deconfiguration
Deconfiguration Policies
Field Core Override
Processor Deconfiguration
Memory Deconfiguration
Processing Unit Deconfiguration
⊟ Program Vital Product Data
System Brand
System Keywords
System Enclosures
⊟ Service Indicators
System Information Indicator
Enclosure Indicators
Indicators by Location code
Lamp Test

Figure 6-51 System Configuration menu

System Name option

From the System Configuration menu, select **System Name** to display the current system name (Figure 6-52). The system name is a value that identifies the system or server. You can change the name here. The name cannot be blank and cannot be longer than 31 characters. To change the system name, enter a new value and click **Save settings**.



System Name

System Name: 8233-E8B-SN10DD51P

Figure 6-52 System Name

This example shows changes to the system name. The valid character values are as follows:

- a - Z
- 0 - 9
- Hyphen (-)
- Underscore (_)
- Period (`.`)

The system includes a default system name, initialized to a 31-character value as follows:

`Server-`*`tttt`*`-`*`mmm`*`-SN0000000`

In this default system name:

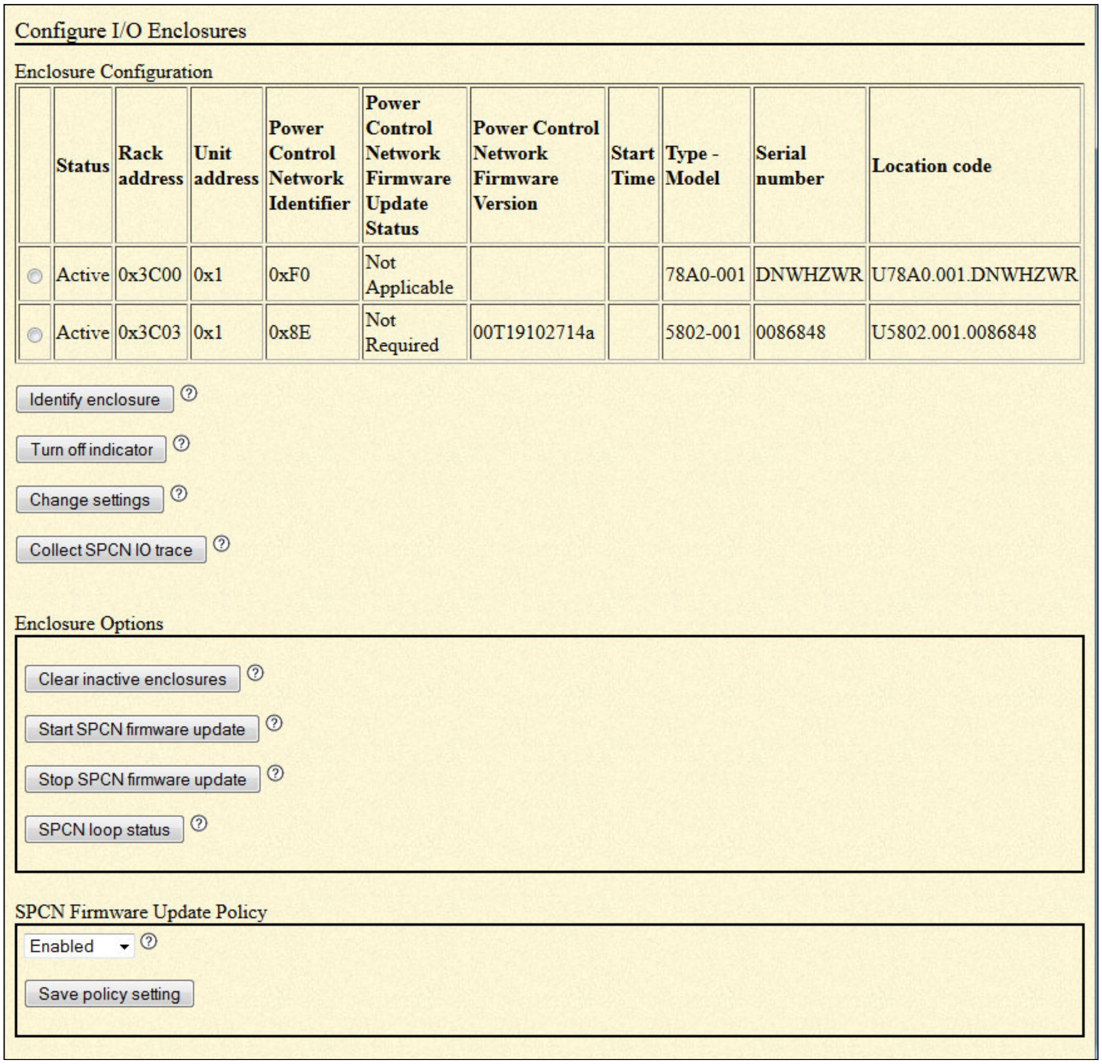
- *`tttt`* = Machine type
- *`mmm`* = Model number
- 0000000 = Serial number

Configure I/O Enclosures function

This function normally is used by your hardware service provider. After the server firmware reaches the `Standby` state, you can configure I/O enclosure attributes as follows:

- Display the status, location code, rack address, unit address, power control network identifier, and the machine type and model of each enclosure in the system.
- Change the identification indicator state on each enclosure to **On** (identify) or **Off**.
- Update the power control network identifier, enclosure serial number, and the machine type and model of each enclosure.
- Change the identification indicator state of the SPCN firmware in an enclosure to **Enable** or **Disable**.
- Remove rack and unit addresses for all inactive enclosures in the system.

When you select this function, the Configure I/O Enclosures window opens (Figure 6-53).



Configure I/O Enclosures

Enclosure Configuration

	Status	Rack address	Unit address	Power Control Network Identifier	Power Control Network Firmware Update Status	Power Control Network Firmware Version	Start Time	Type - Model	Serial number	Location code
○	Active	0x3C00	0x1	0xF0	Not Applicable			78A0-001	DNWHZWR	U78A0.001.DNWHZWR
○	Active	0x3C03	0x1	0x8E	Not Required	00T19102714a		5802-001	0086848	U5802.001.0086848

Enclosure Options

Clear inactive enclosures
Start SPCN firmware update
Stop SPCN firmware update
SPCN loop status

SPCN Firmware Update Policy

Enabled

Figure 6-53 Configure I/O Enclosures window

This window has the following options for the selected enclosure:

- Identify enclosure

  Turns on the enclosure’s indicator. The LED flashes to identify the enclosure.

- Turn off indicator

  Turns off the enclosure’s indicator.

- Change settings

  Changes the settings for the enclosure. The next page displays options for changing the configuration ID, machine type-model, and serial number:

  – Power Control Network Identifier: Enter a hexadecimal number for the power control network identifier.

  > **System server firmware:** The system server firmware must be in `Standby` state or the expansion unit must be turned off when this operation is performed.

  - Type - Model: Enter the enclosure machine type and model in the form *TTTT-MMM*:

    TTTT: The four characters of the enclosure machine type.

    MMM: The three characters of the enclosure model.

    The enclosure machine type cannot be 0000. All alphanumeric characters are valid.

  - Serial number: Enter seven characters for the enclosure serial number. All alphanumeric characters except O, I, and Q are valid. All lowercase letters are converted to uppercase letters.

- Collect SPCN I/O Trace

  Displays SPCN I/O trace for the enclosure.

- Clear inactive enclosures

  Clears the rack and unit addresses of all inactive enclosures.

- Start SPCN firmware update

  Starts pending SPCN firmware downloads if allowed by the SPCN firmware update policy. SPCN firmware downloads cannot all be attempted at the same time. Some downloads can remain in a pending state before starting while others complete. Starting SPCN downloads is done asynchronously.

- Stop SPCN firmware update

  Stops SPCN firmware downloads that are currently in progress. SPCN firmware downloads that are stopped move to a pending state. These SPCN firmware downloads can be restarted from the beginning either automatically by the system or by using Start SPCN Firmware Update, if allowed by the SPCN firmware update policy.

  Stopping the SPCN downloads is done asynchronously and can be monitored showing the power control network firmware update status.

- SPCN loop status

  This displays the overall status of your enclosure loops.

- SPCN Firmware Update Policy

  If Disabled, no SPCN firmware downloads are allowed to start. Changing the SPCN firmware update policy to disabled does not affect SPCN firmware downloads currently in progress.

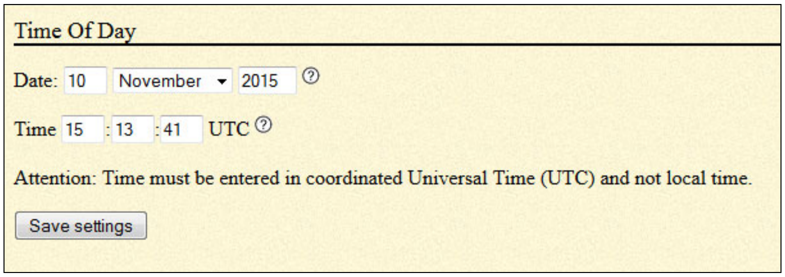
  If Enabled, SPCN firmware downloads are allowed only over the high-speed link (HSL) interface. Changing the SPCN firmware update policy to enabled does not affect SPCN firmware downloads over the serial interface that are currently in progress.

  Changing the SPCN firmware update policy setting to Enabled from Disabled does not automatically cause SPCN firmware downloads over the HSL interface to begin immediately.

  If Expanded, SPCN firmware downloads are allowed over both the HSL and serial interfaces. Changing to the SPCN firmware update policy to Expanded does not cause SPCN firmware downloads to begin immediately.

Time of Day function

You can display and change the current date and time of the system. This function is available if your system is on or off. When you select this option, the Time Of Day window opens (Figure 6-54).



Time Of Day

Date: 10 November 2015

Time 15 : 13 : 41 UTC

Attention: Time must be entered in coordinated Universal Time (UTC) and not local time.

Figure 6-54 Time of Day window

This window has the following options:

- Date

  Enter the current date. Any change to the current date or time is applied to the service processor only, and is independent of any partition.

- Time

  Enter the current time in Coordinated Universal Time (UTC) format. UTC is the current term for what was commonly referred to as Greenwich Mean Time (GMT). Zero (0) hours UTC is midnight in Greenwich, England, which lies on the zero longitudinal (prime) meridian.

  UTC is based on a 24-hour clock. Local time is expressed as a positive or negative offset from UTC, depending on whether the local time zone is east or west of the prime meridian.

Enter the date and time and select **Save settings**.

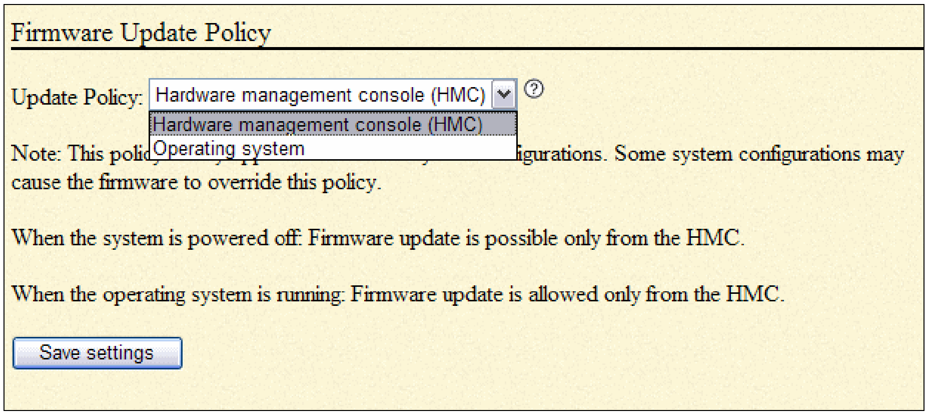
Firmware Update Policy function

This policy defines whether firmware updates are allowed from an operating system when the system is managed by an HMC. The default setting of this policy is to not allow firmware updates through the operating system. This policy takes effect only when a system is HMC managed. When a system is not HMC-managed, firmware updates can be made only through the operating system, so this policy setting is ignored.

When this policy is set to allow firmware updates from the operating system, firmware updates from an HMC are not allowed, unless the system is turned off.

When a system is turned off, firmware updates can be performed from an HMC, regardless of the setting of this policy. However, take care when you update firmware from both an HMC and the operating system.

When you select this option, the Firmware Update Policy window opens (Figure 6-55).


Firmware Update Policy

Update Policy: Hardware management console (HMC)

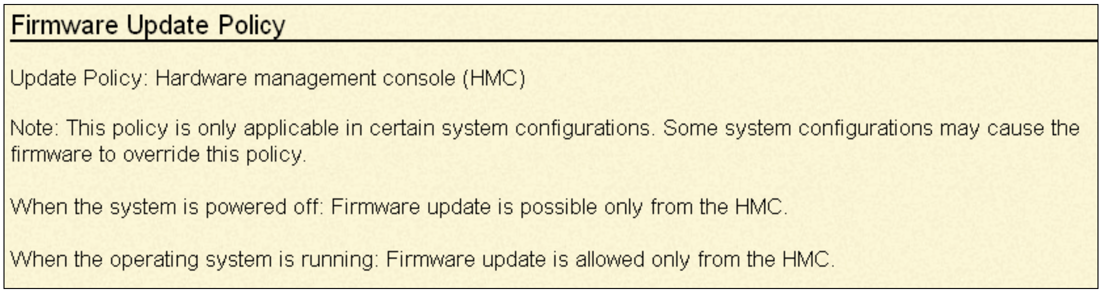
Note: This polic igurations. Some system configurations may cause the firmware to override this policy.

When the system is powered off: Firmware update is possible only from the HMC.

When the operating system is running: Firmware update is allowed only from the HMC.

Figure 6-55 Firmware Update Policy before IBM POWER7 Systems™

Some Power Systems servers require an HMC for firmware updates (Figure 6-56).


Firmware Update Policy

Update Policy: Hardware management console (HMC)

Note: This policy is only applicable in certain system configurations. Some system configurations may cause the firmware to override this policy.

When the system is powered off: Firmware update is possible only from the HMC.

When the operating system is running: Firmware update is allowed only from the HMC.

Figure 6-56 Firmware Update Policy in certain models of IBM POWER7 Systems

PCI Error Injection Policy option

This option controls the PCI error injection policy. If enabled, utilities on the host operating system can inject PCI errors.

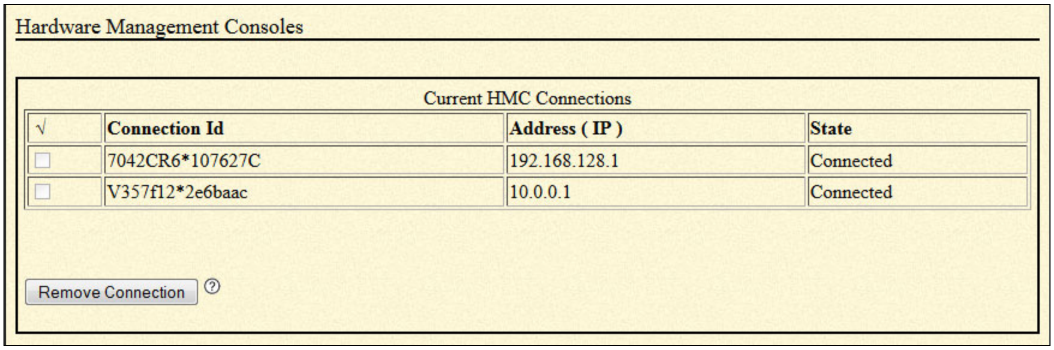
I/O Adapter Enlarged Capacity option

This option controls the size of PCI memory space that is allocated to each PCI slot. When enabled, selected PCI slots, including those in external I/O subsystems, receive the larger direct memory access (DMA) and memory mapped address space. Some PCI adapters might require this additional DMA or memory space, per the adapter specification. This option increases system main storage allocation to these selected PCI slots.

Enabling this option might result in some PCI host bridges and slots not being configured because the installed main storage is insufficient to configure all installed PCI slots.

Hardware Management Consoles option

Use this option to view the HMC that is connected or was connected to the managed system (Figure 6-57). You can also remove the disconnected HMC from your managed system. Select the HMC serial number and click **Remove Connection**.



Hardware Management Consoles

Current HMC Connections

√	Connection Id	Address (IP)	State
□	7042CR6*107627C	192.168.128.1	Connected
□	V357f12*2e6baac	10.0.0.1	Connected

Figure 6-57 Hardware Management Consoles window

Virtual Ethernet Switches option

To use this option, enter a number from 0 to 16 for virtual Ethernet switches. This value controls the number of virtual Ethernet switches that are allocated by system server firmware. Most users leave this value set to its default of zero (0). A value of 0 enables the HMC to control the number of virtual Ethernet switches that are allocated by system server firmware.

For advanced configuration, this number can be set higher to cause the system server firmware to create that many virtual Ethernet switches during platform power-on. It also disables the ability of the HMC to configure the number of virtual Ethernet switches.

With this process, when a virtual Ethernet adapter is created by using the HMC, the adapter is connected to a particular virtual switch depending on the virtual slot number that is chosen during creation.

The adapter’s virtual slot number is divided by the number of virtual Ethernet switches. The remainder of the division is used to determine with which switch the adapter is associated. Each virtual Ethernet adapter is able to communicate only with other virtual Ethernet adapters on the same virtual switch. For example, if the number of virtual Ethernet switches is set to 3, adapters in virtual slot 3, 6, and 9 are assigned to the same switch. A virtual Ethernet adapter in virtual slot 4 is assigned to a different switch, and will not be able to communicate with the adapters in slots 3, 6, and 9.

Floating Point Unit Computation Test option

Use this option to set the floating point unit test policy or to run the test immediately (Save Settings or Run the test immediately). Set one of the following functions:

- Disabled

  Test never runs except when choosing to run the test immediately.

- Staggered (default setting)

  Test is run once on every processor in the platform over a 24-hour period.

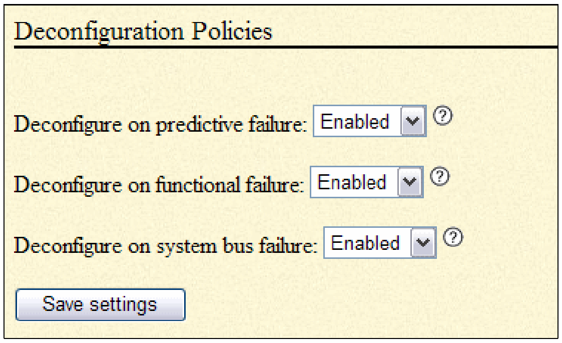
- Periodic

  Test runs at a specified time, sequentially through all processors in the system.

If you run the test immediately, the current policy setting is overridden but not changed. The test is run sequentially on all processors in the system. This feature is available only when the system is on.

Hardware Deconfiguration menu options

You can set various policies to deconfigure processors and memory in certain situations (Figure 6-58). *Deconfiguration* means that the resource is taken from a state of being available to the system, to a state of being unavailable to the system.



Deconfiguration Policies

Deconfigure on predictive failure: Enabled

Deconfigure on functional failure: Enabled

Deconfigure on system bus failure: Enabled

Figure 6-58 Deconfiguration Policies window

The Deconfiguration Policies window has the following settings:

- Deconfigure on predictive failure

  Enable this policy to deconfigure on predictive failures. This configuration applies to run time or persistent boot time deconfiguration of processing unit resources or functions with predictive failures, such as correctable errors over the threshold.

  If enabled, the particular resource or function that is affected by the failure is deconfigured.

- Deconfigure on functional failure

  Select the policy to deconfigure on functional failures. This configuration applies to run time or persistent boot time deconfiguration of processing unit resources or functions with functional failures, such as check stop errors or uncorrectable errors.

  If enabled, the particular resource or function that is affected by the failure is deconfigured.

- Deconfigure on system bus failure

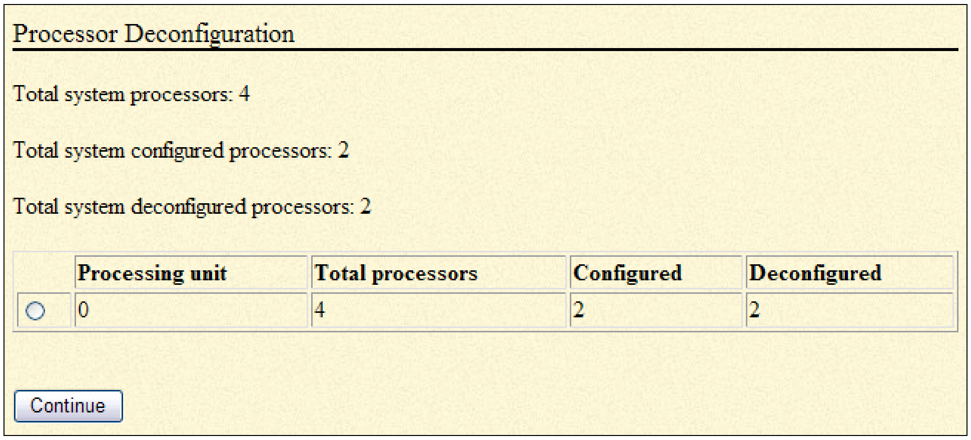
  Select the policy to deconfigure on system bus failures. Applies to run time or persistent boot time deconfiguration of processing unit resources or functions with system bus failures, such as check stop errors or uncorrectable errors.

  This policy is not applicable for systems with one processing unit node. If enabled, the particular resource or function that is affected by the failure is deconfigured.

  This configuration applies to resource types such as processor, L2 cache, L3 cache, and memory.

Processor Deconfiguration option

If a single processor fails, a possibility is to continue operating, with degraded performance, on fewer processors. Use the panel (Figure 6-59) to start removing processors that might have failed or are beginning to generate errors. You can also see processors that might be deconfigured because of an error condition that the system was able to detect and isolate.



Processor Deconfiguration

Total system processors: 4

Total system configured processors: 2

Total system deconfigured processors: 2

	Processing unit	Total processors	Configured	Deconfigured
○	0	4	2	2

Figure 6-59 Processor Deconfiguration window

All processor failures that stop the system, even if intermittent, are reported to the authorized service provider as a diagnostic dial-out for a service repair action. To prevent the recurrence of intermittent problems and improve the availability of the system until a scheduled maintenance window can be found, processors with a failure history are marked `deconfigured` to prevent them from being configured on subsequent boots. Processors marked as deconfigured remain offline and are omitted from the system configuration.

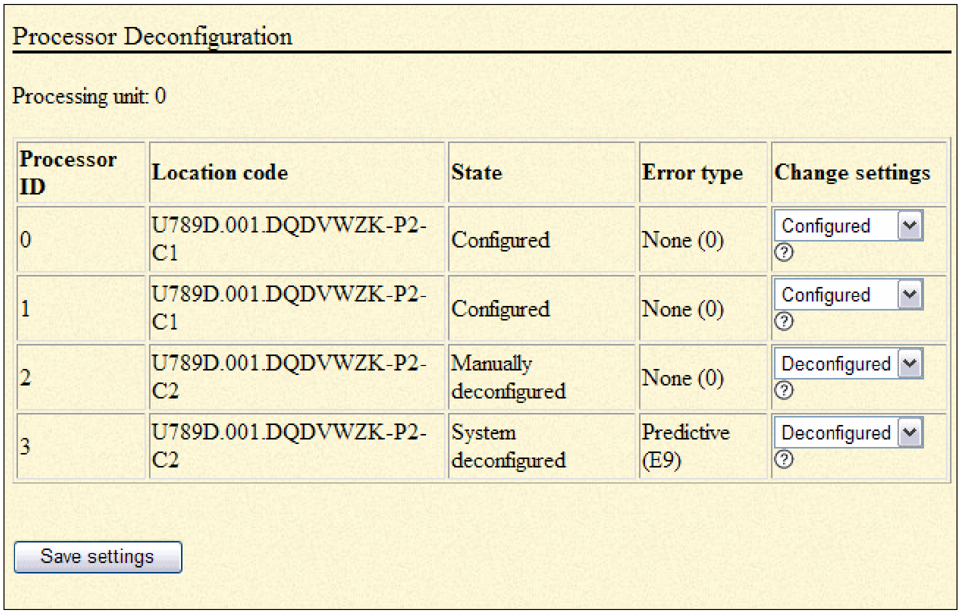
A processor is marked `deconfigured` under the following circumstances:

- If a processor fails built-in self-test or power-on self-test testing during boot (as determined by the service processor).
- If a processor causes a machine check or check stop during run time, and the failure can be isolated specifically to that processor (as determined by the processor runtime diagnostics in the service processor firmware).
- If a processor reaches a threshold of recovered failures that results in a predictive call to the service provider (as determined by the processor runtime diagnostics in the service processor firmware).

The deconfiguration policy also provides the user with the option to manually deconfigure a processor or re-enable a previous manually deconfigured processor.

To begin the process, select a processing unit (one or more processing units can be listed) and click **Continue**.

Select the setting to configure or deconfigure for the processors and select **Save settings** (Figure 6-60).



Processor Deconfiguration

Processing unit: 0

Processor ID	Location code	State	Error type	Change settings
0	U789D.001.DQDVWZK-P2-C1	Configured	None (0)	Configured ?
1	U789D.001.DQDVWZK-P2-C1	Configured	None (0)	Configured ?
2	U789D.001.DQDVWZK-P2-C2	Manually deconfigured	None (0)	Deconfigured ?
3	U789D.001.DQDVWZK-P2-C2	System deconfigured	Predictive (E9)	Deconfigured ?

Figure 6-60 Processor Deconfiguration window

Memory Deconfiguration option

Most System Power Systems have several gigabytes (GB) of memory. Each memory bank contains two dual inline memory modules (DIMMs). If the firmware detects a failure, or predictive failure of a DIMM, it deconfigures the DIMM with the failure, and the other one. All memory failures that stop the system, even if intermittent, are reported to the authorized service provider as a diagnostic dial-out for a service repair action.

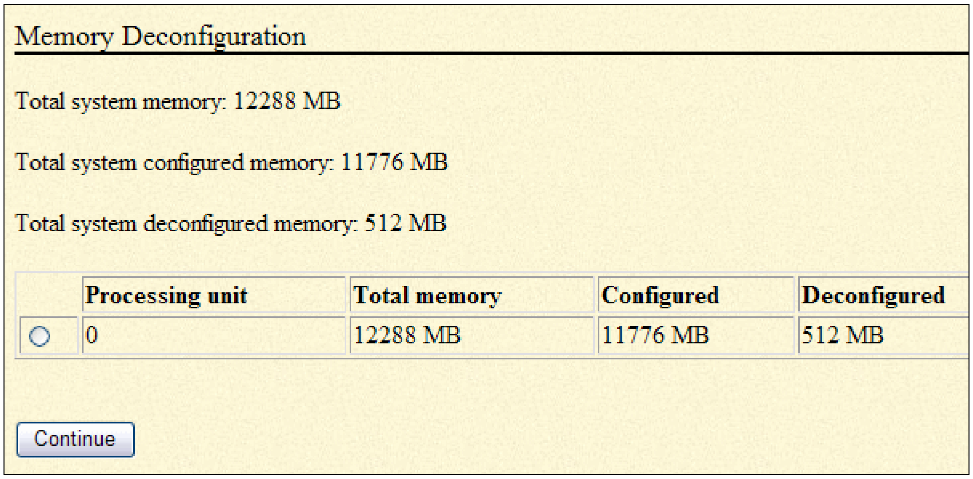
To prevent the recurrence of intermittent problems and improve the availability of the system until a scheduled maintenance window can be found, memory banks with a failure history are marked `deconfigured`. This status prevents them from being configured on subsequent boots. Memory banks marked as deconfigured remain offline and are omitted from the system configuration.

A memory bank is marked `deconfigured` under the following circumstances:

- If a memory bank fails built-in self-test or power-on self-test testing during boot (as determined by the service processor).
- If a memory bank causes a machine check or check stop during run time, and the failure can be isolated specifically to that memory bank (as determined by the processor runtime diagnostics in the service processor firmware).
- If a memory bank reaches a threshold of recovered failures that results in a predictive call to the service provider (as determined by the processor runtime diagnostics in the service processor firmware).

The deconfiguration policy also provides the user with the option to manually deconfigure a memory bank or re-enable a previous manually deconfigured memory bank.

If you select **Memory Deconfiguration** from the Hardware Deconfiguration menu, the Memory Deconfiguration panel opens (Figure 6-61). Use this panel to view the total memory that is installed on your system. From this panel, you can select the processing unit (one or more processing units can be listed). The reason that `Processing Unit` is listed is because the memory is installed on the processor board. Click **Continue** to advance to the next panel.



Memory Deconfiguration

Total system memory: 12288 MB

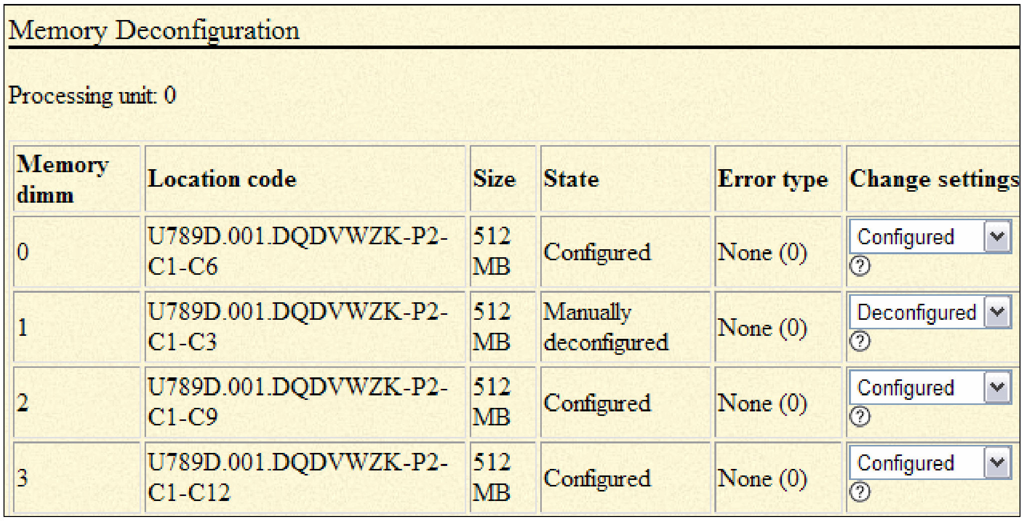
Total system configured memory: 11776 MB

Total system deconfigured memory: 512 MB

	Processing unit	Total memory	Configured	Deconfigured
○	0	12288 MB	11776 MB	512 MB

Figure 6-61 Memory Deconfiguration window

A new panel opens (Figure 6-62). It lists any memory banks that might be deconfigured because of an error condition that the system was able to detect and isolate. You can change the setting to configured or deconfigured for each memory bank and click **Save settings**.



Memory Deconfiguration

Processing unit: 0

Memory dimm	Location code	Size	State	Error type	Change settings
0	U789D.001.DQDVWZK-P2-C1-C6	512 MB	Configured	None (0)	Configured
1	U789D.001.DQDVWZK-P2-C1-C3	512 MB	Manually deconfigured	None (0)	Deconfigured
2	U789D.001.DQDVWZK-P2-C1-C9	512 MB	Configured	None (0)	Configured
3	U789D.001.DQDVWZK-P2-C1-C12	512 MB	Configured	None (0)	Configured

Figure 6-62 Memory deconfiguration memory bank selection

Program Vital Product Data menu options

With ASMI, you can program the system vital product data (VPD) such as system brand, system keywords, and system enclosure type (Figure 6-63). To access any of the VPD-related panels, your authority level must be *administrator* or *authorized service provider*.

> **Starting the system:** You cannot boot the system until valid values are entered for the system brand, system identifiers, and system enclosure type.

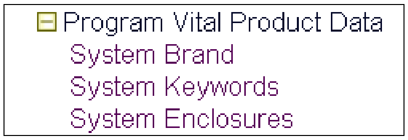


Figure 6-63 Program Vital Product Data panel

System Brand option

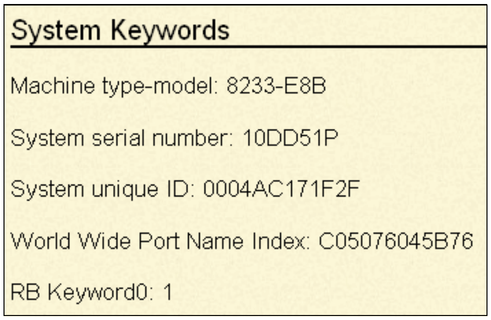
Enter a two-character brand type. The first character must be one of the following characters:

D	IBM Storage
I	IBM System i
N	OEM IBM System i only
O	OEM IBM System p only
P	IBM System p

The second character is reserved. A value of zero means that no specific information is associated with it. This entry is write-once only, except in the case where it is all blanks, or when changing from a System p system to an IBM Storage system. Any other changes are disallowed. A valid value is required for the machine to boot. Additionally, for IBM Storage, each of the systems that constitutes the storage facility must have the first character set to **D** for storage to be accessible online.

System Keywords option

You can set various keywords (Figure 6-64).



System Keywords

Machine type-model: 8233-E8B

System serial number: 10DD51P

System unique ID: 0004AC171F2F

World Wide Port Name Index: C05076045B76

RB Keyword0: 1

Figure 6-64 System Keywords display example

Settings are as follows:

- Machine type-model

  Enter a machine type and model in the form `TTTT-MMM`, where `TTTT` is the 4-character machine type and `MMM` is the 3-character model. A valid value is required for the machine to boot. Also, for storage to be accessible online, this value must exactly match both systems that constitute the storage facility. This entry is write-once only.

- System serial number

  Enter a system serial number in the form *XXYYYYY*, where *XX* is the code for the plant of manufacture and *YYYYY* is the unit sequence number. Valid characters are 0 - 9 and A - Z. A valid value is required for the machine to boot. This entry is write-once only.

- System unique ID

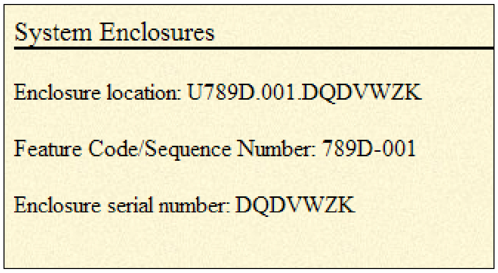
  For the system, enter a unique serial number as 12 hexadecimal digits. The value must be unique to a specific system anywhere in the world. A valid value is required for the machine to boot. If you do not know the system-unique ID, contact your next level of support.

- Worldwide port name

  Enter a 16-digit hexadecimal number for the worldwide node name. This value is an IEEE-assigned 64-bit identifier for the storage facility. A valid value is required for the machine to boot. This entry is write-once only.

System Enclosures option

The System Enclosures panel is shown in Figure 6-65. When setting the system enclosure type, ensure that the enclosure serial number field matches the original value, which can be found on a label affixed to the unit. Updating the enclosure serial number field keeps the configuration and error information synchronized. This information is used by the system when you create the location codes. This task must be done by using the ASMI, not with the control panel. However, if you do not have access to the ASMI, the system still operates without updating this information.



System Enclosures

Enclosure location: U789D.001.DQDVWZK

Feature Code/Sequence Number: 789D-001

Enclosure serial number: DQDVWZK

Figure 6-65 System Enclosures display example

Enter the following information

- Feature code and sequence number

  Enter a feature code and sequence number in the form *FFFF-SSS*, where *FFFF* is the 4-character feature and *SSS* is the 3-character sequence number. The Feature Code/Sequence Number is used to uniquely identify the type of the enclosure that is attached to the system. A valid value is required for the machine to boot. When this value is changed, the service processor reboots so that the location codes can be updated accordingly.

- Enclosure serial number

  Enter an enclosure serial number in the form *XXYYYYY*, where *XX* is the code for the plant of manufacture and *YYYYY* is the unit sequence number. Valid characters are 0 - 9 and A - Z. This serial number is attached to the enclosure. A valid value is required for the machine to boot. When this value is changed, the service processor reboots so that the location codes can be updated accordingly.

Service Indicators menu options

Use this menu (Figure 6-66) to turn off the system attention indicator, enable enclosure indicators, change indicators by location code, and perform an LED test on the control panel.

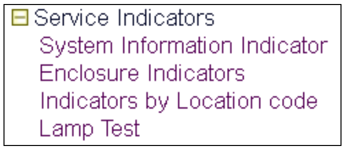


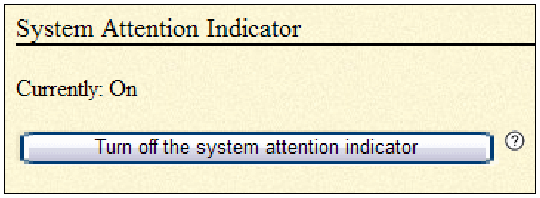
Figure 6-66 Service Indicators menu

The service indicators alert you that the system requires attention or service. It also provides a method for identifying a field-replaceable unit (FRU) or a specific enclosure within the system. A hierarchical relationship exists between FRU indicators and enclosure indicators. If any FRU indicator is in an identify state, then the corresponding enclosure indicator changes to an identify state automatically. You cannot turn off the enclosure indicator until all FRU indicators within that enclosure are in an off state.

System Attention Indicator option

If the indicator is *on*, click **Turn off the system attention indicator** (Figure 6-67).

> **Note:** Depending on the version of HMC, the service indicators can be a System Attention Indicator, System Information Indicator, or System Service Indicator.

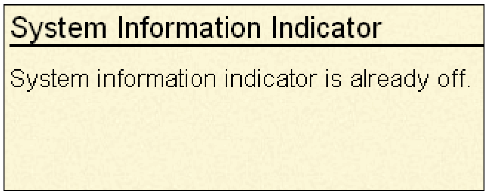


System Attention Indicator

Currently: On

Figure 6-67 System Attention Indicator when indicator is On

If the indicator is *off*, you cannot use this option to turn the system attention indicator on again. Figure 6-68 shows the System Attention Indicator when the indicator is off.



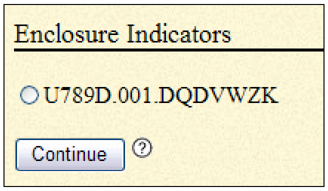
System Information Indicator

System information indicator is already off.

Figure 6-68 System Information Indicator when indicator is Off

Enclosure Indicators option

You can turn on or off the identify indicators in each enclosure. An enclosure is a group of indicators. For example, a processing unit enclosure represents all of the indicators within the processing unit and an I/O enclosure represents all of the indicators within that I/O enclosure. Enclosures are listed by their location code. Select an indicator (Figure 6-69) and click **Continue**.

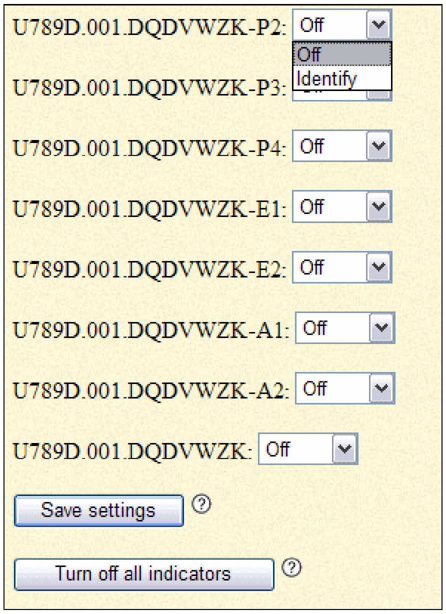


Enclosure Indicators

○ U789D.001.DQDVWZK

Figure 6-69 Enclosure Indicators window

In the next panel (Figure 6-70), select **Off** or **Identify** as appropriate. Alternatively, select **Turn off all indicators** to reset the LEDs. Then, click **Save settings**.



U789D.001.DQDVWZK-P2: Off

U789D.001.DQDVWZK-P3:

U789D.001.DQDVWZK-P4: Off

U789D.001.DQDVWZK-E1: Off

U789D.001.DQDVWZK-E2: Off

U789D.001.DQDVWZK-A1: Off

U789D.001.DQDVWZK-A2: Off

U789D.001.DQDVWZK: Off

Figure 6-70 Enclosure Identify window

Indicators by Location code option

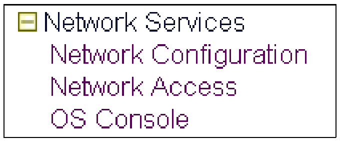
You can specify the location code of any indicator to view or modify its current state. If you provide the wrong location code, the advanced system manager attempts to go to the next higher level of the location code. The next level is the base-level location code for that FRU. For example, a user types the location code for the FRU on the second I/O slot of the third enclosure in the system. If the location code for the second I/O slot is incorrect (the FRU does not exist at this location), an attempt to set the indicator for the third enclosure is initiated. This process continues until an FRU is located or no other level is available.

Lamp test option

You can perform an LED test on the control panel to determine if one of the LEDs is not functioning properly. Select **Lamp test**. Click **Continue** to do the lamp test. The test changes all indicators to the identify the state for a short time (approximately 4 minutes).

6.10.8 Network Services menu options

Use the options in this menu (Figure 6-71) to configure the number and types of network interfaces according to the needs of your system.



⊟ Network Services
Network Configuration
Network Access
OS Console

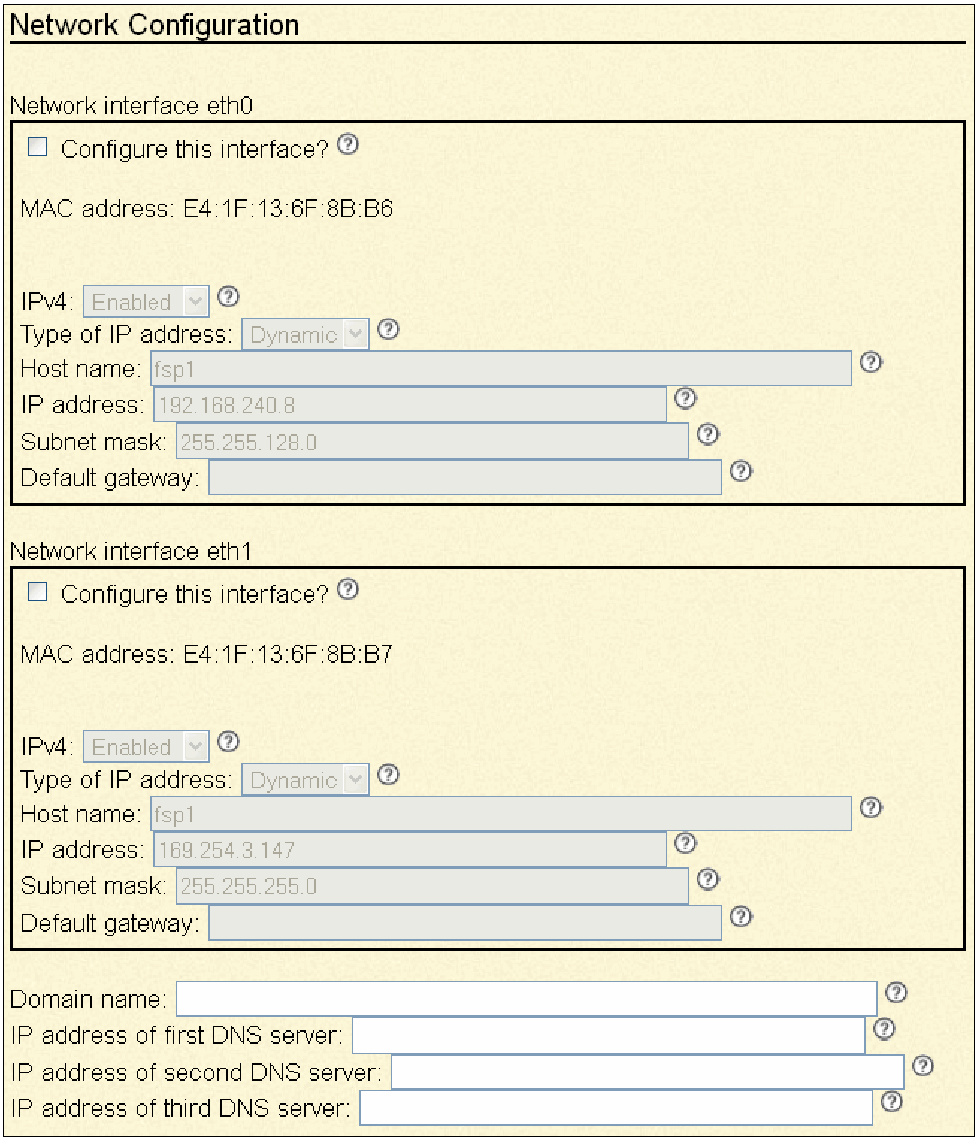
Figure 6-71 Network Services menu

Network Configuration option

This operation can be performed when the system is turned on and off. Because network configuration changes occur immediately, existing network sessions, such as HMC connections, are stopped. If a firmware update is in progress, do not do this operation. The new settings must be used to reestablish any network connections.

More errors can also be logged if the system is turned on.

Figure 6-72 shows the configuration of network interfaces.



Network Configuration

Network interface eth0

□ Configure this interface?

MAC address: E4:1F:13:6F:8B:B6

IPv4: Enabled
Type of IP address: Dynamic
Host name: fsp1
IP address: 192.168.240.8
Subnet mask: 255.255.128.0
Default gateway:

Network interface eth1

□ Configure this interface?

MAC address: E4:1F:13:6F:8B:B7

IPv4: Enabled
Type of IP address: Dynamic
Host name: fsp1
IP address: 169.254.3.147
Subnet mask: 255.255.255.0
Default gateway:

Domain name:
IP address of first DNS server:
IP address of second DNS server:
IP address of third DNS server:

Figure 6-72 HMC Ethernet port configuration

This window sets the following information:

- Configure this interface

  Configures this interface. If not selected, then the corresponding fields are ignored.

- Type of IP address

  Select the IP address type for this interface. If you select **Dynamic**, network configuration data is obtained from the DHCP server. Typically, your HMC is your DHCP server that is connected to service processor Ethernet port1.

- Host name

  Enter a new value for the host name.

  The following characters are valid: hyphen (-), period (.), uppercase and lowercase alphabetics (A - Z and a - z), and numeric (0 - 9).

The first character must be alphabetic or numeric and the last character must not be a hyphen or a period. However, if the host name contains a period, then the preceding characters must have an alphabetic character. This input is required for the static type of IP address.

- Domain name

  Enter a new value for the domain name. All alphanumeric characters and the symbols hyphen (-), underscore (_), and period (.) are valid.

- IP address

  Enter a new value for the IP address. This input is required for the static IP address type.

- Subnet mask

  Enter a new value for the subnet mask. This input is required for the static IP address type.

- Default gateway

  Enter a new value for the default gateway.

- IP address of first DNS server

  Enter a new value for the first DNS server.

- IP address of second DNS server

  Enter a new value for the second DNS server.

- IP address of third DNS server

  Enter a new value for the third DNS server.

- Reset Network Configuration

  Resets the Network Configuration settings to their default factory settings.

- Network Configuration

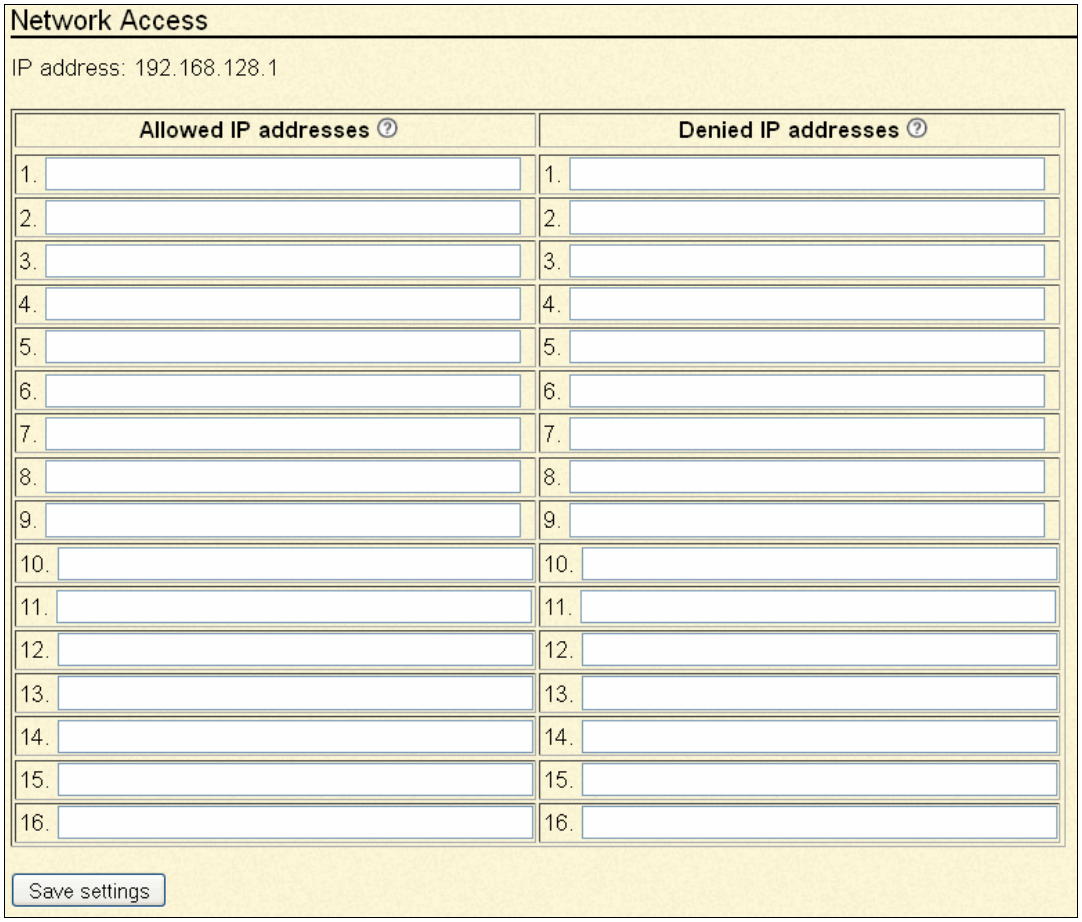
  Select service processor to be configured. The default is the current service processor.

Click **Save Settings**. The network configuration changes are made and the service processor is rebooted. As the service processor reboots, your ASMI session drops and you must reconnect the session to continue. When you reconnect, you are then using the new settings.

Network Access window

When you configure network access (Figure 6-73 on page 504), you specify which IP addresses can access the service processor. You can specify a list of allowed IP addresses and a list of denied IP addresses.

> **Allowed and denied lists:** The allowed list takes priority over the denied list, and an empty denied list is ignored. `ALL` is not allowed in the denied list if the allowed list is empty.


Network Access

IP address: 192.168.128.1

Allowed IP addresses	Denied IP addresses
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.
6.	6.
7.	7.
8.	8.
9.	9.
10.	10.
11.	11.
12.	12.
13.	13.
14.	14.
15.	15.
16.	16.

Figure 6-73 Network Access window

This window has two lists:

- Allowed IP addresses

  Enter up to 16 complete or partial IP addresses:

  – A complete IP address contains all four octets.
  – A partial IP address has only one, two, or three3 octets, and must end in a period. If a login is received from an IP address, which matches a complete or partial IP address in the allowed list, access to the service processor is granted.

  To allow access to the service processor from any IP address, enter `ALL` in the allowed list. An empty allowed list is ignored and access is granted from any IP address.

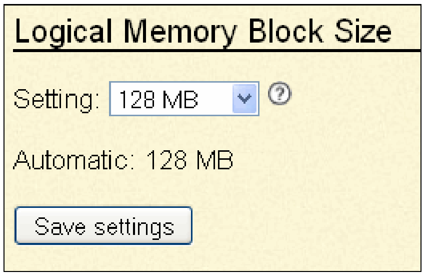
- Denied IP addresses

  Enter up to 16 complete or partial IP addresses to be denied. Access to the service processor is not allowed if a login is received from an IP address that is listed in this list.

  To deny access from any IP address, enter `ALL` in the list. If an incorrect IP address is entered in the allowed list and the denied list contains `ALL`, access to the service processor can be permanently denied. In this case, reset the network parameters by using the network reset parameters switch on the service processor card. An empty denied list is ignored and the allowed list takes priority over the denied list. For these reasons, `ALL` is not allowed in the denied list if the allowed list is empty.

6.10.9 Performance Setup menu options

You can enhance the managed system performance by manually or automatically changing the logical memory block size. The system kernel uses the memory block size to read and write files. By default, the logical memory block size is set to `Automatic`. This setting allows the system to set the logical block memory size that is based on the physical memory available. You can also manually change the logical memory block size (Figure 6-74).


Logical Memory Block Size

Setting: 128 MB

Automatic: 128 MB

Figure 6-74 Performance setup

To select a reasonable logical block size for your system, consider both the performance that is needed and the physical memory size. Use the following guidelines when you select logical block sizes:

- On systems with a small amount of memory installed (2 GB or less), a large logical memory block size results in the firmware consuming an excessive amount of memory. Firmware must consume at least one logical memory block. Generally, select the logical memory block size to be no greater than one-eighth the size of the physical memory of the system.
- On systems with a large amount of memory that is installed, small logical memory block sizes result in many logical memory blocks. Because each logical memory block must be managed during boot, many logical memory blocks can cause boot performance problems. Generally, limit the number of logical memory blocks to 8 K or less.

> **Note:** The logical memory block size can be changed at run time, but the change does not take effect until the system is restarted.

Select **Logical Memory Block Size** and then specify the size and click **Save settings**.

System Memory Page setup

Improve your system performance by setting up the system with larger memory pages. Performance improvements vary depending on the applications running on your system. Only change this setting if advised by service and support.

To change the system memory page setup, select **System Memory Page Setup**. In the right pane, select the settings that you want, and then click **Save settings**.

6.10.10 On Demand Utilities menu options

Activate inactive processors or inactive system memory without restarting your server or interrupting your business. With Capacity on Demand (CoD), you can permanently activate inactive processors or inactive system memory without needing to restart the server or interrupt your business. You can also view information about your CoD resources.

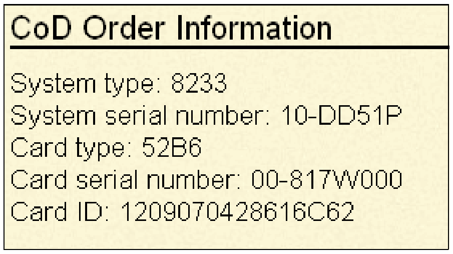
> **Important:**
>
> - Use this information if a hardware failure causes the system to lose its CoD or function on demand purchased capabilities, and if there never was an HMC managing the system. If an HMC is managing the system, use the HMC to do the following tasks instead of the ASMI.
> - To decide whether to use CoD, see 5.11, "Capacity on Demand (CoD)" on page 405.

CoD Order Information option

If you want to permanently activate some or all of your inactive processors or memory, you must first order one or more processor or memory activation features. You then enter the resulting processor or memory-activation key that is provided by your hardware provider to activate your inactive processors or memory.

To order processor or memory activation features select **On Demand Utilities** → **Select CoD Order Information**.

The server firmware displays the information (Figure 6-75) you need for ordering a Capacity on Demand activation feature. Record this information and click **Continue**.



CoD Order Information

System type: 8233
System serial number: 10-DD51P
Card type: 52B6
Card serial number: 00-817W000
Card ID: 1209070428616C62

Figure 6-75 CoD Order Information example

CoD activation

To activate this feature, click **Demand Utilities** → **CoD Activation**. Enter the activation key into the field and click **Continue** to do the specified operation. See Figure 6-76.

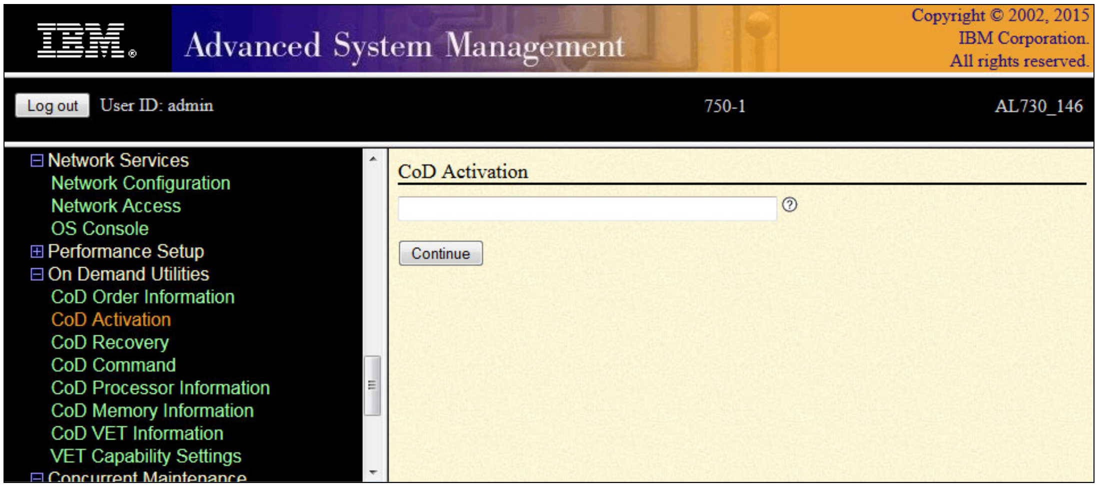


Figure 6-76 CoD Activation window

CoD Recovery option

This process resumes the booting process of the server firmware after the CoD activation keys are entered. Resuming the server firmware causes the CoD key to become recognized and the hardware to become activated. This option allows the server to complete the startup process that is delayed up to one hour to place the server into the On Demand Recovery state that was needed to enter the CoD activation keys.

Select **On Demand Utilities** → **CoD Recovery**. Enter the activation key into the field and click **Continue** to do the specified operation (Figure 6-76).

CoD Command option

Select **On Demand Utilities** → **CoD Command**. Enter the command into the field and click **Continue**.

Options for viewing information about CoD resources

When CoD is activated on your system, you can view information about the CoD processors, the memory that is allocated as CoD memory, and Virtualization Engine technology resources.

Select **On Demand Utilities**, and then select one of the following options for the type of information that you want to view:

- **CoD Processor Information** to view information about the CoD processors.
- **CoD Memory Information** to view information about available CoD memory.
- **CoD VET Information** to view information about available Virtualization Engine technologies.
- **VET Capability Settings** to view information about the CoD capabilities that are enabled.

6.10.11 Login Profile menu options

You can change passwords, view login audits, change the default language, and update the installed languages.

Change Password option

You can change the general user, administrator, and HMC access passwords. As a general user, you can change only your own password. As an administrator, you can change your password and the passwords for general user accounts. As an authorized service provider, you can change your password, the passwords for general and administrator user accounts, and the HMC access password.

Passwords can be any combination of up to 64 alphanumeric characters. The default password for the general user ID is `general`, and the default password for the administrator ID is `admin`. After your initial login to the ASMI and after the reset toggle jumpers are moved, the general user and administrator passwords must be changed. The HMC access password is usually set from the HMC during initial login. If you change this password by using the ASMI, the change takes effect immediately.

> **Security measure:** As a security measure, you are required to enter the current user's password into the current password for the current user field. This password is not the password for the user ID you want to change.

To change the password, select **Login Profile** → **Change Password**. In the window that opens, enter the appropriate information and click **Continue**.

Retrieve Login Audits option

You can view the login history for the ASMI to see the last 20 successful logins and the last 20 logins that failed. To view login audit, select **Login Profile** → **Retrieve Login Audits**.

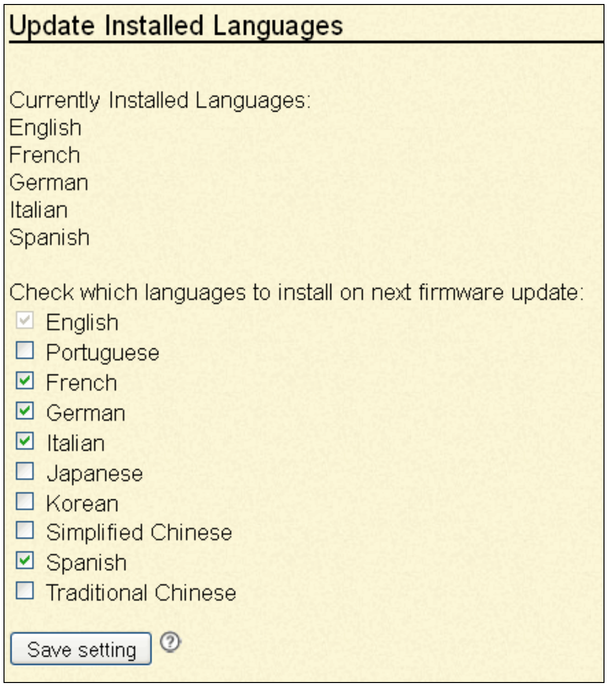
Change Default Language option

You can select the language that is displayed on the ASMI welcome window before login and during your ASMI session if you do not choose an alternative language at the time of login. You must provide all requested input in English language characters regardless of the language that is selected to view the interface.

To change the default language, select **Login Profile** → **Change Default Language**. Select the language and click **Save Settings**.

Update Installed Languages option

A maximum of five languages can be supported on the service processor at any specified time. By default, English is always installed. Languages installation changes take effect when the firmware is updated. See Figure 6-77.



Update Installed Languages

Currently Installed Languages:
English
French
German
Italian
Spanish

Check which languages to install on next firmware update:

- ☑ English
- □ Portuguese
- ☑ French
- ☑ German
- ☑ Italian
- □ Japanese
- □ Korean
- □ Simplified Chinese
- ☑ Spanish
- □ Traditional Chinese

Figure 6-77 Update Installed Languages menu

To choose a language to install at the next firmware update, select **Login Profile** → **Update Installed Language**. Select a maximum of five languages and then click **Save setting**.

User Access Policy option

This menu enables the admin user to grant or deny the access to service and development personnel by enabling or disabling dev, celogin, celogin1, and celogin2. Enabling access policy for celogin1 and celogin2 requires new passwords to be set even if they were set before.

To enable user access, select **Login Profile** → **User Access Policy**. Then, select the user ID and policy setting, and click **Continue**. Enter the admin password and new password for the user.

You have the following password options:

- Current password for user ID

  As a security measure, the current password must be supplied.

- New password for user

  Enter the new password for the user whose password you want to change.

- New password again

  Enter the new password for the user again for verification.

7

Performance and capacity monitoring

This chapter introduces the Performance and Capacity Monitor (PCM) of the Hardware Management Console (HMC).

This chapter describes the following topics:

- Overview
- Enabling Performance and Capacity Monitor data collection
- Graphical user interface (GUI)
- Views pane
- Troubleshooting

7.1 Overview

The Performance and Capacity Monitor (PCM) is an HMC graphical user interface (GUI) that displays performance and capacity data for managed servers and logical partitions (LPARs). The PCM displays data for a single physical server in a new browser window.

The PCM allows the HMC to gather performance data so that a system administrator can monitor current performance and capacity changes in their IBM Power systems environment over time.

Using the PCM information of physical servers and logical partitions, a system administrator can determine whether there are any performance problems, and correct the causes of those performance problems. A system administrator can also gather capacity information to support capacity planning and optimize resource allocation.

The PCM feature is available since HMC V8.8.1.0, and supports Power6 technology-based servers or later. It reports the CPU, memory and I/O utilization of Managed Systems resources. When managing Virtual I/O Server 2.2.3 or later with System Firmware 780 or later, it also provides a view of the PowerVM and I/O utilization.

> **Note:** Virtual I/O Servers (VIOS) upgraded to 2.2.3 might not automatically start the performance provider subsystem. To determine whether the performance subsystem is running, use the following command:
>
> ```
> ps -ef |grep pcm
> ```
>
> The return output is similar to the following line:
>
> ```
> root 7536870 4915370 Jul 07 - 0:41 /usr/perf/pcm/srcloop
> ```
>
> For further information about the issue and recovery see VIOS APAR IV63625:
>
> http://www.ibm.com/support/docview.wss?uid=isg1IV63625

7.2 Enabling Performance and Capacity Monitor data collection

You can enable the PCM. Data collection is disabled for all managed servers by default. Server resource utilization monitoring starts after you enable data collection and continues until you disable it. All utilization data is stored on the HMC hard disk drive (HDD).

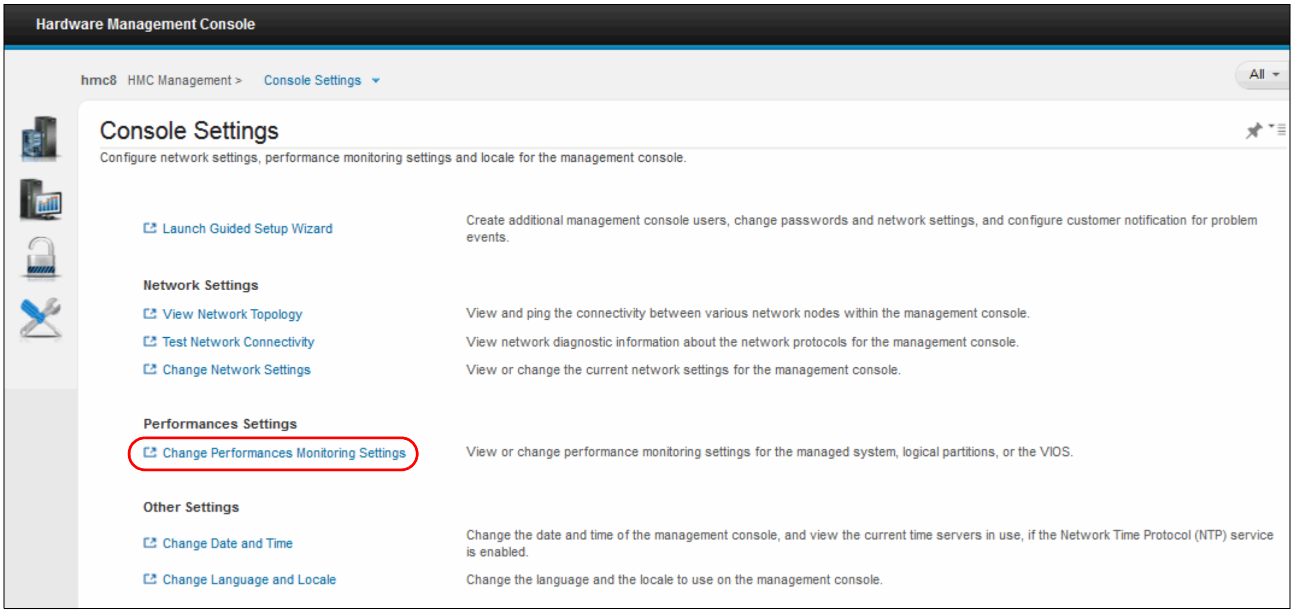
Ensure that the following prerequisites are satisfied:

- You must have the *Manage Utilization Data* access permission to change the data collection settings.
- The data collection can be turned on for managed systems that are in any state, but the data is collected and stored by the HMC only when the managed system is in the Operational state.

To enable the PCM data collection, complete the following steps:

1. In the main window, click **HMC Management** → **Console Settings** → **Change Performances Monitoring Settings** (Figure 7-1).

   (For the old HMC surface, select **HMC Management** → **Change Performance Monitoring Settings**.)



Hardware Management Console

hmc8 HMC Management > Console Settings

All

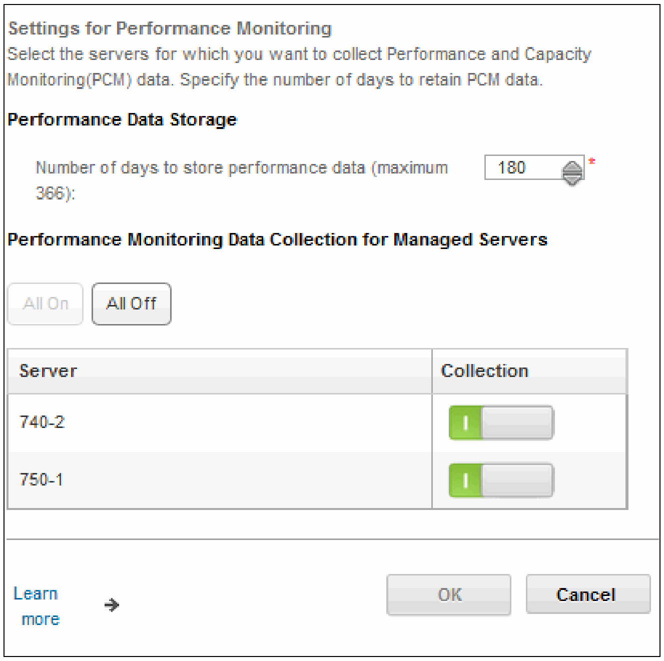
Console Settings

Configure network settings, performance monitoring settings and locale for the management console.

Launch Guided Setup Wizard	Create additional management console users, change passwords and network settings, and configure customer notification for problem events.
Network Settings	
View Network Topology	View and ping the connectivity between various network nodes within the management console.
Test Network Connectivity	View network diagnostic information about the network protocols for the management console.
Change Network Settings	View or change the current network settings for the management console.
Performances Settings	
Change Performances Monitoring Settings	View or change performance monitoring settings for the managed system, logical partitions, or the VIOS.
Other Settings	
Change Date and Time	Change the date and time of the management console, and view the current time servers in use, if the Network Time Protocol (NTP) service is enabled.
Change Language and Locale	Change the language and the locale to use on the management console.

Figure 7-1 Change Performances Monitoring Settings

2. Enable or disable performance monitoring from the Settings for Performance Monitoring window (Figure 7-2).



Settings for Performance Monitoring

Select the servers for which you want to collect Performance and Capacity Monitoring(PCM) data. Specify the number of days to retain PCM data.

Performance Data Storage

Number of days to store performance data (maximum 366): 180 *

Performance Monitoring Data Collection for Managed Servers

All On | All Off

Server	Collection
740-2	I
750-1	I

Learn more

OK | Cancel

Figure 7-2 Settings for Performance Monitoring window

In the Settings for Performance Monitoring window, you can configure these settings:

- Performance Data Storage

  Specify the number of days to store the performance data for the selected managed system. Valid values are 1 - 366; the displayed default value is 180.

- Performance Monitoring Data Collection for Managed Servers

  Click the toggle switch in the collection column next to the name of the managed system for which you want to enable or disable data collection. A green toggle shows that performance monitoring is activated, and a red toggle shows that performance monitoring is disabled. You can click **All On** or **All Off** to enable or disable data collection for all the managed systems in your environment.

  > **Note:** The All On option might be disabled when insufficient storage exists to enable data collection for all the managed systems. A warning message is displayed to indicate the number of managed systems for which the data can be collected.

3. Click **OK** to apply the changes and close the window.

After the data collection is turned on, you can view the collected data on the PCM page (see 7.3.2, “Performance and Capacity Monitor home page” on page 516). On the PCM page, collecting enough data to display some of the graphs and tables might take awhile. If any error messages are displayed, you can wait for more data to be collected and refresh the view.

7.3 Graphical user interface (GUI)

The PCM has its own GUI, which is explained in this section.

7.3.1 Accessing the Performance and Capacity Monitor home page

After data collection is enabled, PCM plots the data in graphs and summarizes the information in tables. A user can view the graphs and table from the PCM home page.

To access the PCM home page from the Enhanced+ login HMC GUI, use these steps:

1. In the main HMC window, select **Resources** → **All Systems** and select your managed system.
2. Select **Actions** → **View Performance Dashboard** (Figure 7-3).

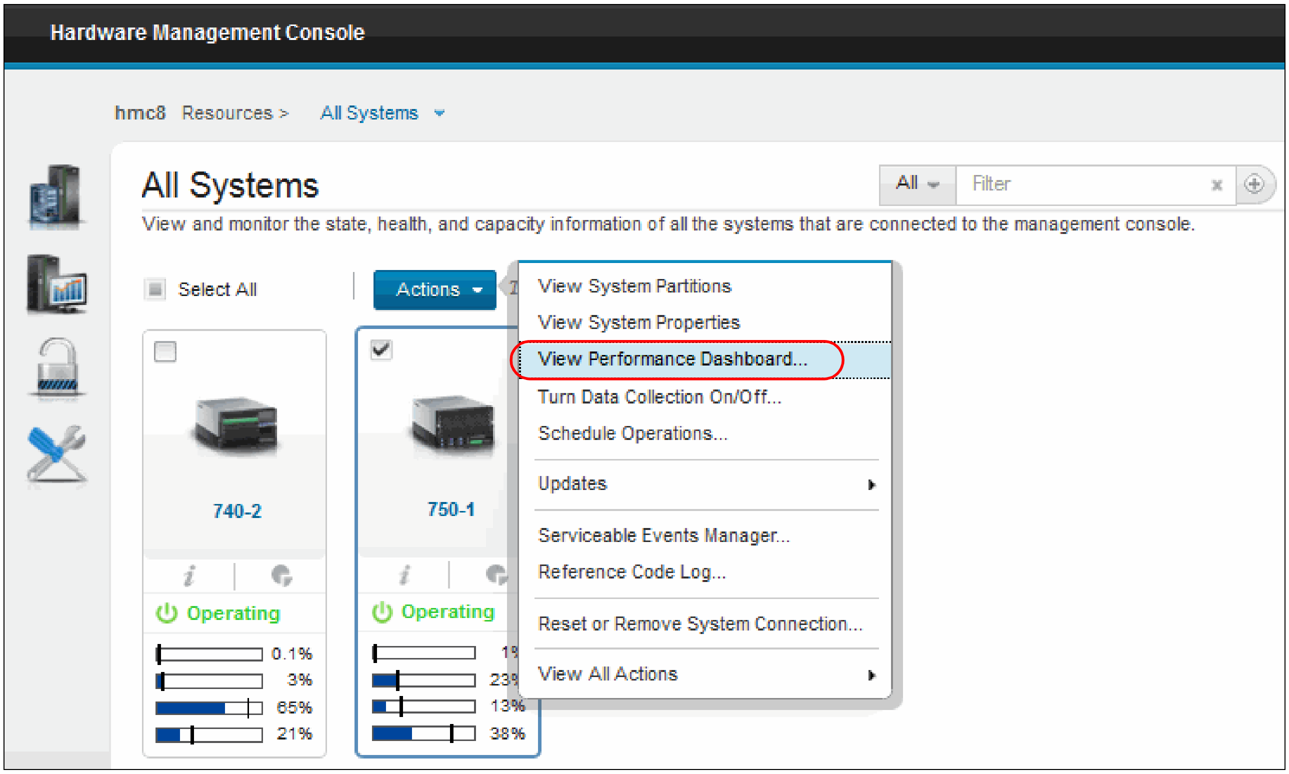

Hardware Management Console
hmc8 Resources > All Systems
All Systems
All
Filter
View and monitor the state, health, and capacity information of all the systems that are connected to the management console.
Select All
Actions
View System Partitions
View System Properties
View Performance Dashboard...
Turn Data Collection On/Off...
Schedule Operations...
Updates
Serviceable Events Manager...
Reference Code Log...
Reset or Remove System Connection...
View All Actions
740-2
750-1
Operating
Operating
0.1%
3%
65%
21%
1%
23%
13%
38%

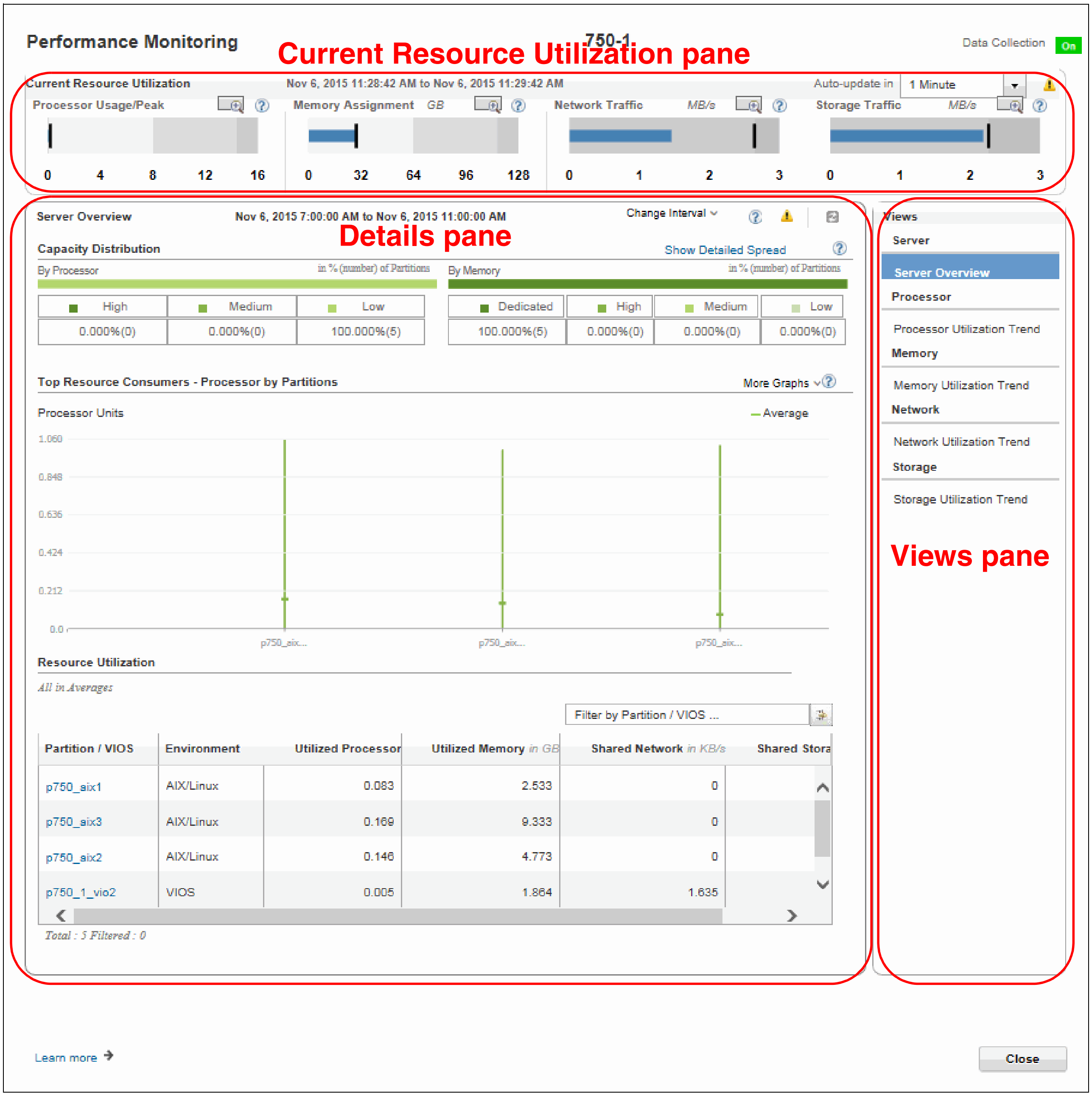
Figure 7-3 View Performance Dashboard

To access the PCM home page from the classic HMC GUI, use these steps:

1. In the navigation pane, click **Systems Management** and select your server.
2. Click **Performance**, or click the menu icon and select **Performance**.

7.3.2 Performance and Capacity Monitor home page

The PCM home page contains graphs and tables representing the data that is collected from the server, as shown in Figure 7-4.



Performance Monitoring 750-1

Data Collection On

Current Resource Utilization pane

Current Resource Utilization Nov 6, 2015 11:28:42 AM to Nov 6, 2015 11:29:42 AM Auto-update in 1 Minute

Details pane

Server Overview Nov 6, 2015 7:00:00 AM to Nov 6, 2015 11:00:00 AM Change Interval

Capacity Distribution Show Detailed Spread

By Processor in % (number) of Partitions

High	Medium	Low
0.000%(0)	0.000%(0)	100.000%(5)

By Memory in % (number) of Partitions

Dedicated	High	Medium	Low
100.000%(5)	0.000%(0)	0.000%(0)	0.000%(0)

Top Resource Consumers - Processor by Partitions More Graphs

Resource Utilization

All in Averages

Filter by Partition / VIOS ...

Partition / VIOS	Environment	Utilized Processor	Utilized Memory *in GB*	Shared Network *in KB/s*	Shared Stora
p750_aix1	AIX/Linux	0.083	2.533	0	
p750_aix3	AIX/Linux	0.169	9.333	0	
p750_aix2	AIX/Linux	0.146	4.773	0	
p750_1_vio2	VIOS	0.005	1.864	1.635	

Total : 5 Filtered : 0

Views pane

Figure 7-4 Performance and Capacity Monitor home page

Three panes are available in the PCM home window:

- Current Resource Utilization pane

  These graphs show the system processor utilization assignment, virtual network traffic, and virtual storage traffic compared against the available capacities or against their maximum historic highs.

- Views pane

  Shows a list of server resources for which a user can view performance data. The views include Server Overview, Processor Utilization Trend, Memory Utilization Trend, Network Utilization Trend, and Storage Utilization Trend.

- Details pane

  Displays the graph and charts that are associated with the view you selected from the Views pane.

7.3.3 Changing the Performance and Capacity Monitor home page settings

A user can change the time interval settings for the graphs in the PCM home page window.

Changing auto-update frequency of Current Resources Utilization pane

The Current Resource Utilization graphs default to an auto-update value of one minute, but a longer time interval can be specified.

To change the duration of time between updates, complete the following steps:

1. In the upper right corner of the Current Resource Utilization section, click the **Auto-update in** drop-down menu.
2. Select one of the following preset values:
   - 1 minute
   - 5 minutes
   - 10 minutes
   - 15 minutes

The data in the graphs refreshes according to the time interval you select. The data also is averaged over that time interval. For example, the bar for current processor utilization represents the average over whichever refresh interval is selected, and the maximum values observed during the selected interval.

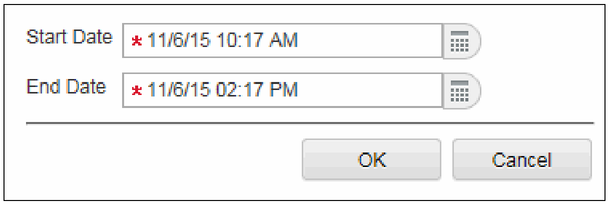
Changing time interval of data displayed in the Details pane

The default time interval in the Details pane is a four-hour time interval. However, a longer time interval can be specified. A user also can specify custom dates and times. The Details pane refreshes and displays the updated content based on the user time interval that is set and ends with the current time.

To change the time interval, complete the following steps:

1. Click the **Change Interval** drop-down menu in the upper right corner of the Detail pane.
2. Select one of the following preset values; otherwise, select **Custom**:
   - Last 4 Hours
   - Last Day
   - Last Week
   - Last Month
   - Last Year

If you select **Custom**, a window opens, where you specify date and time information in the Start Date and End Date fields (Figure 7-5). Click **OK** to apply your changes.



Start Date * 11/6/15 10:17 AM

End Date * 11/6/15 02:17 PM

Figure 7-5 Custom Time interval window

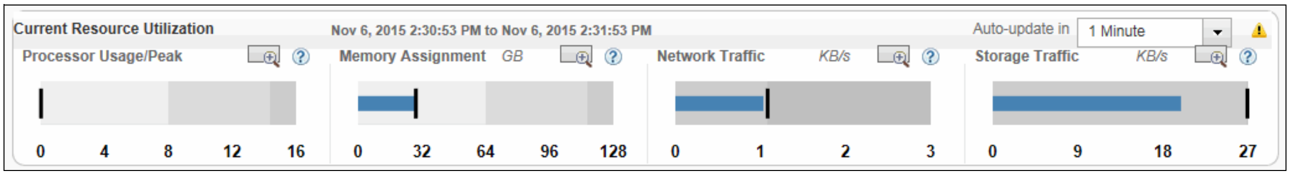
The start and end dates might not correspond exactly to the recent view because of the way the data is aggregated. The data is aggregated in the following ways:

- For the last seven days, the data samples are available every 15 minutes.
- For the last 30 days, the data samples are available every 2 hours.
- For data that is older than 30 days, one sample is available per day.

> **Note:** If the time interval is changed in one view, the interval change applies only to that view. For example, if you change the time interval for the Server Overview page to **Last Week**, the time interval for the Processor Trend view remains **Last 4 hours**.

7.3.4 Current Resource Utilization pane

The top of the PCM home page shows the Current Resource Utilization pane (Figure 7-6).



Current Resource Utilization

Nov 6, 2015 2:30:53 PM to Nov 6, 2015 2:31:53 PM

Auto-update in 1 Minute

Figure 7-6 Current Resource Utilization pane

The pane has four graphs:

- Processor Usage/Peak

  This graph represents current and peak utilization compared to the total number of processors available on the managed system.

- Memory Assignment

  This graph represents the current and recent peak utilization compared to the total amount of memory available on the managed system.

- Network Traffic

  This graph represents the average network traffic compared to the maximum amount of network bandwidth that the system used, this graph does not display traffic over physical adapters that are dedicated to logical partitions.

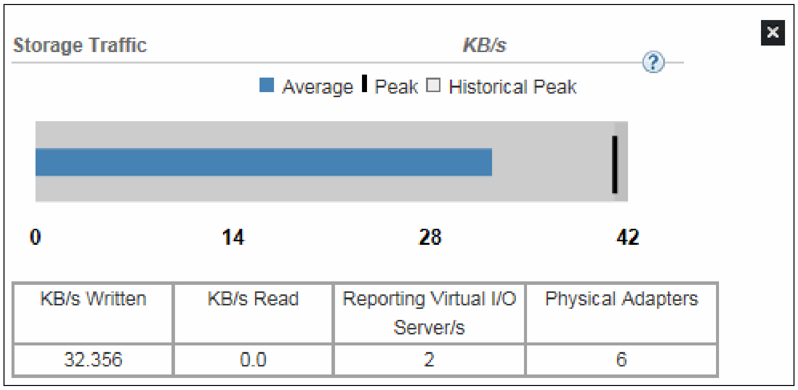
- Storage Traffic

  This graph represents the average storage traffic compared to the maximum I/O storage bandwidth that the system used. This graph does not display storage utilization from physical adapters that are dedicated to logical partitions.

The blue horizontal bar for each graph represents the current utilization; the black vertical bar represents the maximum utilization.

Note: The term *Available* for the Processor Usage/Peak and Memory Assignment graphs refers to activated licensed processor and memory. Additional installed processor and memory resources might be installed that can be activated through Capacity on Demand (see 5.11, “Capacity on Demand (CoD)” on page 405), but these resources are not considered as available resources.

Click the **Magnify** icon to display a larger view of the graph. In the enlarged view, the values that are depicted in the graph are also displayed in the table for easy understanding. For example, Figure 7-7 shows an enlarged view of the Storage Traffic graph.



KB/s Written	KB/s Read	Reporting Virtual I/O Server/s	Physical Adapters
32.356	0.0	2	6

Figure 7-7 Enlarged View of the Storage Traffic graph

If the overall usage is consistently high, you may want to consider activating more processors or more memory, moving workloads to other managed systems, or increasing the capacity.

7.4 Views pane

The Views pane of the PCM home page lists five views (Figure 7-8 on page 520):

- Server Overview
- Processor Utilization Trend
- Memory Utilization Trend
- Network Utilization Trend
- Storage Utilization Trend

The Server Overview displays the current (or recent) data, in contrast to the Utilization Trend views, which display historical trends over longer periods of time.

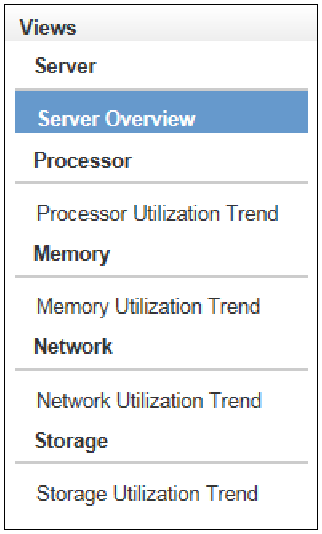


Figure 7-8 Views of the View pane

Select a view to see a graph in the Details pane.

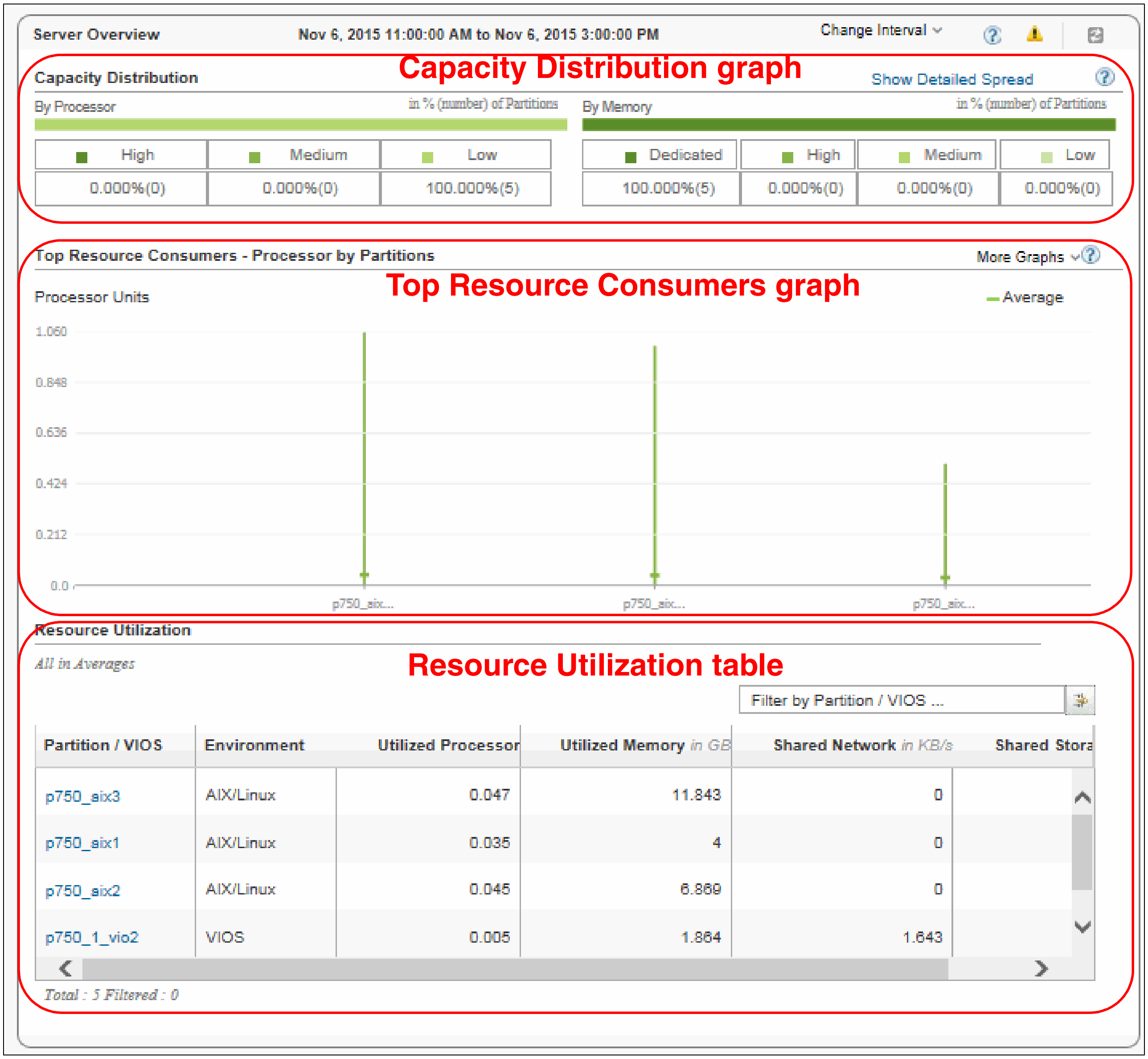
7.4.1 Server Overview view

The Server Overview contains graphs and tables that summarize data from virtualized server resources. This information helps you understand how physical processor and memory resources are allocated among the partitions on your server, Additionally, the information can help you understand whether partitions are using more or less than their entitled capacity for these resources.

The Server Overview is the default view when you open the Performance Monitoring Dashboard. If you open another view you can always return to the Server Overview by clicking **Server Overview** in the Views pane.

The Server Overview (Figure 7-9 on page 521) contains the following information:

- Capacity Distribution graphs (at the top)
  - By Processor
  - By Memory
- Top Resource Consumers graph (in the center)
- Resource Utilization table (at the bottom)



Server Overview Nov 6, 2015 11:00:00 AM to Nov 6, 2015 3:00:00 PM

Capacity Distribution graph

Capacity Distribution

By Processor in % (number) of Partitions

🟩 High	🟩 Medium	🟩 Low
0.000%(0)	0.000%(0)	100.000%(5)

By Memory in % (number) of Partitions

🟩 Dedicated	🟩 High	🟩 Medium	🟩 Low
100.000%(5)	0.000%(0)	0.000%(0)	0.000%(0)

Top Resource Consumers graph

Top Resource Consumers - Processor by Partitions

Resource Utilization table

Resource Utilization

All in Averages

Partition / VIOS	Environment	Utilized Processor	Utilized Memory *in GB*	Shared Network *in KB/s*	Shared Stora
p750_aix3	AIX/Linux	0.047	11.843	0	
p750_aix1	AIX/Linux	0.035	4	0	
p750_aix2	AIX/Linux	0.045	6.869	0	
p750_1_vio2	VIOS	0.005	1.864	1.643	

Total : 5 Filtered : 0

Figure 7-9 Server Overview view

Capacity Distribution By Processor graph

The Capacity Distribution by Processor graph shows the percentage and number of partitions whose processor usage is high, medium, or low relative to the partition’s entitled processor capacity. PCM designated processor utilization is high if the percentage is 91% or more, medium if the percentage is 50 - 90%, and low if the percentage is 50% or less.

No additional configurations are available for this graph. However, you can view a more detailed version. For more information see “Accessing and reviewing the Detailed Spread graphs” on page 522.

Capacity Distribution By Memory graph

The Capacity Distribution by Memory graph shows the percentage and number of partitions whose memory usage is high, medium, or low relative to the partition’s entitled memory capacity. PCM designated memory utilization is high if the percentage is 91% or more, medium if the percentage is 50 - 90%, and low if the percentage is 50% or less.

No additional configurations are available for this graph. However, you can view a more detailed version. For more information see “Accessing and reviewing the Detailed Spread graphs” on page 522.

Accessing and reviewing the Detailed Spread graphs

The Detailed Spread graphs provide an in-depth view of the partition metrics that are shown in the Capacity Distribution By Processor and By Memory graphs. Detailed Spread graphs show dots that represent individual partitions or Virtual I/O Servers whose current processor usage (vertical axis) is plotted against the entitlement (horizontal axis). You can view which partitions are using more or fewer resources than their entitlement. The diagonal lines have slopes of 0.5, 0.9, and 1.0, which represent usage relative to entitlement of 50%, 90%, and 100%. A partition whose position is above the 1.0 line is using more than 100% of its entitled capacity.

To show the Detailed Spread graphs, complete the following steps:

1. On the PCM home page window, click **Show Detailed Spread** (in the upper right corner of the Server Overview pane). The Detailed Spread graph opens in a new window (Figure 7-10).

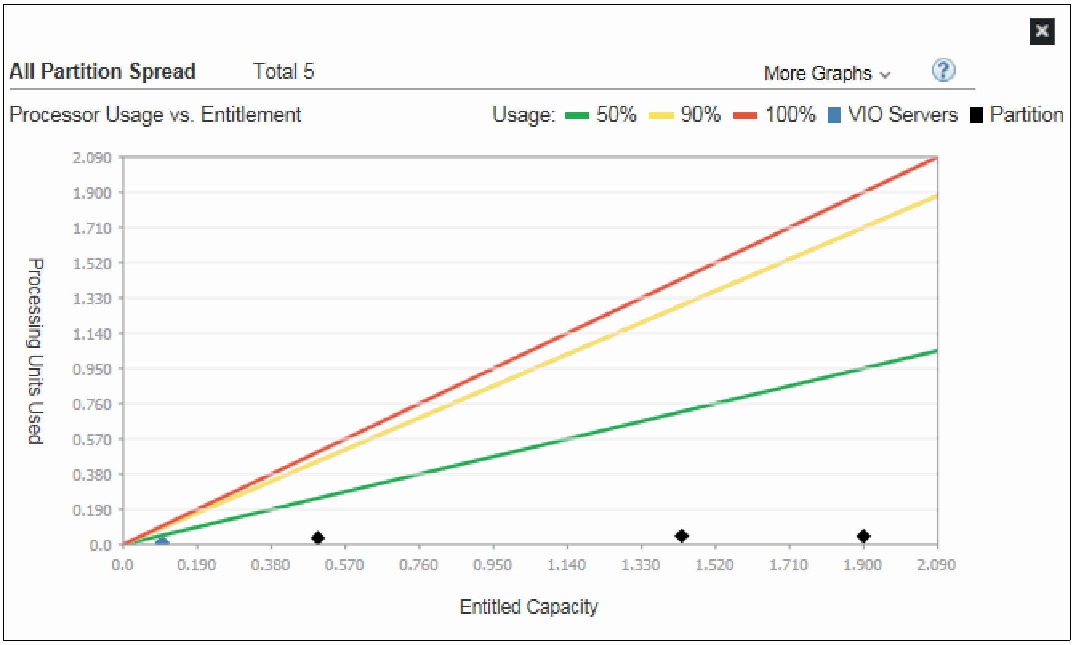


Figure 7-10 Detailed Spread graph

2. Click **More Graphs** to switch between these views: Processor Usage; Entitlement and Memory Usage; Assigned views.
3. Hover the mouse over one of the markers on the graph to display the name of the corresponding partition.

Top Resource Consumers graph

The Top Resource Consumers graph shows up to ten partitions, Virtual I/O Servers, or processor pools that are consuming the highest resources. Each vertical line represents a single partition, Virtual I/O Server, or processor pool. The top of each vertical line shows the maximum number of resource units that are consumed, and the bottom of each line represents the minimum number of resources units that are consumed. The horizontal lines that bisect the vertical lines represent the average number of resource units that can be consumed. The Resource ID appears along the bottom of the graph directly below the vertical line of the partition, Virtual I/O Server, or processor pool that the line represents. By default, the graph displays the client partition that are currently consuming the most processor resources, which are sorted by average utilization. However, you can change the view to display the data only for Virtual I/O Server or storage pools. To change the graphs, complete the following steps:

1. On the PCM home page, click **More Graphs** (in the upper right corner of the Top Resource Consumers graph pane).
2. Click one of the following options:
   - Partitions
   - VIO Servers
   - Processor Pools

   If you select **Partitions** or **VIO Servers**, continue to the next step.
   If you select **Processor Pools**, the graph refreshes and shows the top ten partitions that are using the processor pools.
3. Click one of the following options:
   - Processor
   - Memory
   - Network
   - Storage

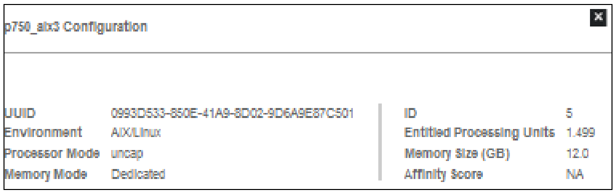
   The graph refreshes and shows the top ten partitions or Virtual I/O Servers that are using the resource that was selected.

Hover your mouse over any horizontal line to see numeric values for minimum, maximum, and average utilization.

> **Note:** If you have fewer than ten partitions or Virtual I/O Servers, the graph shows all of them.

Resource Utilization table

The Resource Utilization table shows the amount of server resources, such as processor or memory, that is used by each partition. You can sort and filter the table. To see more information, click the partition names in the Resource Utilization table. An example of the additional information is shown in Figure 7-11.



p750_aix3 Configuration

UUID	0993D533-850E-41A9-8D02-9D6A9E87C501	ID	5
Environment	AIX/Linux	Entitled Processing Units	1.499
Processor Mode	uncap	Memory Size (GB)	12.0
Memory Mode	Dedicated	Affinity Score	NA

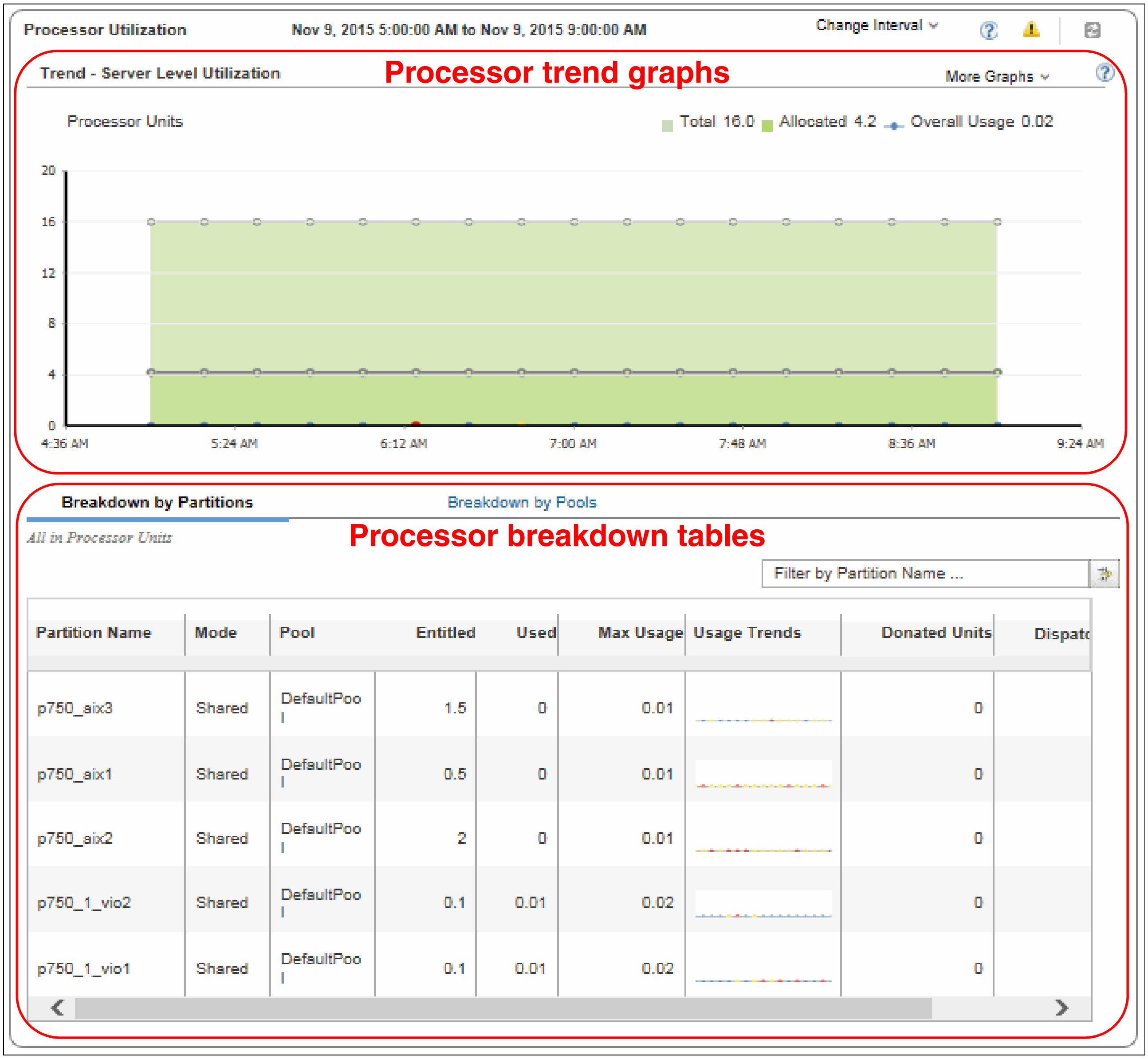
Figure 7-11 Detailed Partitions Information from the Resource Utilization table

7.4.2 Processor Utilization Trend view

The Processor Utilization Trend graphs include historical data and trends that reflect the usage of dedicated or shared processor over time. To access them, click **Processor Utilization Trend** in the Views pane.

The Processor Utilization Trend view (Figure 7-12) contains the following information:

- Processor trend graphs (at the top)
- Processor breakdown tables (at the bottom)



Partition Name	Mode	Pool	Entitled	Used	Max Usage	Usage Trends	Donated Units	Dispatc
p750_aix3	Shared	DefaultPool	1.5	0	0.01		0	
p750_aix1	Shared	DefaultPool	0.5	0	0.01		0	
p750_aix2	Shared	DefaultPool	2	0	0.01		0	
p750_1_vio2	Shared	DefaultPool	0.1	0.01	0.02		0	
p750_1_vio1	Shared	DefaultPool	0.1	0.01	0.02		0	

Figure 7-12 Processor Utilization Trend details view

Processor trend graphs

Two types of graphs are available in the Processor Utilization Trend:

- Sever Level Utilization
- Aggregated Level Utilization

To view these graphs, click **More Graphs** in the upper right of the Processor trend graph pane and click **Server Level Utilization** or click **Aggregated Level Utilization**.

Processor trend graph: Server Level Utilization

The Server Level Utilization graph indicates the number of processors that a server is using at the times that are indicated along the horizontal axis. The lower shaded area represents the total number of activated physical processors on the server, and the upper shaded area indicates how many additional processors are available for activation. The line shows how total processor usage on the server varies over the selected period in comparison with the available processor capacity.

Processor trend graph: Aggregated Level Utilization

The Aggregated Level Utilization graph shows the total number of processors that the server is using. You can see whether processors are being used by the system firmware, Virtual I/O Servers, or client partitions by looking at the shading for each of them.

Processor breakdown tables

The Processor breakdown tables list information that is based on partition or pools over the selected period.

Two breakdown tables are available:

- Breakdown by Partitions
- Breakdown by Pools

Processor breakdown table: Breakdown by Partitions

This table displays the processor utilization data for the logical partitions or Virtual I/O Servers that are associated with the managed system. Mode indicates whether the logical partition is using dedicated processor or resources from the shared processor pool. Pool indicates the shared processor pool that is providing the processor resources (only for logical partitions that are using shared processors).

In addition, you see the number of processors that the logical partition is entitled to use, currently using, and the peak processor utilization over the selected time interval. The Usage Trends column shows the overall usage trend for the logical partition during the specified time interval.

The table lists the total number of partitions for your managed system. The Donated Units column indicates whether the partition is donating unused processor resources to its shared processor pool. The Dispatch Wait Time column indicates the extent to which partitions are waiting to have processor resources made available.

Processor breakdown table: Breakdown by Pools

This table displays the processor utilization within individual processor pools. Entitled indicates the sum of the entitlements for all logical partitions that are using the shared processor pool. Used indicates the sum of average utilization for all logical partitions that are using the processor pool during the selected time interval. You can view the average number of processor units that are borrowed from inactive partitions by using dedicated processors (and possibly from other pools, that have spare processors). Only the default pool (pool 0) can borrow processors. If there are other user-defined pools, they are always represented by using a hyphen (-) in the Borrowed Units column. The Usage Trend column shows a high-level trend view for an individual pool.

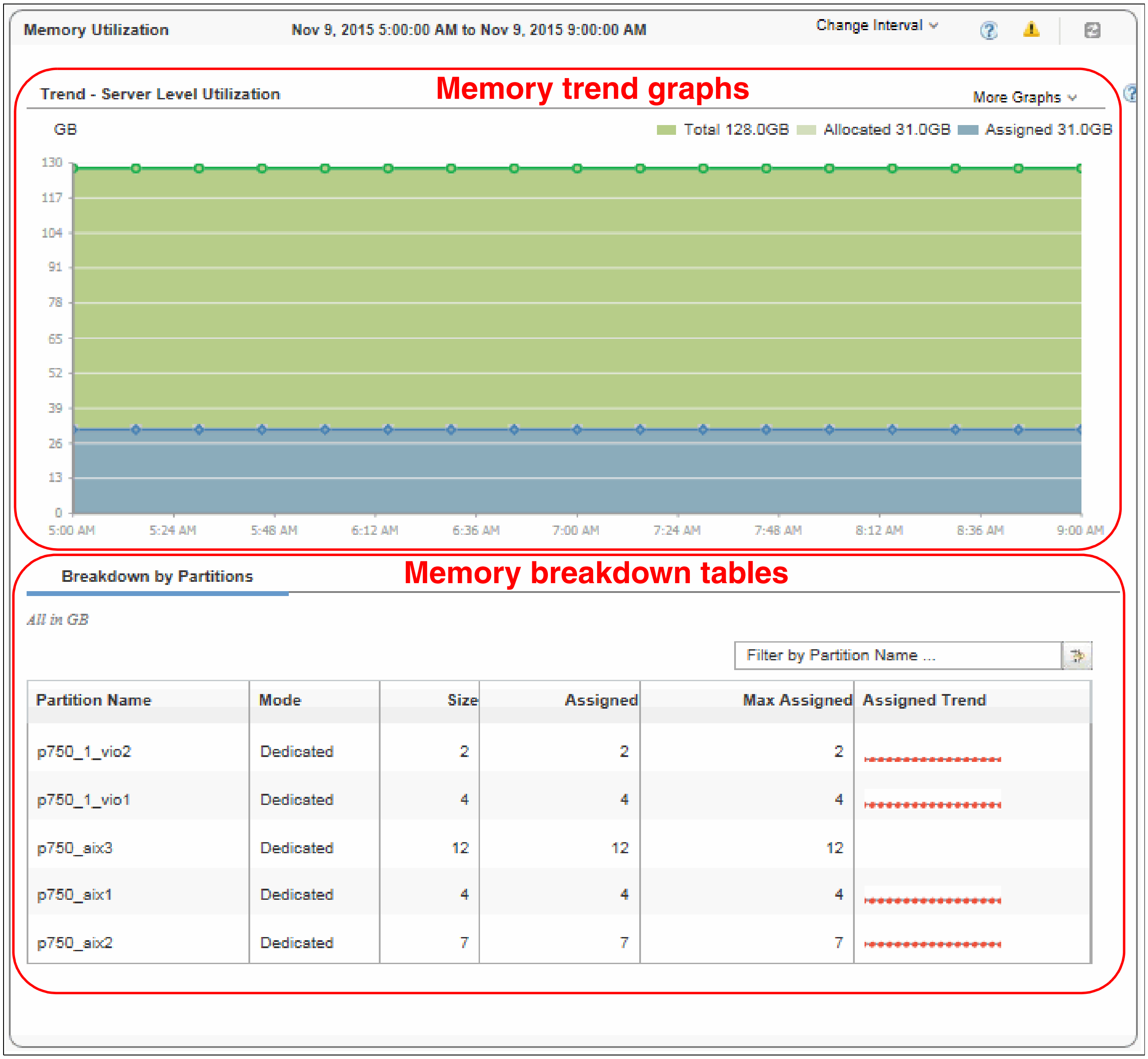
7.4.3 Memory Utilization Trend view

The Memory Utilization Trend graph includes historical data and trends that reflect the amount of dedicated memory that is allocated or shared among logical partitions over time.

To access the Memory Utilization Trend view, click **Memory Utilization Trend** in the Views pane.

The Memory Utilization Trend view contains this information (Figure 7-13):

- Memory trend graphs (at the top)
- Memory breakdown tables (at the bottom)



Partition Name	Mode	Size	Assigned	Max Assigned	Assigned Trend
p750_1_vio2	Dedicated	2	2	2	
p750_1_vio1	Dedicated	4	4	4	
p750_aix3	Dedicated	12	12	12	
p750_aix1	Dedicated	4	4	4	
p750_aix2	Dedicated	7	7	7	

Figure 7-13 Memory Utilization Trend details view

Memory trend graphs

Three kinds of graphs are available in Memory trend graphs:

- Server Level Utilization view
- Aggregated Level Utilization view
- Active Memory Sharing (AMS) Level Utilization view

To view these graphs, click **More Graphs** in the upper right of the Memory trend graphs view and click **Server Level Utilization**, **Aggregated Level Utilization**, or **AMS Level Utilization**.

Memory trend graph: Server Level Utilization

The Server Level Utilization view shows the memory usage for the server. Shaded areas indicate the amount of memory that is assigned to the server, the amount of memory that is allocated for use by the server and the total memory available for use. You can compare the shaded areas to determine whether you maximized the memory allocation for your server.

Memory trend graph: Aggregated Level Utilization

The Aggregated Level Utilization view shows the total memory usage for the partitions on that server. Shaded areas indicate the amount of memory that is allocated to system firmware, the amount of memory that is consumed by all Virtual I/O Servers, and the amount of memory that is used by client partitions. You can compare the trend lines to determine whether you allocated more memory or less memory for the partitions on your server.

Memory trend graph: AMS Level Utilization

The AMS Level Utilization view shows the amount of memory that is consumed from Active Memory Sharing (AMS). The shaded area indicates the amount of memory that is used by the shared memory pool over the selected time interval. you can review this information periodically to determine whether your system benefits from using memory from Active Memory Sharing. If AMS is not configured on the managed system, or the managed system does not support AMS capability, this graph is not available.

Memory breakdown tables

The Breakdown by Partitions table shows the usage of memory by individual partitions during the selected time interval. Mode indicates whether the logical partition is using dedicated memory resources or memory from a shared pool. In addition, you can view the size of the available memory, the assigned memory, and the peak utilization during the selected time interval for that logical partition. The Assigned Trend column shows the overall usage trend for the assigned memory during the specified time interval.

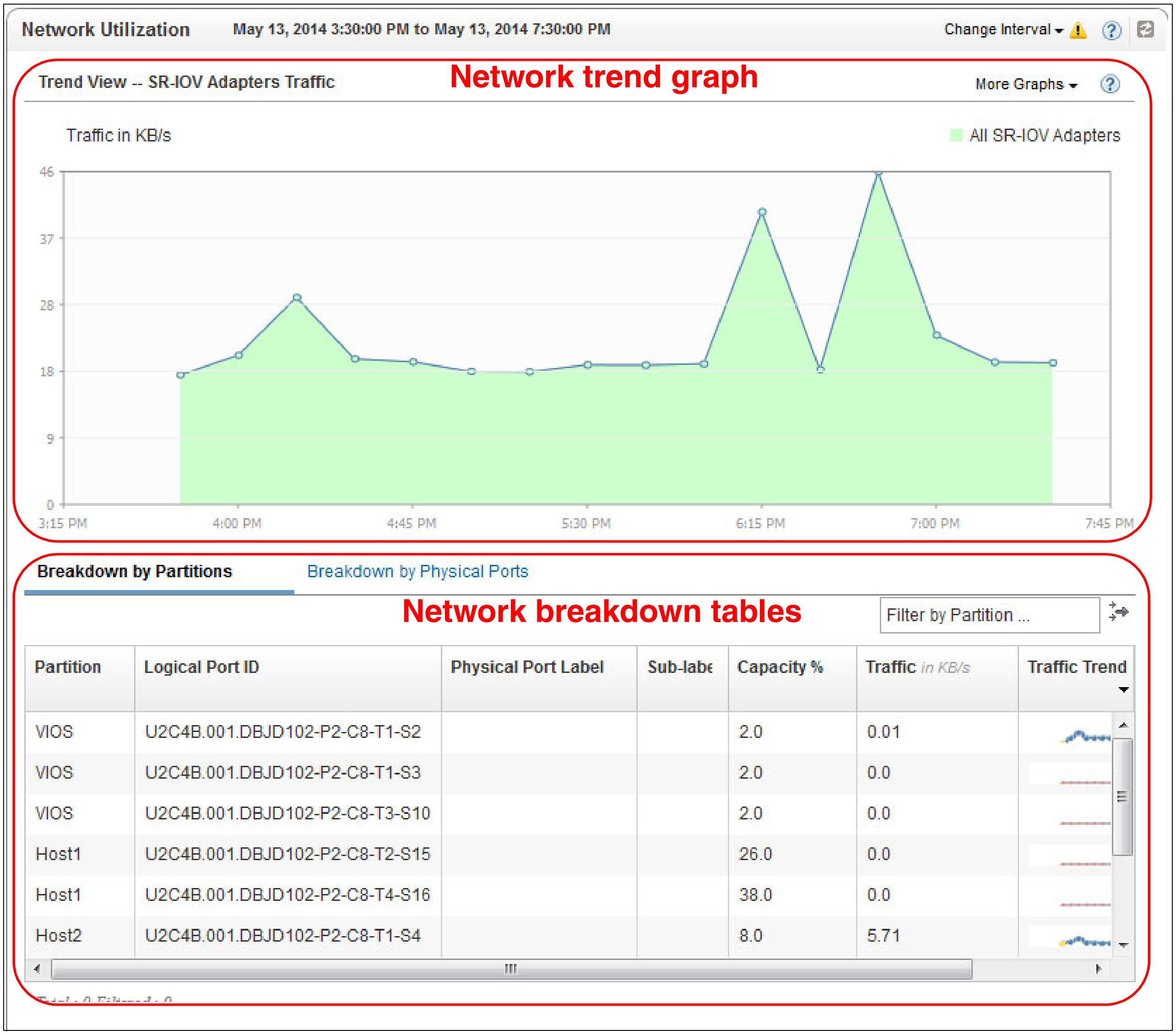
7.4.4 Network Utilization Trend view

The Network Utilization Trend view includes historical data and trends that reflect how logical partitions consume physical network resources or virtual local area network resources over time.

To access the Network Utilization Trend view, click **Network Utilization Trend** in the Views pane.

The Network Utilization Trend view (Figure 7-14) contains the following information:

- Network trend graphs (at the top)
- Network breakdown tables (at the bottom)



Partition	Logical Port ID	Physical Port Label	Sub-labe	Capacity %	Traffic *in KB/s*	Traffic Trend
VIOS	U2C4B.001.DBJD102-P2-C8-T1-S2			2.0	0.01	
VIOS	U2C4B.001.DBJD102-P2-C8-T1-S3			2.0	0.0	
VIOS	U2C4B.001.DBJD102-P2-C8-T3-S10			2.0	0.0	
Host1	U2C4B.001.DBJD102-P2-C8-T2-S15			26.0	0.0	
Host1	U2C4B.001.DBJD102-P2-C8-T4-S16			38.0	0.0	
Host2	U2C4B.001.DBJD102-P2-C8-T1-S4			8.0	5.71	

Total : 0 Filtered : 0

Figure 7-14 Network Utilization Trend details view

Network trend graphs

Two kinds of graphs are available for Network trend graphs:

- Network Bridges Traffic
- SR-IOV Adapters Traffic

To view these graphs, click **More Graphs** in the upper right of Network trend graph and click **Network Bridges Traffic** or **SR-IOV Adapters Traffic**.

Network trend graphs: Network Bridges Traffic

The Network Bridges Traffic view shows the traffic that is flowing over virtual networks at the times that are indicated along the horizontal axis. The shaded areas indicates the amount of internal virtual traffic that is tagged by a Virtual I/O Server and flows over Shared Ethernet Adapters. The dotted line indicates the amount of physical traffic that is routed to a physical

Network Interface Card (NIC) for sharing outside of the virtual network. You can compare the shaded areas to determine how much virtual traffic is flowing across one Virtual I/O Server versus another. Similarly, you can look at the dotted line to compare the amount of physical traffic versus the amount of virtual traffic.

Network trend graphs: SR-IOV Adapter Traffic

The SR-IOV Adapter traffic view shows the traffic that is flowing over the SR-IOV Adapter at the times that are indicated along the horizontal axis.

Network breakdown tables

The Network breakdown tables list information about network traffic over the selected period. Two breakdown tables are available:

- Breakdown by Partitions
- Breakdown by Network Bridges

Network breakdown table: Breakdown by Partitions

This table displays the network traffic data for logical partitions. Network Bridge indicates the virtual network bridge that is used by the logical partition. The table also indicates the number of Virtual I/O Servers that are associated with the logical partition and the amount of virtual and physical traffic that is flowing through the logical partition. The Traffic Trend column shows the overall network traffic for the logical partition over the specified time interval. Click a network bridge ID to display network traffic information, such as the number of packets that are sent, number of packets received, and the rate at which packets were sent or received for the bridge.

Network breakdown table: Breakdown by Network Bridges

This table displays the network traffic for the network bridge. The table indicates the name of the network bridge, the number of logical partitions that are sending traffic across that bridge, the name of the Virtual I/O Server that hosts the network bridge, and the amount of virtual and physical traffic that flows through the bridge. The Traffic Trend column shows the overall network traffic on the network bridge during the specified time interval. Click a network bridge ID to display network traffic information such as the number of packets that are sent, number of packets received, and the speed at which packets were sent or received for the bridge. Click a number that is displayed in the Partitions Using column to see the names of the logical partitions that are using the network bridge.

> **Note:** PCM does not report on network traffic over physical adapter that are dedicated to partitions. A system administrator needs operating system tools to determine physical adapter traffic from each dedicated network adapter’s traffic.

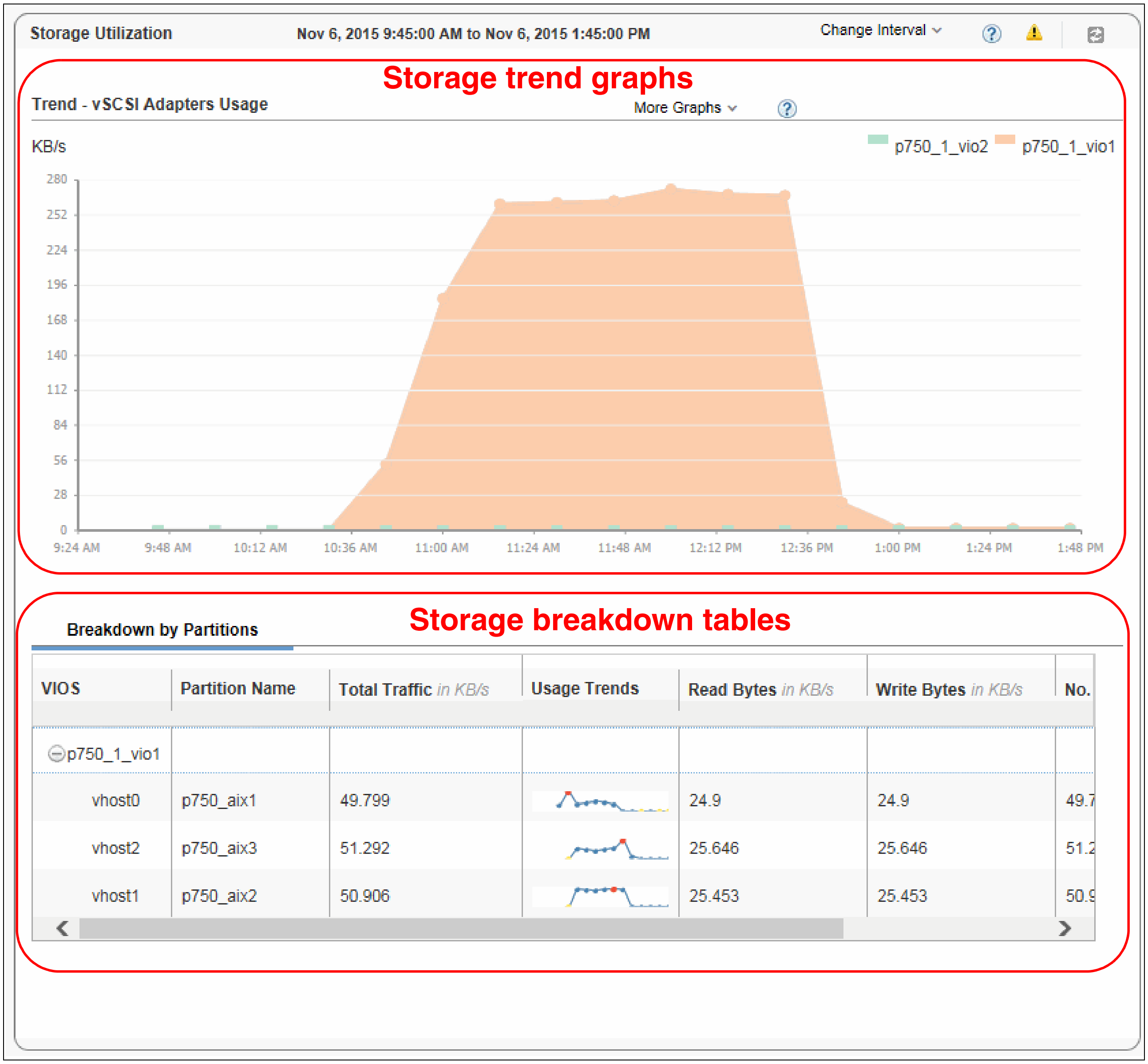
7.4.5 Storage Utilization Trend view

The Storage Utilization Trend view includes historical data and trends that reflect the amount of physical storage each Virtual I/O Server uses and permits logical partitions to consume through virtual Small Computer Interface (vSCSI) connections over time. Storage Utilization Trend also shows the amount of virtualized storage that is provided by a N_Port ID Virtualization (NPIV) adapter to the logical partitions.

To access the Storage Utilization Trend view, click **Storage Utilization Trend** in the Views pane.

The Storage Utilization Trend view contains the following information (Figure 7-15):

- Storage trend graphs (at the top)
- Storage breakdown tables (at the bottom)



VIOS	Partition Name	Total Traffic *in KB/s*	Usage Trends	Read Bytes *in KB/s*	Write Bytes *in KB/s*	No.
⊖p750_1_vio1						
vhost0	p750_aix1	49.799		24.9	24.9	49.7
vhost2	p750_aix3	51.292		25.646	25.646	51.2
vhost1	p750_aix2	50.906		25.453	25.453	50.9

Figure 7-15 Storage Utilization Trend details view

Storage trend graphs

Two kinds of graphs are available in Storage trend graphs:

- vSCSI Adapter Usage
- NPIV Traffic

To view these graphs, click **More Graphs** in the upper right of the Storage trend graph view and click either **vSCSI Adapter Usage** or **NPIV Traffic**.

Storage trend graphs: vSCSI Adapter Usage

The vSCSI Adapter Usage view shows the I/O bandwidth for a Virtual I/O Server that is using physical storage space on SCSI adapter at the times that are indicated along the horizontal axis. Each of the shaded areas represents one Virtual I/O Server. You can compare the shaded areas with one another to determine which Virtual I/O Server is using the most bandwidth, and you can compare individual Virtual I/O Server usage against the total usage.

Storage trend graphs: NPIV Traffic

The NPIV Traffic view shows the I/O bandwidth for a Virtual I/O Server that is using physical storage space through logical ports that are provided by NPIV adapter at the times indicated along the horizontal axis. Each of the shaded areas represents one Virtual I/O Server. You can compare the shaded areas with one another to determine which Virtual I/O Server is using the most storage bandwidth, and you can compare individual Virtual I/O Server usage against the total usage.

Storage breakdown tables

The Storage breakdown tables list information that is based on partitions or physical Fibre Channel (FC) adapters over the selected time period. The following tables are available:

- Breakdown by Partitions
- Breakdown by Physical FC

Storage breakdown table: Breakdown by Partitions

This table shows the storage traffic data for all the Virtual I/O Servers that are associated with the managed system. Physical FC (NPIV) indicates the physical Fibre Channel adapters that are attached to the Virtual I/O Server. The table also indicates the client Fibre Channel adapters, the logical partition name, and the total traffic that is flowing through each Virtual I/O Server. The traffic trend column shows the overall storage traffic for the logical partition during the specified time interval. You can also view the number of bytes or packets that is transferred during the specified time interval.

Storage breakdown table: Breakdown by Physical FC

This table shows the storage traffic for the physical Fibre Channel adapter. The table displays the name of the Virtual I/O Server, the number of logical partitions that are sending traffic by using the Fibre Channel adapter, and the total traffic that flows through the adapter. The Traffic Trend column shows the overall storage traffic during the specified time interval.

> **Note:** Breakdown by Physical FC is available only for the Storage trend graphs NPIV traffic view.

7.5 Troubleshooting

In this section, several troubleshooting topics about PCM are discussed.

Determining whether performance data is being collected

The PCM home page includes a data collection status indication on the home page. If the status is `On`, the PCM function is collecting data from that server. If the status is `Off`, the PCM function is not collecting data from that server. For instructions about collecting data from your system. See 7.2, "Enabling Performance and Capacity Monitor data collection" on page 512.

Permissions to view the managed system utilization data

You must have List Utilization Data access permission for the managed system to view the performance data for that server. For more information about user roles and permissions, see 4.2, "User management" on page 272.

Data not collected for a server event, but data collection is enabled

You can enable data collection for servers that are in any state. However, PCM collects data in the HMC only when the server is in the running or operational state. The PCM automatically disables collection, if the server is not in the running or operational state for 30 minutes or longer.

Home page does not display data, but data collection is enabled

If you access the PCM home page before the initial data is collected the PCM displays a status message. The status message indicates that data is not yet available and recommends that you go to the home page again later. The initial time that is required to collect the information is about 15 minutes.

PCM graphs are not displayed, but Fetching PCM Data message occurs

Clear the cache and cookies from your browser, and then try again.

Home page does not show data for entire length of time selected

The PCM home page can show only the amount of data that the server stored since you enabled data collection. For example if you want to collect data for 250 days and if you immediately access the home page, you can only see the data that represents the minute or minutes passed since you enabled data collection.

In addition, the maximum number of days for which PCM collects data is 366. As a result PCM only shows a maximum of 366 days of data.

Gaps exist in the data that is displayed in the collection graphs

If you disable the data collection an re-enable it, or if the server stopped collecting data because the server stopped, or it is not longer operational, the PCM shows gaps that represents the missing time intervals.

Access to Utilization data after disabling data collection

PCM maintains utilization data after data collection is disabled. You can view the historic data from the PCM home page of your server.

Message says network or storage resources are not available to display

If you dedicate network and storage resources to a single partition on your server, network and storage utilization data is not available. Network an storage utilization data shows how each of the partitions on your server is using network and storage resources that are managed by Virtual I/O Servers. You can compare the data among partitions to determine whether a partition is overloaded or under used. However, if a single partition is entitled to dedicated network and storage resources, there is no data to compare. In addition, you can also check whether you have the required Virtual I/O Server version and firmware. The PCM Monitor requires Virtual I/O Server Version 2.2.3 or later, and a firmware version of 780 or later to display the network and storage data.

Only single partition or VIOS is listed in Top Resource Consumers graph

The Top Resource Consumers graph displays up to ten partitions or Virtual I/O Servers that are using the highest number of units of the resource you chose. However, if you dedicated all of your resources to a single partition or Virtual I/O Server, no other partitions or server can compete for the resources. As a result, only the partition or Virtual I/O Server for which you dedicated all resources is displayed in the Top Resource Consumers graph.

8

Good practices

This chapter provides useful information, suggestions, and good practices for managing the Hardware Management Console (HMC). It includes suggestions on planning for an HMC, initial configurations, security, problem determination, and code installation and maintenance.

This chapter describes the following topics:

- Planning
- Initial configuration
- Security
- Problem determination
- Maintaining Licensed Internal Code
- Maintaining system firmware

8.1 Planning

Planning should be done for any major change in any computing environment, including adding new servers, performing upgrades and implementing software changes. Careful planning involves creating a time line and dividing the project in phases, each with a specific, stated outcome. In effective planning, you draw up a list of assignments and responsibilities, and also document the current environment and the desired result.

To plan for the HMC, begin with some fairly simple questions:

- Is an HMC needed?
- What models are available?
- Where are they set up?
- How do they connect to servers they manage?
- How are they maintained and by whom?
- Where can I find documentation?

8.1.1 Do I need an HMC

Midrange and enterprise Power Servers need an HMC to create and manage logical partitions, dynamically reallocate resources, invoke Capacity on Demand (CoD), utilize Service Focal Point and facilitate hardware control. Two HMCs are suggested for enhanced availability (see 2.8.1, “Dual HMC and redundancy” on page 149). Mission-critical solutions, even those hosted on entry or midrange Power Servers, might benefit for having dual HMCs.

HMCs might not be cost-effective for distributed, entry-level systems that nevertheless require the capabilities of Advanced Power Virtualization. Entry-level servers without an HMC can be configured with a hosting partition called the IBM Integrated Virtualization Manager (IVM). It provides a subset of HMC functions and a single point of control for small system virtualization. IVM does not offer the full range of management capabilities found on an HMC, but it might be sufficient for a small server with one to eight processors.

Another solution might be the vHMC, with which you can run an HMC in a virtualized environment somewhere else in your environment, if you have spare resources available. For further information, see 3.2, “Virtual appliances installations” on page 185.

8.1.2 HMC models

The available hardware models for the HMC are described in 1.3, “Hardware Models” on page 40. The number of servers each HMC can manage varies by server size and complexity. The HMC performance can vary depending on the unique combination of servers and the number of partitions and I/O drawers implemented.

8.1.3 Physical location of an HMC

Locate an HMC close to the servers it manages, nominally 50 feet (15.24 meters). For remote administration, this is normally not necessary, but for service personnel using the HMC and its service applications to maintain systems and record service actions, it is necessary, however, in order to enable them to go back and forth between an HMC and a managed server during a service call.

8.1.4 Planning for network connectivity

Two types of networks are possible for an HMC:

- An *open* network

  An open network is the easiest to describe. It means any standard network connection, such as might be used to connect an HMC and a logical partition, or an HMC and a remote workstation.

- A *private* network

  The private network is a non-routable subnet. It is sometimes referred to as a *service network*. In the context of the HMC, a single HMC will nearly always be the DHCP server for a private network.

A server with dual HMCs would be connected to two private networks with each HMC acting as a DHCP server on a unique, non-routable subnet (see 2.8.1, “Dual HMC and redundancy” on page 149).

To attach multiple managed systems to one or a pair of HMCs, network switches might be required. If you are planning to implement private networks over a switch that supports virtual local area network (VLAN) technology, be sure that a broadcast from the service processor will reach the HMC DHCP server quickly before the service processor port goes to its default IP address. For example, if the switch port must have spanning tree enabled, it should also have PortFast or the equivalent enabled.

As an additional step, determine whether the switch requires that the network interface on the HMC be set to a specific speed or whether auto-detect may be used. Hubs generally require the HMC to be set to a specific speed and duplex setting.

8.1.5 Private versus open

The network connection between the HMC and the service processor can be either private or open. Private is preferred, and therefore a good practice.

On a private network, the HMC acts as a DHCP server for the managed system service processors. The IP address is assigned from a range of non-routable addresses selected by you when you configure DHCP on the HMC. The non-routable subnets isolate the HMC and the service processors from other HMC network interfaces.

An HMC can also manage service processors over an open network on low-end and mid-range systems. This scenario requires that the service processors be network reachable from the HMC. All HMC-to-service-processor communication is SSL-encrypted, whether over a private or open network.

In an open configuration, the service processor IP addresses must be set manually on each managed server. They cannot be DHCP clients of any server other than a managing HMC.

Addresses can be set by using the Advanced System Management Interface (ASMI) on the service processor. This involves directly connecting a notebook to one of the ports on the service processor using HTTPs to log into one of the two predefined IP addresses (see 6.10.2, “Connecting to ASMI” on page 472). If no notebook is available, an ASCII terminal can be used on the native serial port to access the FSP (service processor) menus in character mode.

Open networks are used for communications between a logical partition and the HMC. This connection is largely to facilitate traffic over the Resource Monitoring and Control (RMC) subsystem, which is the backbone of Service Focal Point (SFP) and required for dynamic resource allocation. The open network also is the means by which remote workstations might access the HMC, and it might be the path by which an HMC communicates with IBM Service through an Internet connection.

Regardless of which type of network is involved, you must provide your own networking infrastructure, such as cables, switches, or hubs. Switches that support virtual networks (VLAN) may be used to create one or more private or open networks as conditions require.

8.1.6 Customer setup

The HMC is a customer setup machine. Contracts for support can be purchased for one-year and three-year periods. Hardware service contracts for on-site hardware support are available beyond the initial warranty period.

Customers are responsible for installing and updating the Licensed Machine Code on all HMC and managed servers. An update strategy is discussed later. Systems administrators should become familiar with the information and tools available on the Fix Central website:

`http://www.ibm.com/support/fixcentral/`

As a system administrator, consider signing up for subscription service at the Fix Central website. With a subscription you will receive email notification of new releases of software and firmware.

8.1.7 Documentation

Documentation of the IBM Power Servers and the HMC is available through the IBM Knowledge Center:

`http://www.ibm.com/support/knowledgecenter/POWER8/p8hdx/POWER8welcome.htm`

The Knowledge Center enables you to print documents or portions of them, and also bookmark pages for easy reference in the future.

Carefully consider the interdependencies between HMC code levels and system firmware on Power servers. These relationships can be found on the firmware support web pages. Be sure you understand that new system firmware might require an upgrade of the HMC code. Because upgrading the HMC does not disrupt partition operations, and because dual or redundant HMCs are supported, keeping HMC code on the most current level is a preferred practice. The general rule is that the HMC must support the highest level of system firmware on any server that it manages.

8.2 Initial configuration

The HMC includes preinstalled licensed machine code, but you might need to reinstall if the code is superseded or your have a disk failure. Customized setup and installation instructions are included with all new machines or upgrades. Before you receive a new system, review the IBM Knowledge Center to determine what specific preparations might be needed:

`http://www.ibm.com/support/knowledgecenter/POWER8/p8hdx/POWER8welcome.htm`

8.2.1 Install and configure the HMC first

If you will be using a private network, install and configure your HMC *before* connecting it to a network or powering on the servers the HMC will manage. This approach enables you to configure the networks properly, start DHCP in an orderly manner, and ensure that the managed servers will connect properly.

The HMC includes a setup wizard (see 3.3, “HMC Install Wizard” on page 223) that can be used by a systems administrator to customize the system. The wizard starts the first time you log in after a new installation. You are not required to use it. Administrators who are comfortable with the HMC Configuration menus may use them instead. The setup wizard can be run at any time from the main menu on the HMC console (see 5.2.1, “Console Settings” on page 310).

8.2.2 Changing passwords

Whether you use the setup wizard or the HMC Configurations menu, the first task you should do is change the `hscroot` and `root` passwords from their defaults (see “Predefined user IDs and passwords” on page 3). Logging in as root is disabled. It can be enabled with assistance from IBM support when performing problem determination. Be sure to save all passwords in a secure location where they can be retrieved in an emergency.

8.2.3 Creating user IDs

Create additional user IDs on the HMC so that not every user is accessing the system with the same user ID and password, and not necessarily with the same level of authority.

Administrators with `hmcsuperadmin` authority, which is what hscroot has, should have their own user IDs and passwords. This will facilitate auditing administrative actions on the HMC. Other users may have other predefined roles with more restricted authority.

A special, optional user ID, `hscpe`, can be created initially or when needed. This is the user ID needed to gain root access to the HMC. The hscpe user can enter a password obtained from IBM that allows this user to run the **`pesh`** command to override the restricted shell and switch-user to root. This also requires that the user knows the root password. The password used to override the restricted shell is good for one day and must be obtained by contacting IBM Support and providing the HMC’s serial number.

8.2.4 Configuring the call-home capability

For many years, IBM has offered a *call-home* capability. This feature is the ability to automatically notify IBM Service in the event of a hardware problem, and also the ability to transmit other service related or vital product data as required.

On the HMC, the setup wizard prompts for the necessary information to configure *call-home* (see 6.4, “Connectivity” on page 434). You can also use the HMC menus for configuring customer information and customizing outbound and inbound communications for call-home. If customer information is not configured correctly, the HMC will not be able to “call home” for support.

Note: Inbound communication is optional. When allowed, you have real-time control over the inbound session, and it can be terminated any time.

The inbound and outbound communications are secured by SSL and you can use an SSL-Proxy that allows you to use Network Address Translation (NAT) firewalls between an HMC and IBM Support. In this way, the HMC's true IP address can be hidden behind a corporate firewall and encrypted information can be sent to IBM.

8.2.5 Configure customer notification

During initial configuration, you can decide how events should be called to your attention.

Customer notifications can be configured to send email to customer accounts when service events are generated. The emails can be send to distribution lists. Most customers will want to use the filters to ensure that only serviceable events are sent using email, and not every message generated by the HMC. Optionally, SNMP traps may also be configured to send notifications to specific IP addresses when an event occurs, This can be used in conjunction with a network or system monitoring program.

8.3 Security

Physical security of the HMC is a customer responsibility. The HMC should be located in a secure room, if possible. Usually, because of its proximity to the servers it manages, the HMC will be located in a secured data center. However, when that is not possible, there are ways of providing additional protection against unauthorized physical access. These protections are mainly provided by changes in the BIOS settings on the chip that powers the HMC:

- Change the startup device settings in BIOS to prevent the use of a recovery DVD to boot into single-user mode.
- Assign a power-on password in BIOS to prevent unauthorized changes to BIOS settings.
- Unattended start mode can be set in BIOS to allow the HMC to reboot without the power-on password following restoration of power after an unplanned outage. However, the keyboard and mouse at the local console will remain locked until the power-on password is entered.

8.3.1 Network security

The HMC must be properly networked to perform its server management functions. The private or service network is used to communicate with service processors, and the open network is used to collect serviceable events from managed systems and to dynamically reallocate resources. A network is also the means by which remote administrators access and manage the HMC itself.

The HMC enables a firewall to block all incoming network traffic, with the exception of a well-known set of ports, which are listed in Table 8-1 on page 541. Within these well-known ports, further access restrictions can be customized based on IP address or host name.

Table 8-1 HMC port information

Port	Protocol	Application	Enabled by default	Notes
22	TCP	ssh	No	
443, 12443, 9960	TCP	https	Yes	
5989	TCP	Open Pegasus	No	Open source CIM
657	TCP/UDP	RMC	Yes	
9920	TCP	FCS	Yes	Call home
9900	UDP	FCS	Yes	Call home
2300, 2301	TCP	5250 console	Yes	
n/a	ICMP	ping	Yes	
123	UDP	NTP	No	
427	UDP	SLP	Yes	Used in cluster
12347, 12348	UDP	RSCT Peer Domain	Yes	
162	TCP/UDP	SNMP traps	No	
161	TCP/UDP	SNMP Agent	No	
2049	TCP	NFS	No	
69	TCP	TFTP	No	
500, 4500	UDP	IPSec	No	VPN

The firewall interface allows you to customize remote access to the HMC by IP address and network mask. For further information, see “LAN Adapters Details - Firewall Settings” on page 265.

8.3.2 Network access between HMC and service processor

The HMC communicates with the service processor to perform its management functions. To do this, it establishes a Secure Sockets Layer (SSL) connection with port 30000 and 30001 of the service processor’s Ethernet port. Be sure that the network used for this communication channel is private, although an open network is supported.

8.3.3 Restricted shell on the HMC

The HMC provides a rich set of commands that encompasses most of the tasks found in the graphical user interface. These can be accessed by SSH. However, by itself, SSH can provide to an authenticated user full access to the shell. To protect the HMC from users trying to gain higher privileges by some means of exploiting the system, there is a restricted shell enforced when remotely connecting the HMC using SSH or when opening a local terminal on the HMC console. In the restricted shell environment, users will only have access to a small subset of operating system commands, along with the HMC commands. Users will not be able to use the `cd` command, and cannot use redirection.

For more information about the command line, see 5.1.2, “Command-line interface (CLI)” on page 307.

8.3.4 Auditing capabilities of the HMC

A secure system also requires strong auditing capabilities. This section describes some of the logging and auditing functions on the HMC.

Most tasks performed on the HMC (either locally or remotely) are logged by the HMC in the `iqqylog.log` file. These entries can be viewed by using the Console Events Log task, under **Serviceability** → **Console Events Log** or by using the **`lssvcevents`** command from the restricted shell. A log entry contains the time stamp, the user name, and the task being performed. When a user logs in to the HMC locally or from a remote client, entries are also recorded. For remote login, the client host name or IP address is also captured, as in the following example:

```
lssvcevents -t console

time=11/11/2015 09:52:55,"text=User hscroot has logged on from location
172.16.254.10 to session id 32.  The user's maximum role is ""hmcsuperadmin""."
```

Standard log entries from `syslogd` can be also seen on the HMC by viewing the `/var/hsc/log/secure` file. This file can be read by users with the `hmcsuperadmin` role. It is under `logrotate` control. A valid user can simply use the **`cat`** or **`tail`** command to view the file. A user with the `hmcsuperadmin` role can also use the **`scp`** command to securely copy the file to another system.

If you want to copy `syslogd` entries to a remote system, you may use the **`chhmc`** command to change the `/etc/syslog.conf` file on the HMC to specify a system to which to copy. For example, the following command line causes the syslog entries to be sent to the `myremotesys.company.com` host name:

```
chhmc -c syslog -s add -h myremotesys.company.com
```

The systems administrator must be sure that the syslogd daemon running on the target system is set up to receive messages from the network. On most Linux systems, this can be done by adding the `-r` option to the `SYSLOGD_OPTIONS` in `/etc/sysconfig/syslog` file.

In AIX, edit the `/etc/syslog.conf` file by uncommenting the appropriate lines at the bottom of the file, such as these:

```
*.debug /tmp/syslog.out rotate size 100k files 4
*.crit /dev/console
```

Then, as a systems administrator, you enter the following lines:

```
# touch /tmp/syslog.out
# refresh -s syslogd
```

8.3.5 Managing and understanding security vulnerabilities on the HMC

As stated in 8.5.5, “Updates” on page 548, HMC users can subscribe to email notification of corrective service at the Fix Central website:

http://www.ibm.com/support/fixcentral/

Whenever a vulnerability is discovered on the HMC, a bulletin describing how to obtain the fix will be sent to users. In most cases, because of the closed nature of the HMC and the presence of the restricted shell, some vulnerabilities found on non-HMC systems will not apply. Each time a new release of the HMC code is made available on the support website, a list of security fixes included in the release is also published.

8.3.6 Resource Monitoring and Control (RMC)

The RMC is based on IBM Reliable Scalable Cluster Technology (RSCT). It is installed and used on the HMC for establishing a trusted communication channel between the HMC and the partitions on the managed server. The following examples describe tasks performed through this channel:

- Dynamic allocation of hardware resources on the partitions
- Graceful shutdown of the AIX operating systems running on the partitions
- Sending hardware error log entries from the AIX partitions to the HMC to provide a single focal point for error collection

RMC uses port 657 for HMC-to-partition communications. RMC employs access control lists to authenticate communication between the partitions and the HMC. The authentication is established during configuration steps on the HMC, thus, when transmitting messages over port 657, the HMC and the partition can be sure with whom they are communicating.

8.4 Problem determination

This section covers issues and problems that might be encountered during operation of the HMC itself. Although some mention is made of managed systems in the context of server and frame management, service applications, such as Electronic Service Agent or Service Focal Point, are not discussed.

8.4.1 Problem analysis

The HMC is composed of many subsystems and layers to its code stack. Every subsystem maintains a dynamic trace. The vital traces are stored in persistent files in the HMC file system. At periodic intervals, typically every hour, cron jobs are run, depending on the process, for those subsystems or applications that tend to generate heavier quantities of trace data. This cron job checks the respective trace files size to see if it has exceeded a fixed, static threshold. If the file does exceed this threshold, the trace file is backed up and a new trace file's generation begins. Also, when the HMC is rebooted, the last running trace file for some subsystems will be backed up; for others it will be overwritten.

Typically up to eight backup copies are maintained at any given time. Although this might seem sufficient, the size of the trace files and number of backups maintained depend upon the HMC load. For example, in an environment where an HMC is managing two frames and 40 logical partitions, the amount of trace data generated can be voluminous over a short period. If IBM Support will be needed to diagnose an HMC problem, the trace files must be extracted from the HMC as soon as possible after the problem has been observed.

The HMC provides a **pedbg** command to assist in this process. This command can be run only as user `hscpe` with the `hmcpe` task role. Consult the man page for the full list of options this command provides. For further instruction about using it, see Appendix C, "IBM product engineering debug data collection" on page 575.

Although **pedbg** should suffice for enabling trace collection, situations can arise where having support gain root-level access on the HMC will be helpful. The HMC provides the **pesh** command to escape temporarily from the restricted shell. This command may be run only by user `hscpe` with task role `hmcpe`. This command accepts one parameter, the HMC serial number, which can be obtained by issuing the **lshmc -v** command. You are prompted for a password, which you must obtain from IBM support.

This password is valid until the end of the calendar day on which it was issued. Hence, a password obtained at 11:00 PM will expire one hour later, at midnight. When accepted, the password will give full shell access.

> **Note:** Although the password will expire at the end of the calendar day, after you are logged in as user `root`, you may remain logged in indefinitely. However, staying logged in indefinitely is not recommended because it can be a security exposure. Be sure that this user ID is deleted after use and re-created, temporarily, as needed.

For instructions of how to gather analysis data of Live Partition Mobility (LPM), see Appendix D, “Live Partition Mobility support log collection” on page 581.

8.4.2 Problem logging and tracking

More detailed information about either information or error messages received during command execution can be obtained by using the **`showLog`** command. This command can be run in a Terminal in the HMC console by a user who has become root (to become `root`, follow the previous steps for obtaining a password to run in conjunction with the `hscpe` task role and the **`pesh`** command).

Any user, except users with the `hmcviewer` task role, can view system event information included in the console logs on the GUI by selecting **Serviceability** → **Console Events Log**. This task will display system events logged during HMC operation, enumeration HMC activity in response to user-initiated tasks, whether the command succeeded or failed. This will not display all entries in the HMC Console logs, but a subset of them. This task can also be executed on the command line by using the **`lssvcevents`** command with the **`-t console`** flag.

8.4.3 Problem correction

As mentioned previously, all HMC tasks (user-initiated and otherwise) require interactions between various subsystems on the HMC. Failures in one or more subsystems might occur, and a useful tactic is to isolate the failures if possible. For example, usually when a task fails it is a good idea to try another way to perform the same operation. Assume a task cannot be performed from the GUI; it was initiated but the GUI is not working. Typically, this means the panels is displayed but not available for use, especially after minimizing and maximizing the window. Check whether it can be done through the command line. If both ways do not work, the back end is likely to be the culprit.

Therefore, consider some possible scenarios in HMC system management. A common source of curiosity is HMC performance. Performance can suffer if trace and log files fill the HMC file system. Disk space usage can be checked with the following command:

```
monhmc -r disk
```

If any file system partition is in 100% use, issue the **`chhmcfs`** command, to free the space in the HMC file systems (see the man page for options).

The managed systems and frames can be in one of many states, as reported by the HMC. Among the states that cause confusion are these:

- No Connection

  The HMC cannot build a valid connection to the service processor or BPC. The reason will be displayed as an error code on the GUI. If you believe that this state was reached in error, you can reset the network connection between the HMC and service processor by using one of the following procedures:

  - Right-click on the managed system to open the pop-up menu (or select the managed system). Select **Action**s → **Reset or Remove System Connection** on the HMC Console.

    You must have the `hmcsuperadmin`, `hmcoperator`, or `hmcpe` task role to perform this operation.

  - Use the **`rmsysconn`** command (on the command line) with **`-o reset`** flag.

- Incomplete

  The HMC is unable to gather all system information from the managed system or frame. In some cases this might be because of a network error causing a temporary disruption to HMC and service processor interactions, or managed system hardware configuration changes being performed for a redundant HMC. To verify, an attempt can be made to recover from this state by using either of the following procedures:

  - Select the **Rebuild System** GUI task.
  - Issue the **`chsysstate`** command with **`-o rebuild - r sys`** flags on the command line.

  Neither procedure can be performed by the `hmcviewer` task role. If the state does not change, try resetting the HMC-service processor connection (see the previous bullet, No Connection), then try rebooting the HMC if resetting does not help. If the problem still persists, gather trace files and logs for support.

- Recovery

  The save area of the service processor, where partition profile and some partition information is kept, might be corrupted, cleared, or out-of-sync with the cached copy the HMC maintains in its file system. First, whether the managed system has been updated recently would be good to know; firmware updates can clear Non Volatile Random Access Memory (NVRAM). If no system update has been performed recently, you can perform either of the following procedures:

  - Restore the save area with the cached copy on the HMC; use the GUI or the CLI:
    - **Manage Partition Data - Restore** task from the GUI
    - **`chsysstate - o recover -r sys`** command from the CLI
  - *Clear all partition configuration information*; use the GUI or the CLI:
    - **Manage Partition Data - Initialize** task from the GUI
    - **`rstprofdata -l 4`** command from the CLI

    Do not use this procedure unless you are willing to rebuild the partitions from scratch.

  If neither approach works, gather trace files and logs.

A problem more severe than No Connection is the situation where no systems or frames appear where they had appeared before. Although many reasons exist for those, one common scenario observed is when a managed system or frame is removed from the HMC. This might have happened through the Remove Connection task or **`rmsysconn`** in the CLI.

When this system is then added back into the HMC's management domain, the HMC (as DHCP server) will not redetect it. If you remove a managed system, and have reason to believe this HMC might again manage in the future, run the **`mksysconn -o auto`** command to purge the HMC of its management history and allow it once again to provide IP addresses to the managed server.

Another observed problem has been the GUI is not reflecting the true managed system or frame status or configuration. The CLI can be used to see if it gives up-to-date information. If it does, that means the GUI has either stopped receiving indication data, or no indications are being propagated to it. A Reload (F5) operation can refresh the GUI in this situation. If the command line is also incorrect, the HMC has stopped receiving event notifications from the managed system or frame. To recover from this situation, perform the **Rebuild System** task.

The service processor provides the HMC with the capability to set locks on the platform. The service processor does not interpret the locks, but rather leaves it up to the HMC functions to do that. These locks are used for synchronization of operations from one or two (dual) HMCs. In a dual HMC environment, situations can arise where both HMCs perform tasks against the same managed system and require the same lock.

When HMC 2 needs to perform a task that requires a lock that HMC 1 is currently holding, HMC 2 will wait and retry to acquire the lock. If after a few attempts it is unsuccessful, the operation will fail and the user will be notified accordingly. Although this blocked state is often mistaken for a "hang," that is not the case. However, a possibility is for HMC 1 to acquire a lock and fail to release it. If this happens, HMC 2 can be used to disconnect HMC 1. When an HMC is disconnected, all locks owned by the HMC are reset. To do this, any `hmcsuperadmin` user can run the Disconnect Another HMC GUI task on HMC 2 against HMC 1. This can be done only from the GUI. No corresponding command-line version of this task exists.

8.5 Maintaining Licensed Internal Code

Make sure you keep track of new releases, updates and emergency fixes to HMC code. You can do this in one of two ways:

- Sign up for the technical support subscription service to receive emails when updates become available on the web.
- Monitor the Fix Central website, manually, on a regular basis:

  `http://www.ibm.com/support/fixcentral/`

Read through the website carefully. Select the appropriate Power platform, whichever is appropriate for you. Many additional resources are on the site, such as links or extra technical information, hints and tips, and the latest command-line specifications, where you find new commands that may have been added.

You can order recovery DVDs or download packages that contain the files needed to burn your own recovery DVD, the files used to create DVDs have an `.iso` file extension. The DVDs created from these packages are bootable. You can download updates to HMC code and also emergency fixes, and you can order DVDs containing the updates and fixes. The DVDs containing updates and fixes are *not* bootable.

8.5.1 Management Console Data backups

An important task is to maintain a current backup of the Management Console Data (see 5.3.6, “Backup Management Console Data” on page 321) to use in recovering the HMC after the loss of a disk drive. Whenever you go to a new version level of HMC code, or use a recovery DVD to update the HMC, be sure to create a new backup immediately following the installation. If you update HMC code between releases using the Corrective Service files that are downloadable from the web, and then create a new backup of the Management Console Data after the update, you can use this backup and the last-used recovery DVD to rebuild the HMC to the level in use when the disk was lost.

Another example where a Management Console Data backup can be useful is when replacing an service processor or BPC server. Create a fresh backup before starting the replacement in order to preserve the DHCP lease file on the HMC that lists the starting service processor and BPC IP addresses. If for some reason things do not work after replacing the service processor or BPC, this backup can be used to restore the original information so you can return to the original service processor and BPC. If the replacement is successful, a new IP address will be assigned to the new component and the lease file will be updated. At this point, a new backup should be created capturing that freshly updated DHCP lease file.

8.5.2 HMC code installation, upgrade, or update overview

When HMC systems leave manufacturing, they are preinstalled with the most recent level of code. However, there might be a time when reinstallation is needed. The HMC can be installed using DVD media, or installed over the network by using a server that accepts Preboot Execution Environment (PXE) requests.

8.5.3 Install and recovery

Installation is the simplest form of applying code on the HMC. It is used by manufacturing to install code prior to shipping the HMC. When the HMC is at the customer locations, an installation should be needed only for disaster recovery or when the customer wants to reload the HMC from scratch. In disaster recovery, a systems administrator can use an appropriate recovery DVD and the Management Console Data backup to get the HMC back to the state it was in prior to the failure. An old Management Console Data backup should not be used after upgrading to a newer version or release of an HMC. A new Management Console Data backup should be created as mentioned previously.

8.5.4 Upgrade

Be sure you can distinguish between updating and upgrading a system, The terms are not synonymous. To *upgrade* is to bring the system to a higher version or release of HMC code. When the HMC’s version number is incremented, such as going from Version 7 to Version 8, the upgrade method must be used in order to apply the new version of HMC code. Prior to an upgrade the systems administrator should perform a Save Upgrade Data (see 5.3.8, “Save Upgrade Data” on page 323) to preserve configuration information on the HMC, like network settings, user data and partition profiles. This data is saved in a special location on the HMCs hard disk that will not be erased during the upgrade process. When the upgrade process completes, the data will be restored to the HMCs file system.

Only perform a Save Upgrade Data when you are upgrading an HMC. Do not use it when performing service work on a Power server. If you are planning to service or replace an service processor on a Power server, do a Management Console Data task backup first.

8.5.5 Updates

Between HMC releases, or between upgrades, interim fixes or cumulative service packs might need to be applied. These are types of updates. Interim fixes consist of security fixes that are considered critical to be released immediately to customers. Service packs are generally larger in content. Both can be installed on the HMC by using the Update the Hardware Management Console task (see 5.3.4, “Update the Hardware Management Console” on page 320), or by using the **updhmc** command on the HMC.

The HMC uses Version, Release, and Maintenance (VRM) nomenclature to describe operating system releases. The HMC version and release information can be viewed with the **About** function (see “Getting Started with Hardware Management Console (HMC) window” on page 296). From the command line, you can get the current code level by issuing the **lshmc -V** command.

Every version of HMC code is made available on bootable recovery media. Within a version, releases are available as either recovery DVD or downloadable corrective service files.

Corrective service is a cumulative maintenance release within a single version that customers can use to update the HMC from any previous releases within the same version. For example, a customer who is currently at Version 8 Release 1 or Version 8 Release 3 can update to Version 8 Release 4 using the same corrective service.

Corrective service is not provided whenever the version number is incremented, for example from Version 7 to Version 8. If this happens, only Recover media may be used to perform the upgrade.

Corrective services is relatively easy to apply by using the Update the Hardware Management Console task on the HMC console or by running the **updhmc** command. As successive corrective service updates are installed, the size of the Critical Console Data increases. The Backup Management Console Data task backs up both data and binary changes on the HMC. Over time, this can mean that the size of the backup will be quite large. To shrink the size of the backup, update with Recovery media after performing a Save Upgrade Data task. The latter step only saves needed user and configuration data. After the update, a new Management Console Data backup can be made, and it will be smaller.

Interim fixes or service packs are also treated as corrective service, and they are installed in the same manner as described previously. The difference is primarily the size and how they are shown to users. Customers will see a Program Temporary Fix (PTF) value associated with the interim fix or service pack when using a command such as `lshmc -V`, for example:

```
MH01453: Maintenance Package for V8R8.2 (11-14-2014)
```

8.5.6 HMC code update on multiple machines

Some clients have a large number of HMCs. Updating code on a large number of machines can be time-consuming, especially if manual intervention or physical access to the local HMC is needed. Fortunately, methods are available to overcome this problem.

Remote command

There is a rich set of commands on the HMC. These commands are available locally and also remotely using SSH, which allows a remote workstation installed with SSH client software to remotely execute commands on the HMC. The **updhmc** command is such a command that allows interim fixes, service packs, and cumulative maintenance releases to be remotely installed on the HMC. The following example illustrates a scenario where an HMC code update is performed simultaneously on multiple machines from a remote workstation.

From the remote system installed with SSH, generate public key files with the **ssh-keygen** command using an empty passphrase and deploy the file to all the HMC. In Example 8-1, the HMCs host names are `hmc1` through `hmc7`.

Example 8-1 Update multiple machines simultaneously

```
for i in 1 2 3 4 5 6 7
do
   scp hmc_update.zip hscroot@hmc$i:/home/hscroot
done
for i in 1 2 3 4 5 6 7
do
   ssh hscroot@hmc$i “updhmc -t disk -f /home/hscroot/hmc_update.zip -c -r”
done
```

The first `for` loop in the example copies an interim fix whose file name is `hmc_update.zip`, to seven HMCs. The second for loop runs the **updhmc** command for each of the same seven HMCs. When the command finishes, it removes the update file and reboots the HMC.

8.5.7 HMC code remotely install/upgrade

The traditional method many administrators use to upgrade their HMC is to use recovery media; the procedures for installing or upgrading the HMC are well-documented. Upgrades performed remotely are becoming more popular. This section illustrates an example of performing an HMC upgrade remotely.

HMC CLI commands used

During the remote upgrade process, you will use the following commands:

getupgfiles	Retrieve network installation images.
chhmc	Set up alternate disk boot method.
hmcshutodwn	Reboot the HMC.
updhmc	Apply corrective service patch.

IBM FTP repository for HMC images

Both the **getupgfiles** command and **updhmc** command syntax in following example use an IBM FTP server. If your HMC can get to the IBM FTP server used in this example then you can enter the commands exactly as shown. If not, you can use your own FTP server, SFTP server, or NFS server (see man pages). The IBM FTP repository for HMC and also other product updates is `ftp.software.ibm.com` and HMC has separate directories for various types of fixes as follows:

Network install images:	`/software/server/hmc/network`
HMC updates:	`/software/server/hmc/updates`
Corrective service fixes:	`/software/server/hmc/fixes`

Example command syntax used in remote upgrade

The following example assumes that your HMC is at V7R7.2 and you want to upgrade to V8R8.4. Here are the steps for the upgrade:

1. Prior to starting an upgrade a good practice is to use the following commands first:

   ```
   chsvcevents -o closeall
   chhmc -o f -d 0
   hmcshutdown -t now -r
   ```

2. Save upgrade data to HMC hard disk:

   ```
   saveupgdata -r disk
   ```

3. Download the network install images to HMC:

   ```
   getupgfiles -h ftp.software.ibm.com -u anonymous --passwd ftp \
   -d /software/server/hmc/network/v8840
   ```

   > **Note:** The **getupgfiles** operation will mount the /hmcdump file system, copy the install files into the directory, and then unmount the file system.

4. Set the HMC to boot from an alternate disk partition:

   ```
   chhmc -c altdiskboot -s enable --mode upgrade
   ```

5. Reboot the HMC to begin the upgrade:

   ```
   hmcshutdown -r -t now
   ```

   > **Note:** The HMC will boot from the alternate disk partition then start processing the upgrade files, a process that takes some time. Most of the installation is complete between one to two hours.

6. After the upgrade is completed you might need to install the available corrective service fixes, which you can do from the command line as follows:

   ```
   updhmc -t s -h ftp.software.ibm.com -u anonymous -p ftp \
   -f /software/server/hmc/updates/HMC_Update_<Version>.iso /r
   ```

   Where <Version> is the version number of the service pack.

Considerations when doing a remote network upgrade

Although the HMC CLI environment is restricted, some common scripting commands can be used to monitor the status of network image downloads, which can be constructed as hscroot:

```
while true ; do
date
ls -la /hmcdump
sleep 60
done
```

Typically the file system /hmcdump remains mounted until the **getupgfiles** command completely exits. You can use the commands to see the files collected in /hmcdump to ensure the sizes are correct.

Post upgrade verification

You can use the command **lshmc -V** post upgrade to verify the build level of your HMC.

8.5.8 Network installation, update, backup, and restore

Since HMC Version 5 Release 1.0, you can select the integrated network adapter in your HMC as a start-up or IPL device. This approach allows the HMC to contact a remote system that supports PXE requests to perform installation, upgrade, backup, or restore operations on the HMC. To perform a secure backup/restore operation over the network, the remote system must have an SSH server running. The PXE setup is explained in Appendix E, “Preboot Execution Environment” on page 587.

8.5.9 Tips for maintaining Licensed Internal Code

Be sure to keep track of new releases, updates, and emergency fixes to HMC code. You can do this in one of two ways:

- Sign up for the technical support subscription service to receive emails when updates become available on the web
- Monitor the web manually on a regular basis at the Fix Central website:

  `http://www.ibm.com/support/fixcentral/`

Code and resources on the web

Read the website carefully. Select the correct HMC version, whichever is appropriate. The Fix Central website has many resources, such as these examples:

- Links to additional technical information.
- Hints and tips.
- The latest command-line specification (command-line reference).
- Recovery DVDs to order.
- Download packages that contain ISO files needed to burn you own recovery media.

  > **Note:** This media is bootable.

- Download updates to HMC code and also emergency fixes, or order DVDs containing the updates and fixes.

  > **Note:** This media is *not* bootable.

Maintain backups

Maintain a current Management Console Data backup. If you use Recover Media to update your Licensed Internal Code to a new release level, make a new backup after the upgrade process. A Management Console Data backup created at V8R8.1 will *not* work on a system that was upgraded to V8R8.4 using a recovery DVD. However, if you are trying to recover after losing a disk on a system that was updated using the Corrective Service files, you *can* use a Management Console Data backup (created at V8R8.4) with your V8R8.4 Recovery DVD.

8.6 Maintaining system firmware

The naming convention for system firmware update files is as follows:

```
01WW_XXX_YYY_ZZZ
```

Where:

- `WW` is an identifier, consisting of two letters.
- `XXX` is the release level.
- `YYY` is the service pack level.
- `ZZZ` is the latest disruptive service pack level.

Upgrades from one release level to another (`XXX`) are always disruptive, meaning you must restart your managed system (do an IPL again). Updates between service pack levels may be run concurrently, but you need to check.

You might need to upgrade existing HMC code to support a new server that is running the latest system firmware. As soon as you upgrade the HMC for the new server, you should plan to upgrade the existing managed server to the new system firmware level. Upgrade the HMC code before upgrading system firmware on the existing server or attaching new servers.

8.6.1 Concurrent versus disruptive updates

An installation is *disruptive* if the following statements are *true*:

- The release levels (XXX) differ.
- The service pack level (YYY) and the last disruptive service pack level (ZZZ) are the same.
- The service pack level (YYY) currently installed on the system is lower than the last disruptive service pack level (ZZZ) of the service pack to be installed.

An installation is *concurrent* if *both* of the following statements are *true*:

- The release level (XXX) is the same.
- The service pack level (YYY) currently installed on the system is the same or greater than the last disruptive service pack level (ZZZ) of the service pack to be installed.

8.6.2 Memory considerations for firmware upgrades

Firmware release level upgrades and service pack updates can consume additional system memory. Server firmware requires memory to support the logical partitions on the server. The amount of memory required by the server firmware varies according to several factors:

- Number of logical partitions
- Partition environments of the logical partitions
- Number of physical and virtual I/O devices used by the logical partitions
- Maximum memory values given to the logical partitions

Generally, you can estimate the amount of memory required by server firmware to be approximately 8% of the system installed memory. The actual amount required will generally be less than 8%. However, some server models require an absolute minimum amount of memory for server firmware, regardless of the previously mentioned considerations.

A

myHMC

With the myHMC Android or iOS application, you can connect to and monitor managed objects on your Power systems Hardware Management Console (HMC).

Monitoring includes the status of your managed systems, logical partitions or virtual machines, and Virtual I/O Servers. The application also allows you to view resource groups, serviceable events, and performance data.

This appendix describes the installation, configuration, and operation of the myHMC application.

Installation

The myHMC application is available for Android and iOS smartphones and tablets.

For installation, go to your App Store, search for the myHMC application and install it to your device.

Android

For Android, the application is available in the Google Play App Store.

Requirements are as follows:

- The operating system on your device must be Android version 4.4 or later.
- The size of the application is 3.8 MB.

iOS

For iOS, the application is available in the Apple App Store.

Requirements are as follows:

- The operating system on your device must be iOS 7.0 or later.
- The application is compatible with iPhone, iPad, and iPod touch.
- The size of the application is 8.4 MB.

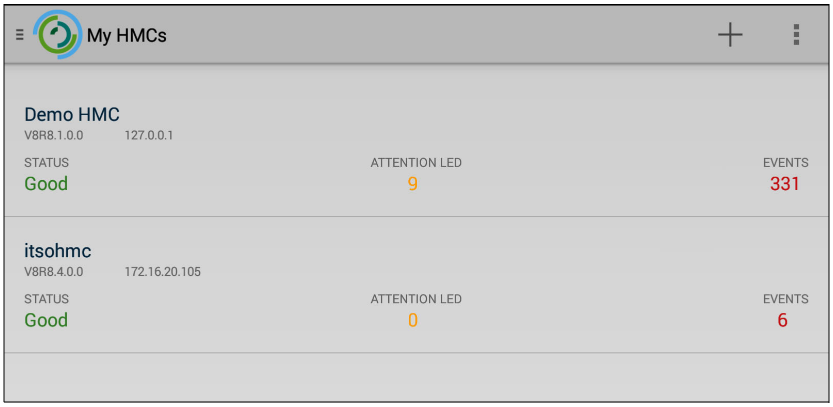
Configuration

After you install the application, click the myHMC icon (Figure A-1), to start the application.

Figure A-1 myHMC icon

The initial screen opens (Figure A-2 on page 555). It has the overview of all HMCs known to the application.

Note: The screens can look different from the examples presented here, depending on the operating system you use (Android or iOS) and on the device you use.



Demo HMC
V8R8.1.0.0 127.0.0.1

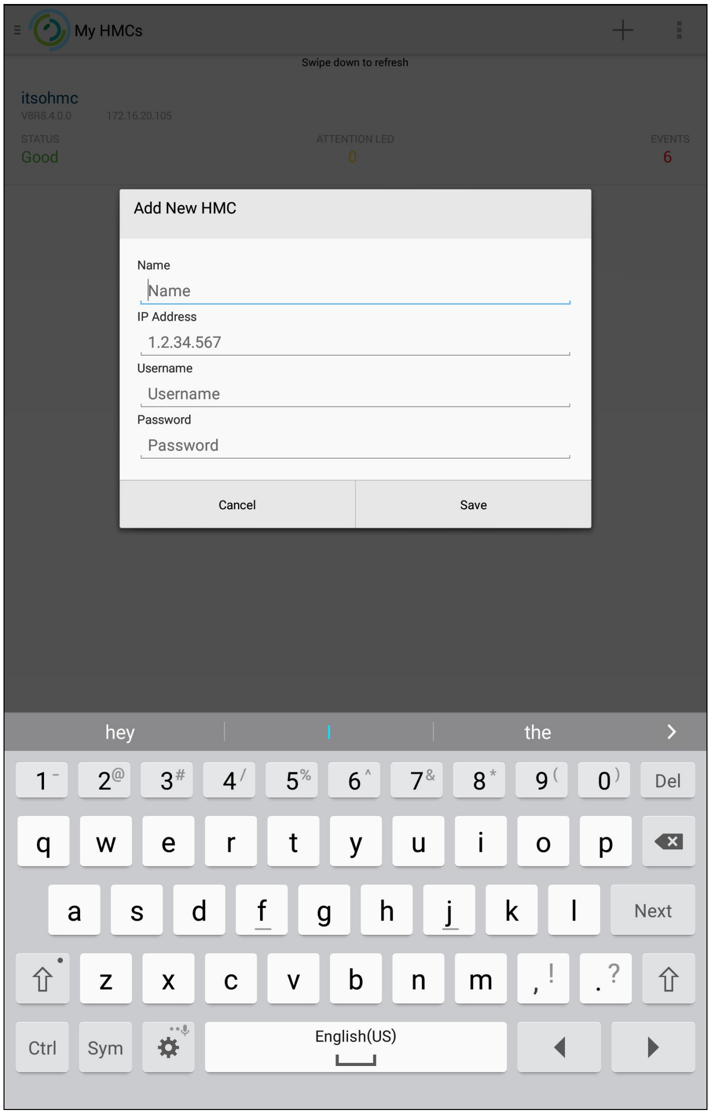
STATUS	ATTENTION LED	EVENTS
Good	9	331

itsohmc
V8R8.4.0.0 172.16.20.105

STATUS	ATTENTION LED	EVENTS
Good	0	6

Figure A-2 Initial Overview screen

When you first start the application, a virtual demo HMC is already installed. Pay with it to get a feeling of how it works and what you will see, but you can also delete it. To add a new HMC, select the plus sign (**+**). The **Add New HMC** screen is displayed (Figure A-3).



itsohmc
V8R8.4.0.0 172.16.20.105

STATUS	ATTENTION LED	EVENTS
Good	0	6

Add New HMC

Name: Name

IP Address: 1.2.34.567

Username: Username

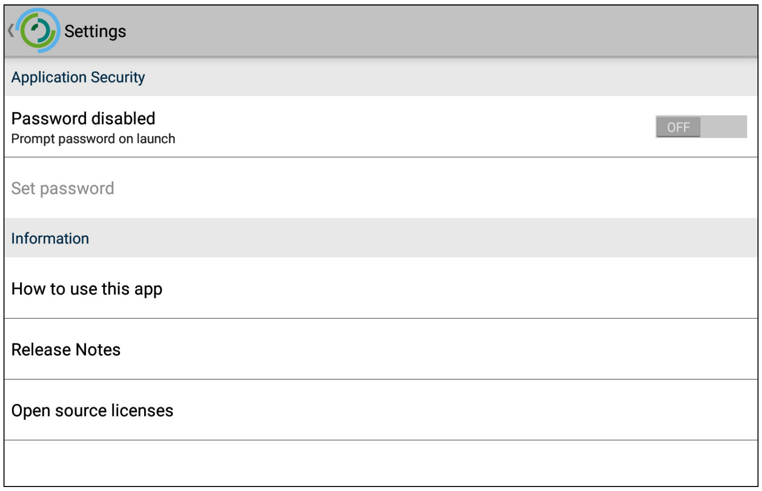
Password: Password

Figure A-3 Add new HMC screen

Here, you type in the connection data for your HMC (Name, IP Address, Username, and Password). Be sure your device can reach your HMC by network (firewall or firewalls). Then, the application tries to connect to your HMC. If the connection is successful you see your HMC on the Overview screen (Figure A-2 on page 555).

Settings

The top of the Overview screen has an icon, which you can use to get to the **Settings** screen (Figure A-4). On the Settings screen, you specify whether you want to use a password for the myHMC application and if so which password. From this screen, you can also get version information about the application, a short introduction of how to use the application, and the open source licenses for the application.



Settings

Application Security

Password disabled
Prompt password on launch

OFF

Set password

Information

How to use this app

Release Notes

Open source licenses

Figure A-4 Settings screen

To modify or delete an HMC from the Overview screen, press the HMC for a longer time. A menu opens (Figure A-5) where you can choose to edit the settings for the connection to the HMC (changing IP address, password, and so on) and where you can choose to delete an HMC from the Overview screen.

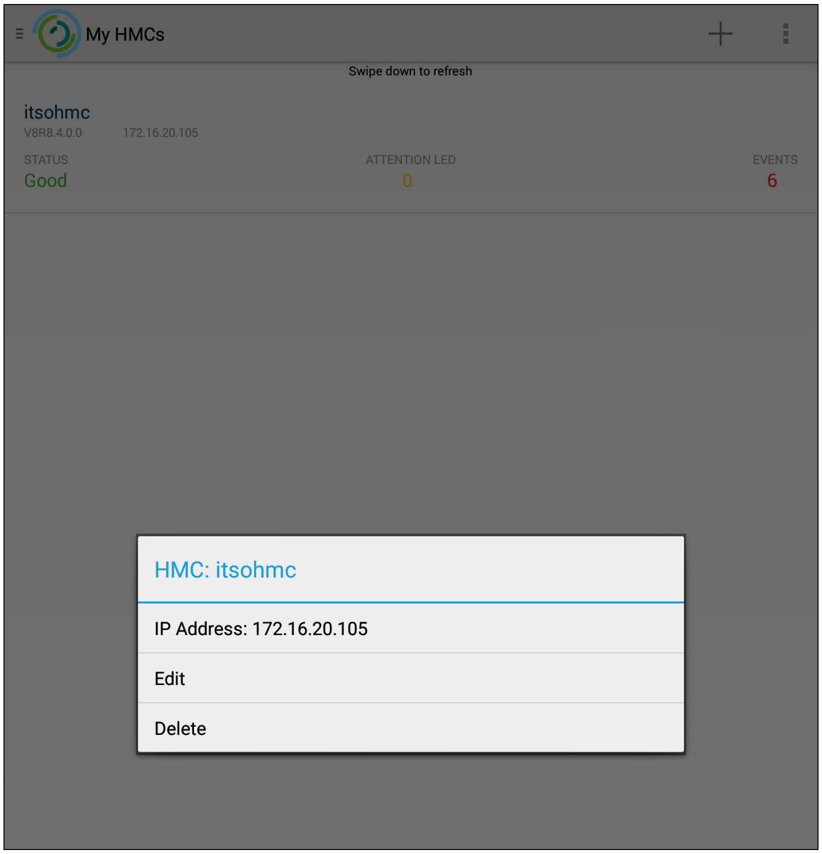


Figure A-5 Edit/Delete menu for an HMC

If you have any problems with the myHMC application, shake the device. A feedback menu opens (Figure A-6). Use it to get help by sending feedback to the development team of the myHMC application.

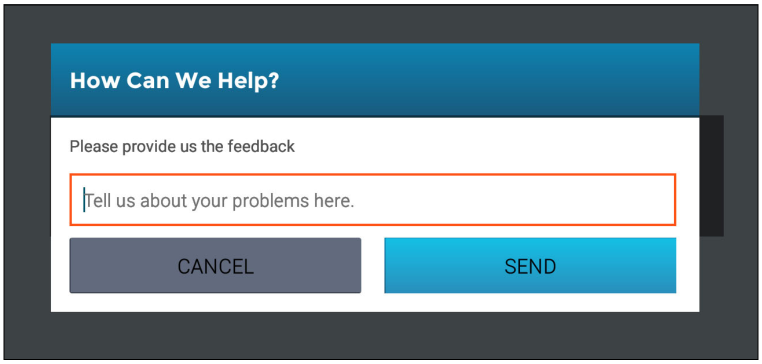

How Can We Help?
Please provide us the feedback
Tell us about your problems here.
CANCEL
SEND

Figure A-6 Feedback menu

Operation

On the Overview screen (Figure A-2 on page 555), you can choose between the Overview screen and the My Dashboard view of all your HMCs (Figure A-7). A graphical presentation of the status of your managed systems and of your logical partitions are displayed.

Note: All the operation screens that are available in the myHMC application are only views. No screen is available where you can actually configure something on the HMC, such as stopping or starting a managed system or a logical partition.

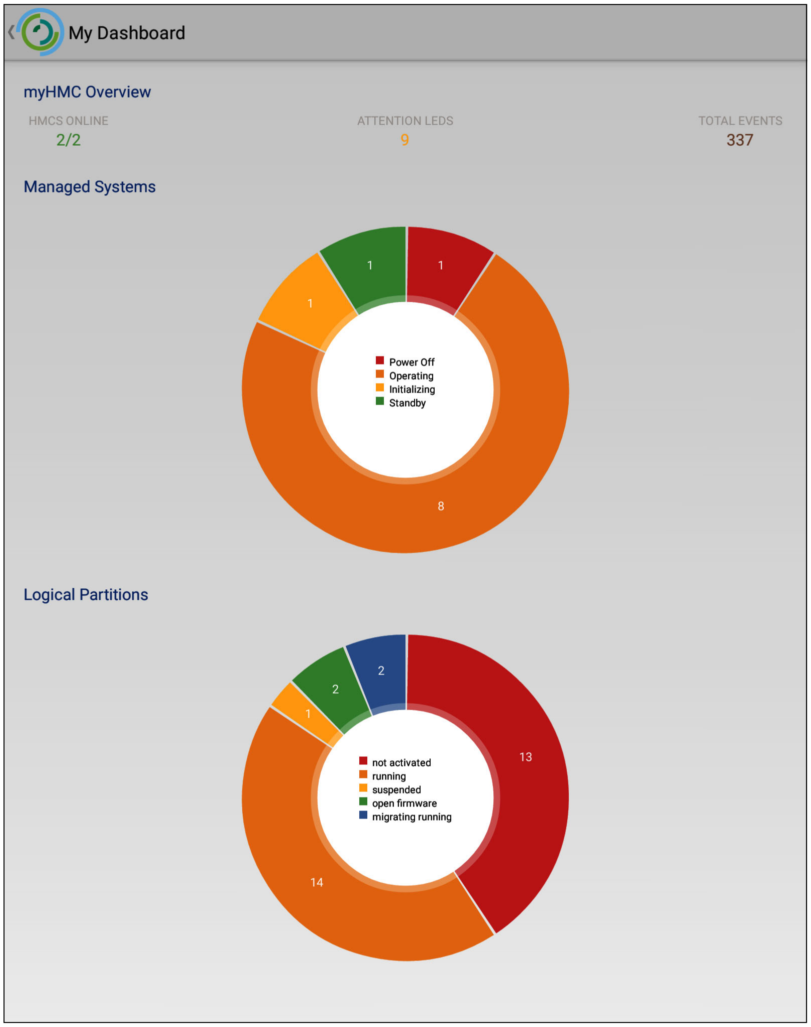
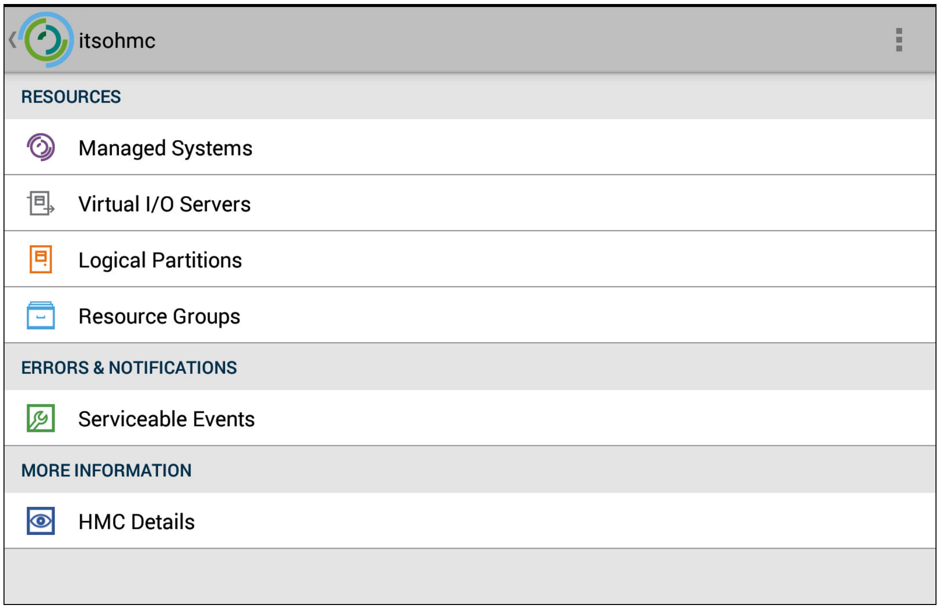


Figure A-7 myHMC Dashboard

When you select an HMC on the Overview screen, the main menu for the selected HMC is displayed (Figure A-8). Here you can select between views of the resources you have, the errors and notifications of the HMC, and information about your HMC.



itsohmc

RESOURCES

Managed Systems

Virtual I/O Servers

Logical Partitions

Resource Groups

ERRORS & NOTIFICATIONS

Serviceable Events

MORE INFORMATION

HMC Details

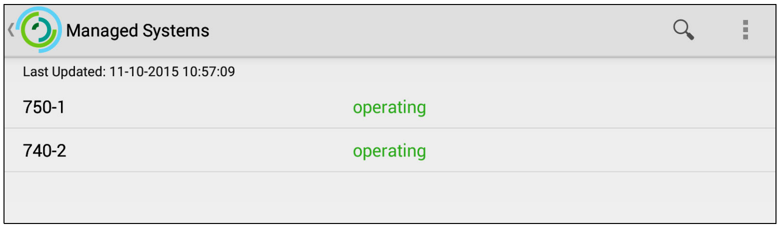
Figure A-8 HMC main menu

The menu options are as follows:

- Resources
  - Managed Systems
  - Virtual I/O Servers
  - Logical Partitions
  - Resource Groups
- Errors & Notifications
  - Serviceable events
- More Information
  - HMC Details

Managed Systems option

If you select **Managed Systems** from the menu, the Managed Systems screen opens and lists the name and status of your managed systems (Figure A-9).



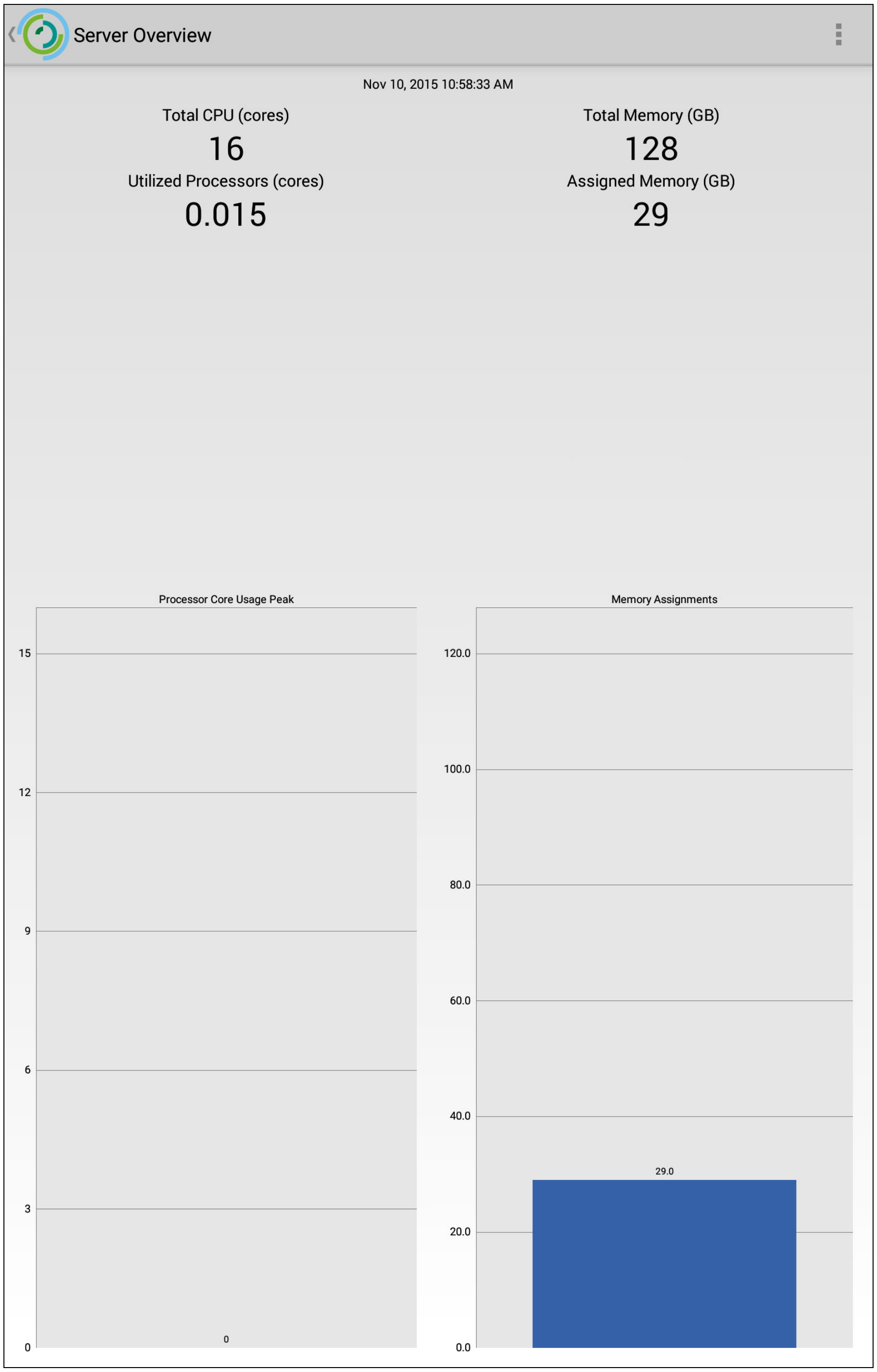
Managed Systems

Last Updated: 11-10-2015 10:57:09

750-1	operating
740-2	operating

Figure A-9 Managed Systems screen

If you select one of your managed systems, a Server Overview screen opens to show an overview of your managed system (Figure A-10). It indicates the resources (CPU and memory) that your managed system has.



Server Overview

Nov 10, 2015 10:58:33 AM

Total CPU (cores)
16

Utilized Processors (cores)
0.015

Total Memory (GB)
128

Assigned Memory (GB)
29

Figure A-10 Server Overview screen

Furthermore you can view two screens, with values for Total, Allocated, and Used resources:

- CPU Performance (Figure A-11)
- Memory Performance (Figure A-12 on page 562)

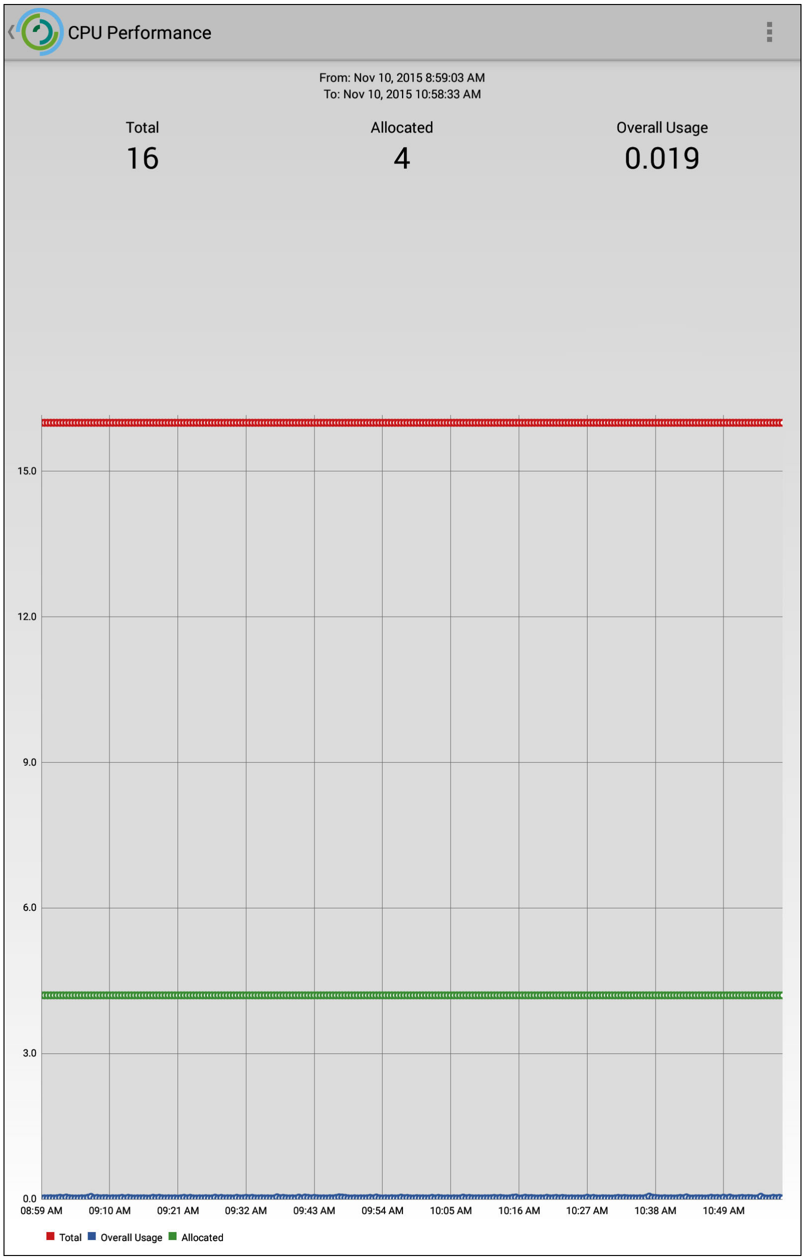
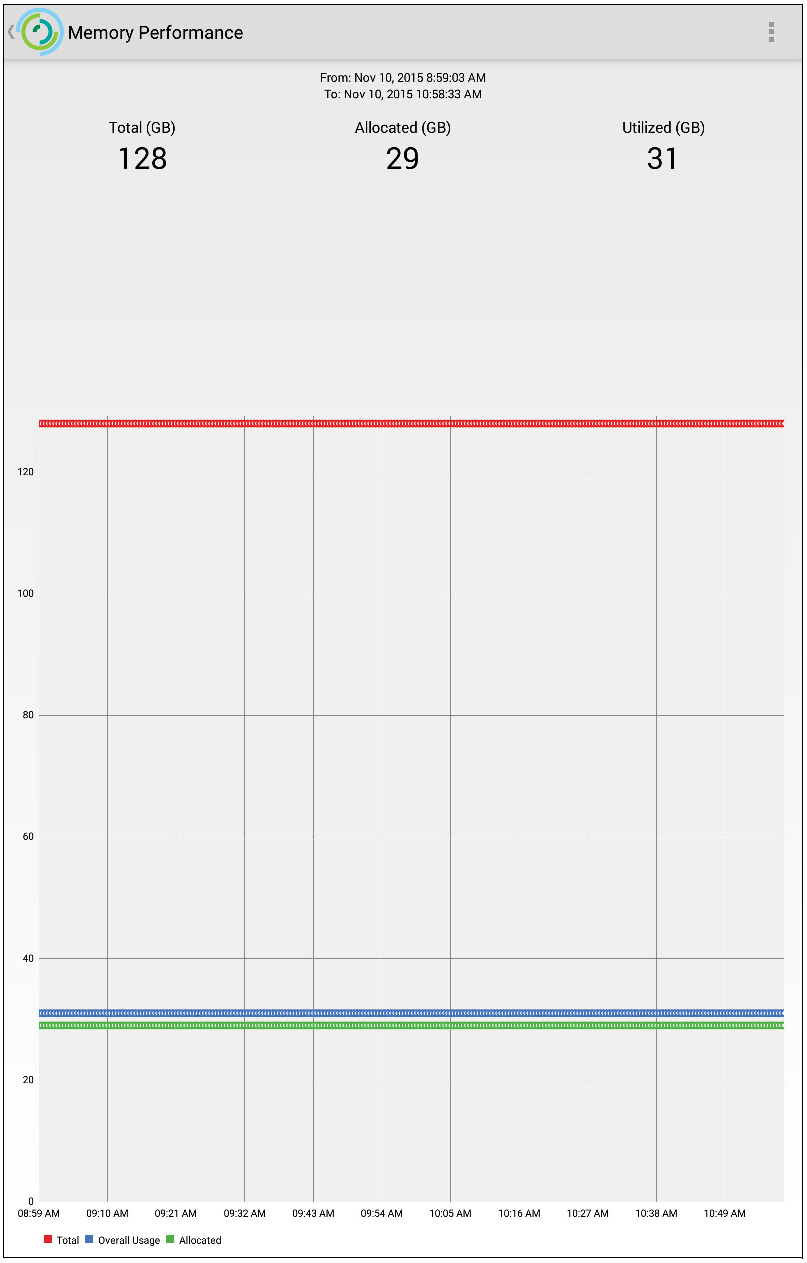


Figure A-11   CPU Performance screen



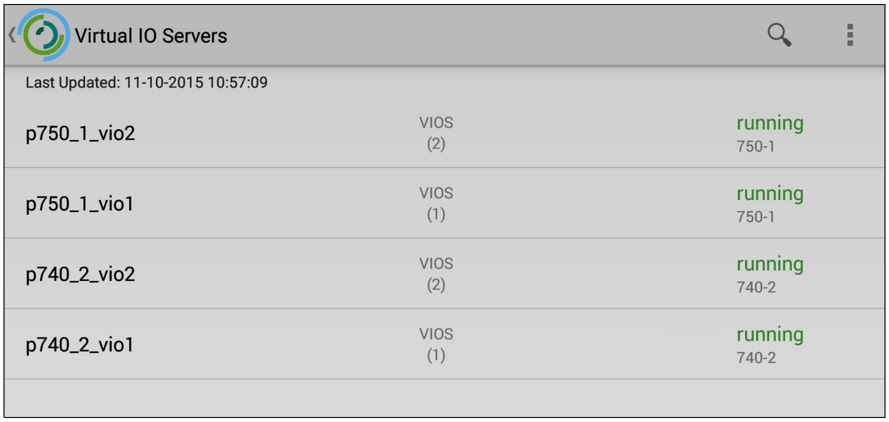
From: Nov 10, 2015 8:59:03 AM
To: Nov 10, 2015 10:58:33 AM

Total (GB)	Allocated (GB)	Utilized (GB)
128	29	31

Figure A-12 Memory Performance screen

Virtual I/O Servers option

If you select **Virtual I/O Servers** from the menu, an overview screen of your Virtual I/O Servers opens (Figure A-13 on page 563). It lists the names and the status of your Virtual I/O Servers.



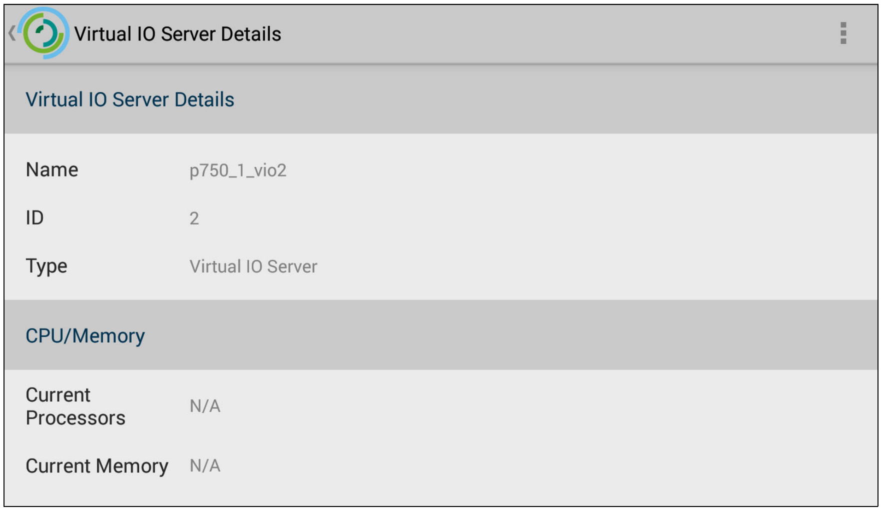
Virtual IO Servers

Last Updated: 11-10-2015 10:57:09

p750_1_vio2	VIOS (2)	running 750-1
p750_1_vio1	VIOS (1)	running 750-1
p740_2_vio2	VIOS (2)	running 740-2
p740_2_vio1	VIOS (1)	running 740-2

Figure A-13 Virtual I/O Servers screen

If you select a Virtual I/O Server, you can view more details about the selected Virtual I/O Server (Figure A-14). It lists information such as name or ID of the Virtual I/O Server.



Virtual IO Server Details

Virtual IO Server Details

Name	p750_1_vio2
ID	2
Type	Virtual IO Server

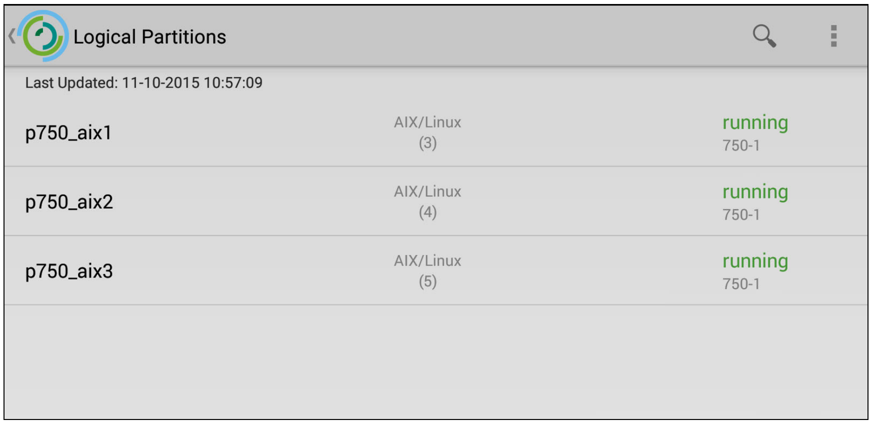
CPU/Memory

Current Processors	N/A
Current Memory	N/A

Figure A-14 Virtual I/O Server Details screen

Logical Partitions option

If you select **Logical Partitions** from the menu, an overview of your logical partitions is displayed (Figure A-15). It lists names and status of your logical partitions.



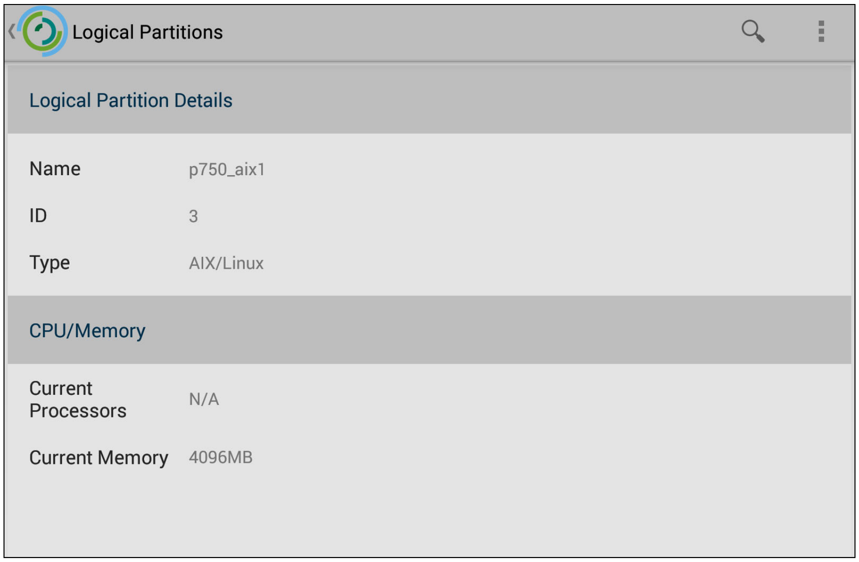
Logical Partitions

Last Updated: 11-10-2015 10:57:09

p750_aix1	AIX/Linux (3)	running 750-1
p750_aix2	AIX/Linux (4)	running 750-1
p750_aix3	AIX/Linux (5)	running 750-1

Figure A-15 Logical Partitions screen

If you select a logical partition, a screen with more details for the selected logical partition opens (Figure A-16). It lists information such as Name, ID, and type of the logical partition.



Logical Partitions

Logical Partition Details

Name p750_aix1

ID 3

Type AIX/Linux

CPU/Memory

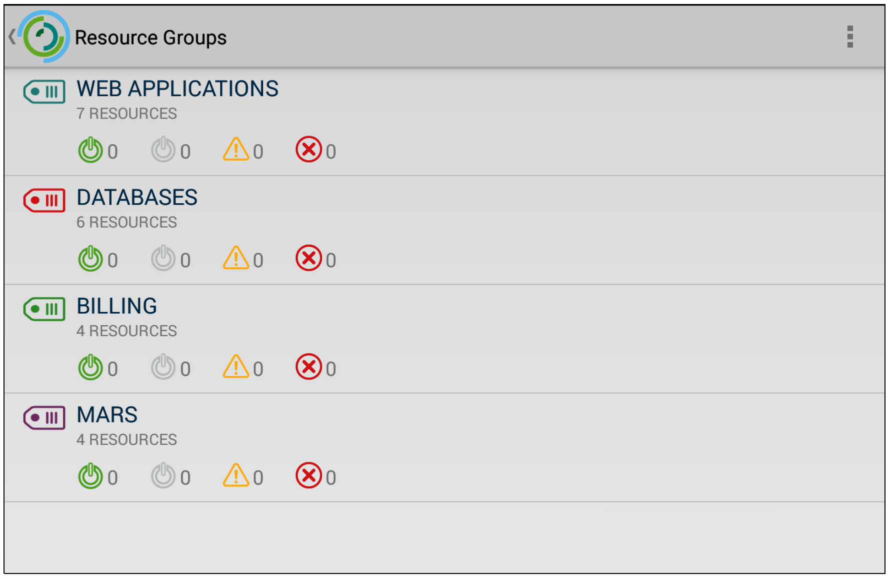
Current Processors N/A

Current Memory 4096MB

Figure A-16 Logical Partitions screen

Resource Groups option

If you select **Resource Groups** from the menu, an overview of your groups is displayed (Figure A-17), if you have any specified on the HMC. It lists overall status and number of members in the Resource Group.



Resource Groups

WEB APPLICATIONS
7 RESOURCES
⏻ 0 ⏻ 0 ⚠ 0 ⊗ 0

DATABASES
6 RESOURCES
⏻ 0 ⏻ 0 ⚠ 0 ⊗ 0

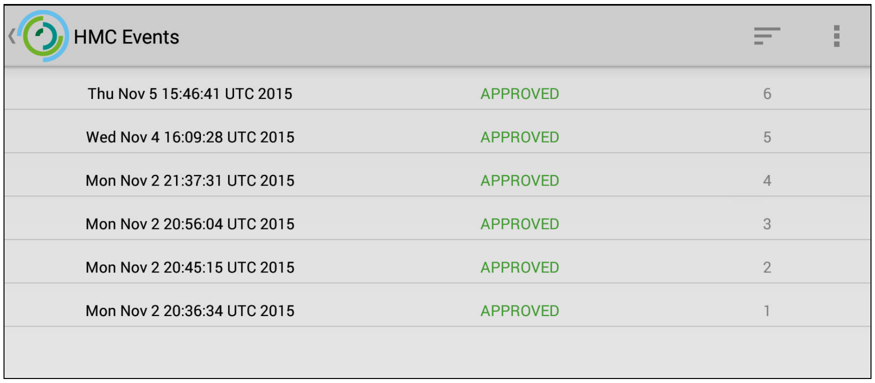
BILLING
4 RESOURCES
⏻ 0 ⏻ 0 ⚠ 0 ⊗ 0

MARS
4 RESOURCES
⏻ 0 ⏻ 0 ⚠ 0 ⊗ 0

Figure A-17 Resource Groups screen

Serviceable Events option

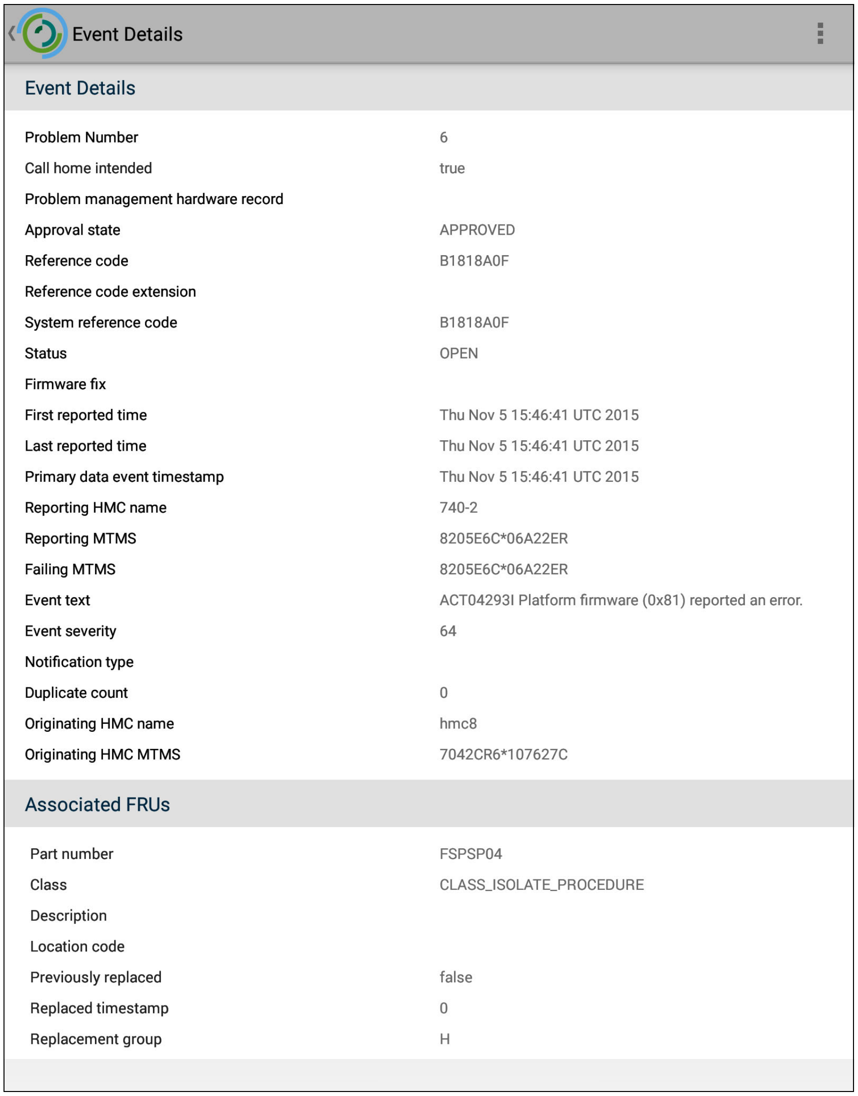
If you select **Serviceable Events** from the menu, an overview of the events of the HMC that was selected in the Overview screen is displayed (Figure A-18). It lists the timestamp and status of the event.



Thu Nov 5 15:46:41 UTC 2015	APPROVED	6
Wed Nov 4 16:09:28 UTC 2015	APPROVED	5
Mon Nov 2 21:37:31 UTC 2015	APPROVED	4
Mon Nov 2 20:56:04 UTC 2015	APPROVED	3
Mon Nov 2 20:45:15 UTC 2015	APPROVED	2
Mon Nov 2 20:36:34 UTC 2015	APPROVED	1

Figure A-18 HMC Events screen

If you select an Event, the Event Details screen opens (Figure A-19). It list all the information about an event, as you would see in the Event screen on the HMC.



Event Details

Problem Number	6
Call home intended	true
Problem management hardware record	
Approval state	APPROVED
Reference code	B1818A0F
Reference code extension	
System reference code	B1818A0F
Status	OPEN
Firmware fix	
First reported time	Thu Nov 5 15:46:41 UTC 2015
Last reported time	Thu Nov 5 15:46:41 UTC 2015
Primary data event timestamp	Thu Nov 5 15:46:41 UTC 2015
Reporting HMC name	740-2
Reporting MTMS	8205E6C*06A22ER
Failing MTMS	8205E6C*06A22ER
Event text	ACT04293I Platform firmware (0x81) reported an error.
Event severity	64
Notification type	
Duplicate count	0
Originating HMC name	hmc8
Originating HMC MTMS	7042CR6*107627C

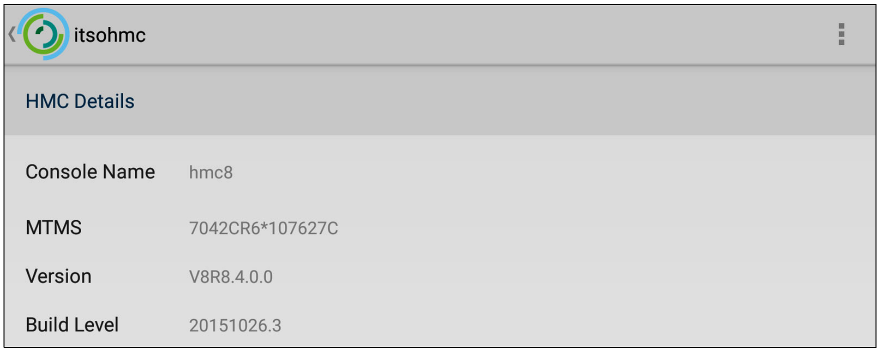
Associated FRUs

Part number	FSPSP04
Class	CLASS_ISOLATE_PROCEDURE
Description	
Location code	
Previously replaced	false
Replaced timestamp	0
Replacement group	H

Figure A-19 Event Details screen

HMC Details option

If you select **HMC Details** from the menu, details of the HMC you selected in the Overview screen are displayed (Figure A-20). Details include information such as model and serial number of the HMC, version of the HMC, and the build level.



HMC Details

Console Name hmc8

MTMS 7042CR6*107627C

Version V8R8.4.0.0

Build Level 20151026.3

Figure A-20 HMC Details screen

B

CLI commands examples

Common HMC command-line interface (CLI) commands are described in this appendix.

List and manage the HMC configuration

Use the commands described here to list and manage the HMC configuration.

lshmc

The **lshmc** command lists information related to the HMC itself, such as in these examples:

- List the BIOS level of the HMC (this might not be relevant for virtual HMCs):

  ```
  lshmc -b
  ```

- List the network settings for the HMC:

  ```
  lshmc -n
  ```

- List the VPD information for the HMC:

  ```
  lshmc -v
  ```

- List detailed version and maintenance level of the HMC:

  ```
  lshmc -V
  ```

- List the state of the HMC Network Time Protocol (NTP) client, and IP address of its NTP server:

  ```
  lshmc -r -F xntp
  ```

chhmc

Use the **chhmc** command to change the HMC configuration, as shown in these examples:

- Change the HMC host name:

  ```
  chhmc -c network -s modify -h newhostname
  ```

- Set the IP address and network mask for network interface eth0:

  ```
  chhmc -c network -s modify -i eth0 -a 10.10.10.1 -nm 255.255.255.0
  ```

- Change the HMC date, time, and time zone:

```
chhmc -c date -s modify --datetime 110920262015\
--clock local --timezone 'America/New_York'
```

- Activate the NTP client, then add an NTP server and allow the firewall rule on eth1:

```
chhmc -c xntp -s enable
chhmc -c xntp -s add -h 172.16.20.1 -i eth1
```

hmcshutdown

Use the **hmcshutdown** to halt or reboot the HMC, as shown in these examples:

- Reboot the HMC after 3 minutes:

```
hmcshutdown -t 3 -r
```

- Halt the HMC immediately:

```
hmcshutdown -t now
```

Manage users on the HMC

Use the commands described here to manage users on the HMC.

lshmcusr

List HMC user information with the **lshmc** command, as shown in these examples:

- List all HMC users:

```
lshmcusr
```

- List only user names and managed resource roles for all HMC users, and separate the output values with a colon:

```
lshmcusr -F name:resourcerole
```

- List the HMC users hscroot and user1:

```
lshmcusr --filter \"names=hscroot,hscpe\"
```

- List all user with hmcpe task roles:

```
lshmcusr --filter taskroles=hmcpe -F name
```

mkhmcusr

Create HMC user information with the **mkhmcusr** command, as shown in these examples:

- Create the user `myhmcuser` (the user's password must be entered when prompted); use *either* of the following commands:

```
mkhmcusr -u myhmcuser -a hmcviewer
mkhmcusr -i "name=myhmcuser,taskrole=hmcviewer"
```

- Create user hscpe, with the `hmcpe` task role and a seven-character password:

```
mkhmcusr -u hscpe -a hmcpe -d pe --passwd abc1234
```

chhmcusr

Use the **chhmcusr** command to change HMC user information, as shown in these examples:

- Change the password for the user tester (the new password must be entered when prompted):

```
chhmcusr -u tester -t passwd
```

rmhmcusr

Use the **rmhmcusr** command to remove HMC user information, as in this example:

- Remove the user tester:

```
rmhmcusr -u tester
```

Manage systems configuration

The commands described here are for managing systems configuration.

lssyscfg

The **lssyscfg** command lists system resources, as shown in these examples:

- List all systems that are managed by this HMC with their current state, with a header:

```
lssyscfg -r sys -F name,state --header
```

- List all partitions in the managed system, and display their name, operating system environment type, operating system version, ID, and current state, using a colon as a separator:

```
lssyscfg -r lpar -m 740-2 -F name:lpar_env:os_version:lpar_id:state
```

- List all partitions in the managed system, and display their name, Resource Monitoring and Control (RMC) state, and RMC IP address:

```
lssyscfg -r lpar -m 740-2 -F name,rmc_state,rmc_ipaddr
```

mksyscfg

The **mksyscfg** command creates resources, as shown in these examples:

- Create an AIX or Linux partition:

```
mksyscfg -r lpar -m 740-2 -i
name=itsolpar,profile_name=prof1,lpar_env=aixlinux,min_mem=256,desired_mem=1024
,max_mem=1024,proc_mode=ded,min_procs=1,desired_procs=1,max_procs=2,sharing_mod
e=share_idle_procs,auto_start=1,boot_mode=norm,lpar_io_pool_ids=3,\"io_slots=21
010003/3/1,21030003//0\"
```

- Create partition profiles by using the configuration data in the `/tmp/profcfg` file:

```
mksyscfg -r prof -m 740-2 -f /tmp/profcfg
```

- Create a partition profile by saving the current configuration of a partition:

```
mksyscfg -r prof -m 740-2 -o save -p p1 -n newProfile
```

chsyscfg

The **chsyscfg** command changes system resources, as shown in this example:

- Change a partition profile's memory amounts (reduce the profile's current memory amounts each by 256 MB), and number of processors you want:

```
chsyscfg -r prof -m 740-2 -i
name=prof1,lpar_name=itsolpar,min_mem=256,desired_mem=256,max_mem=256,desired_p
rocs=2
```

rmsyscfg

Use the **rmsyscfg** command to remove a system resource, as shown in these examples:

- Remove the partition lpar1:

  ```
  rmsyscfg -r lpar -m 740-2 -n lpar1
  ```

- Remove the partition profile test_profile for partition lpar1:

  ```
  rmsyscfg -r prof -m 740-2 -n test_profile -p lpar1
  ```

Manage hardware resources

The commands described here are for managing hardware resources.

lshwres

List hardware resources with the **lshwres** command, as show in these examples:

- List all system level memory information:

  ```
  lshwres -r mem -m 740-2 --level sys
  ```

- List all virtual slots for partition lpar1:

  ```
  lshwres -r virtualio --rsubtype slot -m 740-2 --level slot --filter
  “lpar_names=lpar1”
  ```

chhwres

Use the **chhwres** command to change hardware resources, as shown in these examples:

- Move 0.5 processing units from the partition with ID 3 to the partition with ID 5 (both partitions are using shared processors):

  ```
  chhwres -r proc -m 750-1 -o m --id 3 --tid 5 --procunits 0.1
  ```

- Add 1 GB of memory to the partition named `p750_aix2`, and time out after 10 minutes:

  ```
  chhwres -r mem -m 750-1 -o a -p p750_aix2 -q 1024 -w 10
  ```

- Move the partition sharedlpar1 to shared processor pool pool1:

  ```
  chhwres -r procpool -m 740-2 -o s -p sharedlpar1 -a
  "shared_proc_pool_name=pool1"
  ```

- Add a virtual Ethernet adapter to the partition `p750_aix3`, in slot 9, with PVID 4 and VLANs 105 and 106:

  ```
  chhwres -r virtualio -m 750-1 -o a -p p750_aix3 --rsubtype eth -s 9 -a
  ieee_virtual_eth=1,port_vlan_id=4,\"addl_vlan_ids=105,106\"
  ```

Commands to manage system connection

Use the commands described here to manage system connection.

lssysconn

The **lssysconn** command displays the systems and frames connected to the HMC, as shown in this example:

- List connection information for all systems and frames that are managed by this HMC:

  ```
  lssysconn -r all
  ```

mksysconn

Use the **mksysconn** command to create a system connection, as shown in these examples:

- Connect to and add the system with the IP address 9.3.152.145 (the HMC Access password for the system must be entered when prompted):

```
mksysconn --ip 9.3.152.145
```

- Enable all systems and frames to be automatically discovered by the HMC when using DHCP:

```
mksysconn -o auto
```

rmsysconn

Remove system connection with the **rmsysconn** command, as shown in this example:

- Disconnect from the managed system sytem1, and remove it from the HMC:

```
rmsysconn -o remove -m 740-2
```

Manage Capacity on Demand (CoD) resources

Use the commands described here to manage CoD resources.

lscod

Use the **lscod** command to list CoD information, as shown in these examples:

- Display CUoD processor capacity information:

```
lscod -m 740-2 -t cap -r proc -c cuod
```

- Display CUoD processor activation code generation information:

```
lscod -m system1 -t code -r proc -c cuod
```

- Display the CoD history log:

```
lscod -m 740-2 -t hist
```

chcod

Use the **chcod** command to change CoD resources, as shown in these examples:

- Enter a CoD code:

```
chcod -m 740-2 -o e -k code
```

- Activate 2 GB of On/Off CoD memory for 10 days:

```
chcod -m 740-2 -o a -c onoff -r mem -q 2048 -d 10
```

- Deactivate all On/Off CoD processors:

```
chcod -m 740-2 -o d -c onoff -r proc
```

Use VM virtual terminals

The commands in this section describe are for using VM virtual terminals.

mkvterm

Open a virtual terminal session for a Linux, AIX, or Virtual I/O Server partition with the **mkvterm** command, as shown in this example:

- Open a virtual terminal session for partition lpar1:

```
mkvterm -m 740-2 -p p740_2_vio2
```

rmvterm

Use the **rmvterm** command to close a virtual terminal session, as shown is this example:

- Close a virtual terminal session for partition lpar1

```
rmvterm -m 740-2 -p p740_2_vio2
```

vtmenu

Use the **vtmenu** command for an interactive session where you can select a logical partition to connect to with a virtual terminal session, as shown in Example B-1.

Example: B-1 vtmenu selection

```
----------------------------------------------------------
Partitions On Managed System:  750-1
OS/400 Partitions not listed
----------------------------------------------------------
   1)    LPAR1                                 Running
   2)    p750_1_vio1                           Running
   3)    p750_1_vio2                           Running
   4)    p750_aix1                             Not Activated
   5)    p750_aix3                             Running


Enter Number of Running Partition (q to quit):
```

C

IBM product engineering debug data collection

This appendix describes the process of collecting Hardware Management Console (HMC) IBM product engineering (PE) debug data. To support problem determination in an IBM Systems environment, this data collection might be required.

Preparing to collect the pedbg

In preparation to collect the data, the following conditions must be met:

- A special user (hscpe) to collect the data must exist.
- A transfer method to offload debug data must exist.

To run the collection, the user ID hscpe with task role hmcpe must exist in the HMC.

To verify the existence of the hscpe user on the HMC, use one of the following ways:

- Log in to the graphical user interface (GUI) and select **Users and Security** → **Users and Roles** → **Manage User Profiles and Access**.
- Use the command-line interface (CLI).

The following steps describe how to use the CLI to verify the hscpe user exists on the HMC:

1. Log in to the CLI by using the hscroot user or a user with hmcsuperadmin role.
2. Run the following command:

   ```
   lshmcusr --filter “names=hscpe”
   ```

   If the hscpe user *does not* exist, the output is similar to Example C-1.

   Example: C-1 The lshmcusr command shows no hscpe user

   ```
   hscroot@hmc8:~> lshmcusr --filter "names=hscpe"
   No results were found.
   hscroot@hmc8:~>
   ```

   If the hscpe user exists, the output is similar to Example C-2 and you can skip to step 4.

   Example: C-2 lshmcusr command show hscpe user

   ```
   hscroot@hmc8:~> lshmcusr --filter "names=hscpe"
   name=hscpe,taskrole=hmcpe,description=new user from
   Wizard,pwage=99999,resourcerole=ALL:,authentication_type=local,remote_webui_acc
   ess=0,remote_ssh_access=1,min_pwage=0,session_timeout=0,verify_timeout=15,idle_
   timeout=0,inactivity_expiration=0,resources=<ResourceID = ALL:><UserDefinedName
   = AllSystemResources>,password_encryption=sha512,disabled=0
   hscroot@hmc8:~>
   ```

3. Create the hscpe user, run the following command:

   ```
   mkhmcusr -u hscpe -a hmcpe -d IBM Service
   ```

   In the GUI follow the steps to create a user, as described in 4.2.2, “Manage User Profiles and Access option” on page 273.

4. Prepare a removable media (such as DVD-RAM or USB flash memory device) that you want to use to offload the logs. See 5.3.5, “Format Media” on page 321 for Instructions.

Run the PE debug (pedbg) collection command

Log in to the HMC CLI as user `hscpe` and run the PE debug collection in quiet mode by using the following command:

```
pedbg -c -q 3
```

You may also use the following command option to be prompted to copy files to media:

```
pedbg -c -q 9
```

> **Note:** The valid options for collecting HMC data in quiet mode are as follows:
>
> 1 = Network information only.
> 2 = Network information + base logs.
> 3 = Network information + base logs + extended logs.
> 4 = Network information + base logs + extended logs + archives.
> 5 = Collect only those files in the `/home/hscpe/ibmsupt` directory.
> 7 = Collect RMC ctsnap only.
> 9 = Run prompt to copy files to media.

Another way is to run **pedbg** without options, which creates a file on the HMC and automatically prompts the you to move the file to a removable media or to leave it on the HMC. Use these steps:

1. Run the command:

   ```
   pedbg -c
   ```

2. Respond with **Yes** to all questions *until* you are prompted to collect archives:

   ```
   Would you like to collect archived log data?
   ```

   Respond with **No** unless the archives are specifically requested by the support representative.

Offload pedbg collection

Complete the following steps:

1. Verify the DVD-RAM or USB flash memory device is correctly formatted for service data and inserted.
2. When you see the following prompt, select **Yes** to move the data to DVD-RAM, USB flash memory device, or to a remote secure copy server (scp server) with the **scp** command:

   ```
   Would you like to move zip file to a DVD or other device?
   ```

3. The HMC spends several seconds to recognize the USB device. At the prompt, enter the name or the device.

   The device name is the mount point for the target device, for example a DVD would be `/media/cdrom` and an USB flash memory device would be `/media/sdb1`.

4. For the network option, you are prompted for user name, IP address of the scp enabled server, and the working directory. You might also be prompted to accept the RSA key fingerprint of the SCP server. Select Yes or No:
   - Select **Yes** to accept the key, then wait for the offload to start.
   - Select **No** if any other method is used to copy the data from the HMC. the HMC keeps the collection on the hard disk drive.

Example C-3 shows the process of offloading logs to a USB flash memory drive.

Example: C-3 Process of offloading logs to a USB flash memory device

```
These additional logs would be collected on request of PE support.
No

   Created /dump/HMClogs.hmc71108H44.zip

   Would you like to move zip file to a DVD or other Device?
   The answer no will write to the HMC harddisk
   Please type yes or no.
yes

The file is 114683212 bytes. Ensure you have enough room on the device.
Use formatted Read/Write media only
Enter a device name from the list below. example /media/cdrom

/media/cdrom=CD/DVD
/media/sdb1=USB flash memory device
network=move to another system via the scp command

/media/sdb1

Copy to /media/sdb1 in progress
```

Example C-4 shows the process of offloading logs to a network scp server.

Example: C-4 Process of offloading logs to a network scp server

```
/media/cdrom=CD/DVD
/media/sdb1=USB flash memory device
netwok=move to another system via the scp command

network

   Enter the user name on the destination host.
ftpuser
   Enter the desination host. Example myhost.mycompany.com
172.16.254.42
   Enter the destination filesystem on the host. Example /tmp/hmcdir
   The directory must exist and have correct permissions.

/users/ftpuser
   scp /dump/HMClogs.hmc71108H45.zip ftpuser@172.16.254.42:/users/ftpuser
The authenticity of host ‘172.16.254.42 (172.16.254.42)’ can’t be established.
RSA key fingerprint is 86:a4:f4:c9:47:b5:33:9f:39:37:29:eb:99:1c:81:6f.
Are you sure you want to continue (yes/no)? yes
Warning: Permanently added ‘172.16.254.42’ (RSA) to the list of known hosts.
Password:
HMClogs.hmc77108H45.zip                       100%  111MB 705.7KB/s  02:41
The send was successful
hscpe@hmc8:~>
```

Sending the data to IBM

The data can be sent in several ways to IBM. This section describes preferred methods. The method used varies depending on the network access of the HMC, remote support connections available to the HMC, and the availability of media.

Use HMC FTP

If the HMC has a network connection that allows FTP to the Internet, type the following command to send the file directly to IBM Support:

```
sendfile -f /dump/HMClogsxxxxxxxx.zip -h testcase.software.ibm.com -d /toibm/aix
-n nnnnn.bbb.ccc.HMClogs.zip -u anonymous --passwd noone@nowhere.com
```

This command has the following meanings:

-f The pedbg ZIP file name created. The **ls /dump** command can be used to display the file name.

-n The pedbg ZIP file renamed to start with PMR number in this format:

`nnnnn.bbb.ccc.HMClogsxxxxxxxxx.zip` where:

nnnn	IBM Problem Number
bbb	IBM Branch Number
ccc	IBM Country Code

HMClogsxxxxxxxx.zip The pedbg file created. The **ls /dump** command can be used to display the file name.

-d Directory to upload to:

For IBM i:	/toibm/os400/
For AIX:	/toibm/aix/

Note: If the data was mistakenly copied to DVD-RAM, use the following procedure to access the data from the HMC CD/DVD drive:

1. Type the **mount /media/cdrom** command.
2. Display the file using the **ls /media/cdrom** command.
3. Use the path name `/media/cdrom/HMClogsxxxxxxxx.zip` in the **sendfile** command.
4. Type the **umount /media/cdrom** command.

Use removable media (DVD-RAM or USB) and another workstation or server with Internet access

If another PC or server has both Internet access and either a USB drive or a DVD drive that can read DVD-RAM, it can be used to attach the ZIP file to an email or to use FTP to transfer the file to IBM Support.

Use SCP or FTP to another server with Internet access

If another server or workstation on the network has Internet access (email or FTP) and network access to the HMC, then the data can be copied to the other server using FTP or secure copy. It can then be emailed or sent by FTP to IBM support.

The **sendfile** command uses FTP to send the data from the HMC to the other server. See "Use HMC FTP" on page 579 for an example of the syntax or use the **--help** option.

The **scp** command can also be used to copy the file from the HMC.

Send the pedbg from another workstation or server with Internet access

Use these steps:

1. Rename the `pedbg` file.

   As you rename, add the PMR information from IBM Support to the beginning of the file name by using the following format:

   nnnn.bbb.ccc.HMClogsxxxxxxxxx.zip

   This name has the following components:

HMClogsxxxxxxxxx.zip	The `pedbg` file name
nnnnn	IBM problem number
bbb	IBM branch number
ccc	IBM country code

2. Send the file to IBM.

   To upload the `pedbg` file, select the preferred server for your geography from Table C-1.

Table C-1 Preferred servers depending on geography

Geography	Server	URL
North America	Testcase	https://testcase.boulder.ibm.com
Europe	ECuRep	https://www.ecurep.ibm.com/app/upload
Asia Pacific	Testcase or ECuRep	https://testcase.boulder.ibm.com

D

Live Partition Mobility support log collection

This appendix describes the information to gather for problems that involve Live Partition Mobility (LPM) errors. This process ensures that the log files do not wrap or get overwritten. Having these logs beforehand when calling IBM Support helps you to get a faster response in problem determination.

Background information

You must provide background information of the current Live Partition Mobility (LPM) configuration or any changes that were made before the problem occurs:

- Indicate whether this worked in the past:

  If it did, what changed, if known? Was the change related to the HMC, server firmware, Virtual I/O Server (VIOS), Virtual I/O Server adapter microcode, IBM i, IBM AIX, or SAN updates since the last failure?
- The name of the server and partition that failed.
- The approximate date and time (both the HMC and partition times) of the failure.
- Virtual I/O Server LPAR level, partition name, and ID, both source and target.
- HMC level and fixes that run the LPM.
- How the LPM was initiated, graphical user Interface (GUI) or command-line Interface (CLI).

HMC log collection

For a configuration with more than one HMC, you must repeat the following steps on both the source and the target HMC:

1. Use PE debug to collect data (HMC log). See details in Appendix C, “IBM product engineering debug data collection” on page 575.
2. Rename the logs with the problem management record (PMR) number if the LPM moves across the HMC (and see Example D-1):

   nnnn.bbb.ccc.HMClogsxxxxxxxxx.zip

   This name has the following components:

HMClogsxxxxxxxxx.zip	The `pedbg` file name
nnnnn	IBM problem number
bbb	IBM branch number
ccc	IBM country code

   Example D-1 HMC pedbg logs for LPM for more than one HMC

   ```
   nnnn.bbb.ccc.HMClogsxxxxxxxxx.source.zip
   nnnn.bbb.ccc.HMClogsxxxxxxxxx.target.zip
   ```

Operating system log collection

The following list describes the level requirements for LPM activity:

- IBM i:

  Verify that a minimum IBM i 7.1 technology refresh is installed. Issue these commands:

  ```
  DSPPTF OUTPUT (*PRINT)
  WRKPTFGRP OUTPUT (*PRINT)
  ```

  Get the spooled file to your local workstation.

- IBM AIX:
  - AIX LPAR level, partition name, and ID.
  - Collect **snap** information for AIX LPAR and copy it to your workstation (Example D-2).

Example D-2 Provide AIX client snap report

```
snap -r
snap -ac
mv /tmp/ibmsupt/snap.pax.Z
/tmp/ibmsupt/nnnn.bbb.ccc.client.src_msp.target_msp.snap.pax.Z
```

> **Note:** You should have one client LPAR snap. For more clients failing, you need an operating system log for every client LPAR.

Virtual I/O Server Mover Server Partition snaps

Collect **snap** data from each Virtual I/O (VIOS) Server Mover Server Partition (MSP). This process includes one or two (if redundant VIOS is configured) source partitions and one or two (if redundant VIOS is configured) target partitions.

1. Run **snap**. To collect the snap data on the Virtual I/O Server partition, use these steps:
   a. Log on to the Virtual I/O Server.
   b. Run the **snap** command and press Enter. Wait until the command completes the process.
   c. The `snap.pax.Z` file is in the `/home/padmin` directory. Rename the file to include the PMR number provided by IBM Support and indicate if it is the source or target:

   ```
   mv /home/padmin/snap.pax.Z nnnn.bbb.ccc.vio1.source.snap.pax.Z
   ```

   If you have redundant HMC, your files will be as follows:

   ```
   nnnn.bbb.ccc.vio1.source.snap.pax.Z
   nnnn.bbb.ccc.vio2.source.snap.pax.Z
   nnnn.bbb.ccc.vio1.target.snap.pax.Z
   nnnn.bbb.ccc.vio2.target.snap.pax.Z
   ```

2. Run **ctsnap**. This log is needed if an RMC-related issue exists. Use these steps:
   a. Run the following commands that are shown in Example :

   ```
   $ oem_setup_env
   # ctsnap -x runrpttr
   ```

   This command produces a report log in the `/tmp/ctsupt/ctsnap*.tar.gz` file.

   b. Rename the file to include the PMR number provided by IBM Support and indicate if it is the source or target:

   ```
   mv /tmp/ctsupt/ctsnap*.tar.gz /tmp/nnnn.bbb.ccc.source.ctsnap.pax.Z
   ```

   If you have redundant HMC, your file will be as follows:

   ```
   nnnn.bbb.ccc.vio1.source.ctsnap.pax.Z
   nnnn.bbb.ccc.vio2.source.ctsnap.pax.Z
   nnnn.bbb.ccc.vio1.target.ctsnap.pax.Z
   nnnn.bbb.ccc.vio2.target.ctsnap.pax.Z
   ```

Hypervisor HMC resource dump

The hypervisor HMC resource dump is to be collected only if requested by an IBM service representative. If you have dual HMCs to manage the system, you need only one resource dump. Do not run it again from the redundant HMC. For collecting hypervisor dumps on the command line, use the following steps:

1. Find your managed system:

   ```
   # lssyscfg - r sys - F name
   ```

2. Initiate the system dump:

   ```
   # startdump -t resource -m {managed system} - r “system”
   ```

   The file will be created in the `/dump` directory.

3. View the file:

   ```
   # ls -l /dump
   ```

   Do not offload the dump unless there is a file name `.IN_PROGRESS` extension removed by the HMC. This file indicates that the system dump is still in progress offloading from managed system service processor to HMC.

4. After the process completes, you can offload the dump through file transfer from the command line or by using the manage dump GUI in HMC.

Sending logs to IBM

You can send the logs to IBM in several ways. See also “Sending the data to IBM” on page 579. There is also an option to send the log individual by using HMC outbound connectivity. However, use either of these way to transfer a single created file:

- FTP to IBM
- IBM Enhanced Custom Data Repository (ECuRep) website

A single file is preferred. If the file is too large, a couple of files can be transferred. Move all previous `pax.Z` compressed and log files in to a single directory, then archive this directory. See Example D-3.

Example D-3 Archiving log files in AIX

```
$ mkdir -p /tmp/pmrnumber/pmdata
move,ftp, or scp data to sample directory above.
$ cd /tmp/pmrnumber
$ pax -xpax -vw pmdata | gzip -c > data_collected.pax.gz
```

FTP to IBM

Complete the following steps:

1. After a single file is created, rename the file to include the PMR number.

   For example, if `12345,999,000` is your PMR, it has these meanings:

   – 12345 is the PMR number
   – 999 is the branch number
   – 000 is the country code

Run the following command:

```
$ mv data_collected.pax.gz 12345.999.000_data_collected.pax.gz
```

2. Transfer the files to IBM through FTP. See Example D-4.

Example D-4 Transferring PMR files through FTP to IBM

```
$ ftp testcase.software.ibm.com
login: anonymous
passwd: (your email address in format your_email_id@your_email_domain)
ftp> cd /toibm/aix (for IBM AIX) or ftp> cd /toibm/os400 (for IBM i)
ftp> bin
ftp> put <filename> (in the example 12345.999.000_data_collected.pax.gz)
ftp> quit
```

IBM ECuRep

IBM Enhanced Customer Repository (IBM ECuRep) is another way to transfer logs to IBM. IBM ECuRep is a secure and fully supported data repository with problem determination tools and functions. It updates PMRs and maintains full data lifecycle management. IBM ECuRep needs an IBM ID and qualified PMR/Incident Number to send data.

For more information, see the IBM ECuRep website:

https://www.secure.ecurep.ibm.com/app/upload

E

Preboot Execution Environment

You can perform installation, backup, and restore operations on the HMC over the network through the Preboot Execution Environment (PXE). This appendix describes the process of setting up the PXE and how to install, back up, and restore through it.

HMC network installation, backup, and restore setup

The integrated Ethernet adapter on the HMC can be selected as a startup device, capable of sending PXE requests. This allows a Dynamic Host Configuration Protocol (DHCP) server in the same network, capable of accepting PXE requests, to acknowledge and serve as an IP address to the HMC. Subsequently, the HMC can then contact the server to start in an environment that will allow it to backup and restore data on the HMC, and install or upgrade the code on the HMC over the network.

Attention: To perform a network install, backup, or restore operation on the HMC over the network, the HMC must be shut down and restarted. If you perform an install or restore operation, all data on the HMC hard drive will be lost.

Prerequisites

To perform a network boot of the HMC, be sure you have the following prerequisites:

- A system that has DHCP, NFS and TFTP server installed and running. Linux is suggested and is used in the example that in this appendix. To perform a backup and restore in secure mode, you must also have an SSH server running on the system.
- The system must be network-accessible by the HMC, and be able to communicate with DHCP and TFTP. By default, gateways block DHCP and TFTP access. To reduce such issues, be sure the system and the HMC are connected to the same switch, and that the switch permits DHCP and TFTP.
- The syslinux package must be installed on the system in order to have the `pxelinux.0` boot loader file.
- The required HMC images. Download the files and put them in the locations specified in the instructions.

Server setup

The assumption in this example is that the DHCP/TFTP server resides on a private network and the address of the server is 192.168.1.1. Another assumption is that this server has the authority to give out addresses in the range of 192.168.1.101 to 192.168.1.200.

The following steps describe the setup required on the server to allow an HMC to contact and perform an install, backup, and restore operation over network. The server in these steps is installed with SUSE Linux.

1. Log in as root on the Linux system. Check the configuration file `/etc/xinetd.d/tftp` and look up the `server_args`. The default setting is usually `/var/tftp`.
2. Create the `/var/tftp` directory by running the **`mkdir -p /var/tftp`** command.
3. Edit the `/etc/dhcpd.conf` file by adding the following two lines if they are not already in the file:

   ```
   allow bootp;
   allow booting;
   ```

   A sample `dhcpd.conf` file is shown in Example E-1 on page 589.

Example E-1 A dhcpd.conf file

```
allow bootp;
allow booting;
ddns-update-style none;
default-lease-time 14400;
max-lease-time 172800;
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.100 192.168.1.200;
option router 192.168.1.1;
option domain-name “somecompany.com:;
option domain-name-server 102.168.1.1;
filename “pxelinux.0”;
}
```

This file specifies the range of IP addresses to be served by the DHCP server. That is, one of the IP address in this range is assigned to the HMC when it broadcasts a request to obtain an IP address.

4. The bootloader to use is `pxelinux.0`, which is in the `/var/tftp` directory. This file is part of the `syslinux` package and normally resides in the `/usr/lib/syslinux` directory. Copy this file to the `/var/tftp` directory.
5. Create two directories:

   ```
   /var/tftp/hmc
   /var/tftp/pxelinux.cfg
   ```

6. Download the `bzimage` and `initrd.gz` files, then copy them to the `/var/tftp/hmc` directory. Obtain the files from the HMC support website or from the HMC Recovery media:
   - The `bzImage` file should be under the directory `isolinux/` on the HMC Recovery media.
   - The `initrd.gz` file should be under the directory `images/` on the HMC Recovery media.
7. Create a directory, for example, `/home/hmc`, and then do an NFS export of this directory. To use this directory to back up the HMC over the network, you must allow write access to it.
8. Download the `disk1.img`, `disk2.img`, and `disk3.img` files, then copy them to the `/home/hmc` directory. Obtain them from the HMC support website or from the HMC Recovery media:
   - The `disk1.img` file should be under the `base/` directory on the HMC Recovery media.
   - The `disk2.img` file should be under the `images/` directory on the HMC Recovery media.
   - The `disk3.img` file should be under the `images/` directory on the HMC Recovery media.
9. Create a file named `default` in the `/var/tftp/pxelinux.cfg/` directory, containing the following data:

   ```
   default hmc
   label hmc
      kernel hmc/bzImage
      append initrd=hmc/initrd.gz media=network server=192.168.1.1 dir=/home/hmc
      mode=manual vga=0x317
   ```

   This default configuration file indicates that the `bzImage` kernel file will be loaded from the `/var/tftp/hmc` directory. The parameter passed to the kernel informs the HMC of the following information:

   - To use the `initrd.gz` file in the `/var/tftp/hmc` directory as the RAM disk.
   - The server’s IP address is 192.168.1.1.
   - The `/home/hmc` directory on the server will have the necessary images.

The server is now ready to accept HMC requests.

Installing the HMC over network

After the server is set up, follow these steps to start the HMC using the network adapter as the startup device:

1. Power on the HMC, or if the HMC is currently running, shutdown and restart the HMC by using the **hmcshutdown** command or by exiting the console.
2. When the HMC starts, the following options are displayed:

   ```
   Press F1 for Setup
   Press F12 for Startup Device
   ```

   If the F12 option is not displayed, press F1, and then specify the network interface as one of the startup devices in the BIOS Setup utility, as follows:

   a. From BIOS Setup, find and select Startup or Start Options, and then Startup Sequence to view the list of startup devices.

   b. Depending on the type of HMC, use the plus (+), minus (-), or arrow keys to make the network interface an entry in the startup list, after the hard disk.

   When you finish, save the settings, and then exit the BIOS setup utility to restart the boot process. Continue with the next step.
3. Press the F12 key, and then select the network adapter. The specified network adapter then becomes the startup device for this instance of the boot, while the existing startup device list remains unchanged.

   > **Note:** If you did not press the F12 key in time to select the network adapter, as the startup device, the HMC restarts from the hard disk. If the HMC restarts, data preserved by the Save Upgrade Data task is restored when the HMC completes the boot process and displays the HMC login dialog. Log in and run the Save Upgrade Data task again before starting the upgrade.

4. If you press the F1 key, the BIOS setup menu is invoked. In this mode, you can select the Startup menu, and then follow instructions to permanently change your startup device. *Do not* permanently set the network adapter as a startup device *before* the hard disk.
5. The HMC now broadcasts a request to obtain an IP address, and is given one by the DHCP server.
6. Next, the HMC obtains the `bzImage` and `initrd.gz` files from the TFTP server, and then starts the boot process.
7. The Install/Backup/Restore Wizard panel opens.
8. Select **Install**, and then click **Next** to continue.
9. Select the network interface to install from network. In this example, where there is one server dedicated to provide the network install/backup/restore capability, select the default settings. Selecting **Default** tells the HMC to use the same network interface that originally contacted the server to load the `bzImage` and `initrd.gz` files. If the installation images reside on a different server, you can select another network adapter and configure it in order to obtain the installation images. Click **Next** to continue.
10. The summary panel is displayed. The Remote Directory value should be `/home/hmc`, and the remote host should show the IP address of the server, as specified in the default PXE configuration file. Click **Finish** to start the install process.
11. You will have the option to restore Management Console Data when the installation process completes. The HMC login dialog is displayed after the Management Console Data is restored.

Upgrading the HMC

Follow these steps to upgrade the HMC:

1. Save Upgrade Data to hard drive (see 5.3.8, “Save Upgrade Data” on page 323).

   Wait for the task to complete. If the Save Upgrade Data task fails, contact you next level of support before proceeding.

2. Shut down and restart the HMC by using the **`hmcshutdown`** command or by exiting the console.

3. When the HMC starts, the following options are displayed:

   ```
   Press F1 for Setup
   Press F12 for Startup Device
   ```

   If the F12 option is not displayed, press F1 and then specify the network interface as one of the startup devices in the BIOS Setup utility, as follows:

   a. From BIOS Setup, find and select **Startup** or **Start Options**, and then **Startup Sequence** to view the list of startup devices.

   b. Depending on the type of HMC, use the plus (+), minus (-), or arrow keys to make the network interface an entry in the startup list, *after* the hard disk.

   When you finish, save the settings, and then exit the BIOS setup utility to restart the boot process. At this point, continue with the next step.

4. Press the F12 key, and then select the network adapter. The specified network adapter then becomes the startup device for this instance of the boot, while the existing startup device list remains unchanged.

   Note: If you did not press the F12 key in time to select the network adapter, as the startup device, the HMC restarts from the hard disk. If the HMC restarts, data preserved by the Save Upgrade Data task is restored when the HMC completes the boot process and displays the HMC login dialog. Log in and run the Save Upgrade Data task again before starting the upgrade.

5. If you press the F1 key, the BIOS setup menu is invoked. In this mode, you can select the Startup menu, and then follow instructions to permanently change your startup device. *Do not* permanently set the network adapter as a startup device *before* the hard disk.

6. Next, the HMC obtains the `bzImage` and `initrd.gz` files from the TFTP server, and then starts the boot process.

7. The Install/Backup/Restore Wizard panel is then displayed.

8. Select **Upgrade** and then click **Next** to continue.

9. Select the network interface to use. In this example, where there is one server dedicated to provide the network install/backup/restore capability, select the Default settings. Selecting Default tells the HMC to use the same network interface that originally contacted the server to load the `bzImage` and `initrd.gz` files. If the install images reside on a different server, you can select another network adapter and configure it in order to obtain the install images. Click **Next** to continue.

10. The summary panel is displayed. The Remote Directory value should be `/home/hmc`, and the Remote host should show the IP address of the server, as specified in the default PXE configuration file. Click **Finish** to begin the upgrade process.

11. If upgrade data exists as previously preserved then the data is restored. After upgrade data is restored, the HMC login dialog is displayed.

Automating the process

To perform the network tasks without physically being at the HMC console, follow the steps described in this section.

> **Note:** You will still have to be physically at the HMC console to initially set the network interface as the startup device.

Server setup

Add the following extra two parameters to the append tag in the default PXE configuration file:

```
append initrd=hmc/inited.gz media=network server=192.168.1.1 dir=/home/hmc
mode=auto autocfg=/home/hmc/HMCInstall.cfg vga=0x317
```

- Set the **mode** parameter to **auto** to indicate that you want an unattended mode.
- Set the **autocfg** parameter to indicate the configuration file that will specify other information. The file must be named HMCInstall.cfg and must be in the same directory as specified in the **dir** parameter.

The HmcInstall.cfg file specifications are listed in Table E-1. Values are in Italic, and they are case-sensitive.

Table E-1 HMCInstall.cfg file specifications

Field name	Possible values	Description
optype	*Install*, *Upgrade*, *Backup*, *Restore*	Operation to perform.
media	*network*, *media*	Network access to the images.
interface	*ethX* (where X is 0, 1, 2, or 3)	Network interface used to access images.
protocol	*dhcp*, *static*	Obtain IP address dynamically or statically.
transtype	*nfs*, *ssh*	Non-secure or secure transfer.
host	IP address	IP address of server. Can be a hostname if DNS is specified. However, the full qualified host name should be specified.
xdir	Directory or File name	Directory or Full path of file to backup or restore from.
restore	*yes* or *no*	Optional. Specify no only if you are *not* restoring from a file that was backed up from the exact same machine.
mode	*auto* or *normal*	Indicates auto or normal mode.
ipaddr	IP address of the interface	Specify this *only* if protocol is static.
gateway	IP address of gateway	Specify this *only* if protocol is static.
dns	IP address of Dynamic Name Server	Specify this *only* if protocol is static.
userid	User Name	Specify this *only* if transtype is ssh. This user ID MUST exist on the server specified by the host value.
passwd	Password	Specify this *only* if transtype is ssh.

Preparing the HMC

After the server is set up, follow the steps in this section to prepare the HMC.

If the HMC is currently running, you must first shut down and restart it by using the **hmcshutdown** command or by exiting the console.

When the HMC starts, the following options are displayed:

```
Press F1 for Setup
Press F12 for Startup Device
```

Press F1 to go to Setup. Select **Startup Sequence**, and change the first startup device to be network. Save the settings and exit.

If you are not ready to start your network operation, you can reboot the HMC at this point using the hard disk as the startup device. To do this, you must override the current startup device (which is the network adapter you have just selected), by pressing F12 key when powering on the HMC, and select the hard disk as current startup device. This will start the HMC from hard disk. When you are ready to start the network operation, you can issue the command `hmcshutdown -r -t now`. This will restart the HMC and use the network adapter on the HMC to send out PXE requests.

After the HMC starts, it recognizes that an unattended operation is desired, based on the **mode** and **autocfg** parameters in the default PXE configuration file. Next it will obtain the `HmcInstall.cfg` file from the server and use it to proceed with the operation specified in the file. When the operation finishes, the booting process ends and the HMC login panel is displayed. You will have to change the startup device list and move the network interface to the position after the hard disk at a later time. Otherwise the HMC will always be installed new, when it is rebooted.

Setup on the server when there are multiple HMCs

In an environment with multiple HMCs, each running at a different code level or possessing a different configuration, the best approach sometimes is to have a unique configuration on the server for each HMC to send PXE requests. For example HMC A might choose to contact the server to do automatic backup to System X, while HMC B might choose to contact the same server with user intervention. In addition HMC B has multiple Ethernet adapter cards, requiring it to specify the network interface that is used with the xNIF (`xNETWORK_INTERFACE`) parameter. In this scenario, the server can be set up to specify the PXE configuration files by using the Media Access Control (MAC) address or IP address of each HMC. If you want to use the IP address as a file name, note that it is *not* the IP address of the HMC, but an IP address served by this server. This information can be obtained by looking up the DHCP lease file on the server.

For example, if HMC A is served IP address 192.168.1.21, then you must create a file, `C0A80115`, under the `/tftpboot/pxelinux.cfg` directory. C0A80115 is the hexadecimal value of the IP address without the dot. If you want to use the MAC address instead, and the value is 00025557165A then you must create a file `00-02-55-57-16-5a` under the `/tftpboot/pxelinux.cfg` directory.

The contents of two PXE configuration files are shown in these examples:

- File C0A80115 (HMC A):

```
default hmc
label hmc
   kernel hmc/bzImage
   append initrd=hmc/initrd.gz media=network server=192.168.1.1
   dir=/home/hmc/SQ6 mode=auto autocfg=/home/hmc/HmcInstall.cfg vga=0x317
```

- File C0A80126 (HMC B):

```
default hmx
label hmc
   kernel hmc/bzImage
   append initrd=hmc/initrd.gz media=network server=192.168.1.1
   dir=/home/hmc/mydir mode=manual xNIF=eht1 vga=0x317
```

Using HMC Recovery DVDs to perform network installation

If no PXE, TFTP, or DHCP server is available, there is still an option to startup the HMC from recovery media and contact a remote server that has an NFS server running.

Server setup

For install/upgrade/backup using NFS, these are the steps:

1. Create a `/home/hmc` directory on the server. Export this directory. Write access is required if you want to use this directory for backup.
2. Download the `disk1.img`, `disk2.img`, and `disk3.img` files and copy them to the `/home/hmc` directory. For location of the files see step 9 in "Server setup" on page 588.

Installing the HMC

For installation follow these steps:

1. Insert the first volume of the Recovery DVD set into the HMC's DVD-RAM drive.
2. Shut down and restart the HMC.

   The HMC begins to read the DVD media and starts the boot process.
3. An Install/Backup/Restore wizard is displayed. Select **Install** and then click **Next**.
4. Select the network interface to use, and then click **Next**.
5. Select Static IP address, enter the required information for the HMC network interface, and then click **Next**.
6. Enter the IP address or the host name of the server, For host name, use the fully qualified host name. Next, enter the fully qualified file name for the file, on the remote server, to be used for the process. In this example, the file name is `/home/hmc/<some file name>.tgz`. Click **Next**.
7. A summary panel is displayed. Review this information, and then click **Finish** to start the installation process.

   The HMC continues the boot process after the operation completes, prompts for Management Console Data to be restored, and then displays the HMC login dialog.

Upgrading the HMC

For upgrading, follow these steps:

1. Save the upgrade data to hard drive (see 5.3.8, “Save Upgrade Data” on page 323).

   Wait for the task to complete. If the Save Upgrade Data task fails, contact you next level of support before proceeding.

2. Insert the first volume of the Recovery DVD set into the HMC’s DVD-RAM drive.
3. Shut down and restart the HMC.

   The HMC begins to read the DVD media and starts the boot process.

4. An Install/Backup/Restore wizard is displayed. Select **Upgrade** and then click **Next**.
5. Select the network interface to upgrade from network, and then click **Next**.
6. Select Static IP address, enter the required information for the HMC network interface, and then click **Next**.
7. Enter the IP address or the host name of the server. For hostname, use the fully qualified hostname. Next, enter the fully qualified file name for the file, on the remote server, to be used for the process. In this example, the file name is `/home/hmc/<some file name>.tgz`. Click **Next**.
8. A summary panel is displayed. Review this information, and then click **Finish** to start the upgrade process.

   The HMC continues the boot process after the operation completes, restores previously upgraded data, and then displays the HMC login dialog.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications listed here might be available in softcopy only.

- *IBM Power Systems HMC Implementation and Usage Guide,* SG24-7491
- *IBM Power Systems SR-IOV: Technical Overview and Introduction*, REDP-5065
- *IBM PowerVM Enhancements What is New in 2013,* SG24-8198
- *IBM PowerVM Virtualization Introduction and Configuration,* SG24-7940
- *IBM PowerVM Virtualization Managing and Monitoring,* SG24-7590

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- IBM System Planning Tool

  http://www.ibm.com/systems/support/tools/systemplanningtool/

- IBM Knowledge Center

  http://www.ibm.com/support/knowledgecenter/

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Redbooks

IBM Power Systems HMC Implementation and Usage Guide

SG24-8334-00

ISBN 0738441554

IBM

(1.0” spine)
0.875”<->1.498”
460 <-> 788 pages

SG24-8334-00

ISBN 0738441554

Printed in U.S.A.