HP OpenView Configuration Management OS Manager

for the Windows operating system

Software Version: 5.00

System Administrator Guide

Document Release Date: April 2007

Software Release Date: April 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

Microsoft®, Windows®, and Windows® XP are U.S. registered trademarks of Microsoft Corporation.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

DHTML Calendar

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Table 1 lists new features added for the Configuration Management 5.00 release.

Table 1 New features added for Configuration Management 5.00

Chapter	Version	Changes
All	5.00	General minor changes and fixes. Removed many screen shot images. Began rebranding. Changed Pico to Nano due to licensing. Prerequisites and requirements changed to version 5.00. Clarified the distinction between a device and the ROM object.
Chapter 1	5.00	Added topic Required Infrastructure on page 17.
Chapter 1	5.00	Added topic Platform Support on page 17.
Chapter 1	5.00	Added definition for ROM object in Terminology on page 20.
Chapter 1	5.00	Revised step 2 in Using the CM OS Manager on page 26 to specify that the original product media must be used.
Chapter 3	5.00	Added backup recommendations to Prerequisites on page 34.
Chapter 3	5.00	Added information about creating the CM OS Manager installation media on page 35.

Chapter	Version	Changes
Chapter 3	5.00	In the topic, Installing the CM OS Manager Server on page 36, added steps for entering the Admin User ID and password for the CM Portal.
Chapter 3	5.00	In the topic, Installing the CM OS Manager Server on page 36, removed a note regarding noting the name of DSML_ZONE and replaced it with a new warning about the PORTAL_ZONE attribute.
Chapter 3	5.00	In the topic, Enabling Communication between the CM OS Manager and the CM Configuration Server on page 39, DES encryption was changed to AES.
Chapter 3	5.00	Updated and added attributes in the section To update the edmprof.dat file on page 43.
Chapter 3	5.00	Removed the topic Updating the CM Configuration Server and CM Configuration Server Database.
Chapter 3	5.00	Updated To use the CM Image Preparation Wizard on page 59 and removed references to PowerQuest.
Chapter 3	5.00	Removed the topic Specifying the CM Configuration Server for CM OS Manager administrative tasks.
Chapter 4	5.00	Changed chapter title from Installing and Configuring the Image Preparation Architecture to Preparing and Capturing OS Images and revised content.
Chapter 4	5.00	Revised step 1 in Task 1 - Prepare the Reference Machine on page 52 to specify that you must run the installation from the original product media.
Chapter 4	5.00	Revised To create Sysprep.inf on page 56.
Chapter 6	5.00	Changed title About Machine Discovery to About Discovery on page 76.
Chapter 6	5.00	Added query for Pending Hardware Configuration Selection to Filtering Machines on page 103.
Chapter 6	5.00	Added Selecting HW Configuration for Pending Machines on page 107.
Chapter 6	5.00	Change to Downloading Resources on page 120. This task includes a new text box to specify the RPS port in the UI.

Chapter	Version	Changes
Chapter 6	5.00	Updated Notifying Target devices on page 123.
Chapter 7	5.00	In About Local Service Boot on page 130, removed note referring to the Windows 9.x operating systems.
Chapter 7	5.00	In About Local Service Boot on page 130, removed list of supported platforms.
Chapter 7	5.00	Added an item to Prerequisites on page 131.
Chapter 7	5.00	In Prerequisites on page 131, removed information about updating the CM Configuration Server DB.
Chapter 9	5.00	Added To start the multicast test sender module on page 158.
Chapter 10	5.00	Removed section Restoring from a Local Image and updated Restoring Operating Systems on page 170.
Chapter 11	5.00	Added new chapter for About Double Byte Character Support on page 179.
Chapter 12	5.00	Updated Frequently Asked Questions on page 194.
Appendix A	5.00	Updated AppEvents on page 197. Removed RIM references and combined tables while removing Event Type column.
Appendix C	5.00	Removed appendix Dynamic Maintenance.

Support

You can visit the HP Software support web site at:

www.hp.com/managementsoftware/services

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction

At the end of this chapter, you will:

- Understand the purpose and benefits of the HP OpenView Configuration Management OS Manager (CM OS Manager).
- Know what operating systems are supported.
- Be familiar with the CM OS Manager components.
- Be familiar with key terminology.
- Have a high level understanding of the product architecture.

The HP OpenView Configuration Management OS Manager (CM OS Manager) allows you to use policy-driven, real-time, state-based management to configure and deploy operating systems (OSs). Use the CM OS Manager to install or replace operating systems on a device and maintain the device according to policy. The CM OS Manager ensures the installation of the appropriate operating system based upon the targeted device's capabilities. For example, an image built for a computer with an ACPI BIOS will not be delivered to a computer that lacks an ACPI BIOS.

The CM OS Manager creates images of operating systems that you have prepared on a reference machine or uses the native install media of the operating system. Policy determines the appropriate operating system for a particular target device based upon:

- An asset tag or other unique identifier imbedded in the device's BIOS
- The network segment the device is connected to
- The manufacturer of the device
- The model of the device
- The role of the device plays in your IT infrastructure

Criteria are extensible – you can add to this list.

Benefits of the CM OS Manager

- The CM OS Manager is a fully integrated component of the HP OpenView Configuration Management Solutions, which reduces the learning curve for your administrators.
- The CM OS Manager improves the speed and reliability of OS deployment using policy-based management.
- The CM OS Manager provides increased service levels by maintaining operating system configurations using desired-state management.
- The CM OS Manager reduces IT costs by simplifying and streamlining the OS management process across multiple platforms.

Required Infrastructure

CM OS Manager for Windows is supported on the CM Management Infrastructure for Windows only.

Platform Support

For information about the platforms that are supported in this release, see the release note document that accompanies this release.

CM OS Manager Components

The CM OS Manager consists of the following components:

- **HP OpenView Configuration Management Application Manager (CM Application Manager)** is the CM agent that runs in the operating system of the target device and is used to manage service packs, patches, hot fixes, applications and other content. It also works with the Configuration Management OS Manager Boot Loader and the Configuration Management OS Manager Agent to enable management of the operating system according to policy.
- **Boot Server** is a Windows-based PXE server and TFTP server.

  Open Source PXE Server and TFTP Server are provided "as is" as defined by the Open Source Licensing model. These components are not maintained by HP; HP is not responsible for any defects related to them.

  Open Source PXE Server and TFTP Server are provided for use in two cases:

  - QA\Testing in Pre-Production Environment.
  - Image Capture on isolated Network.

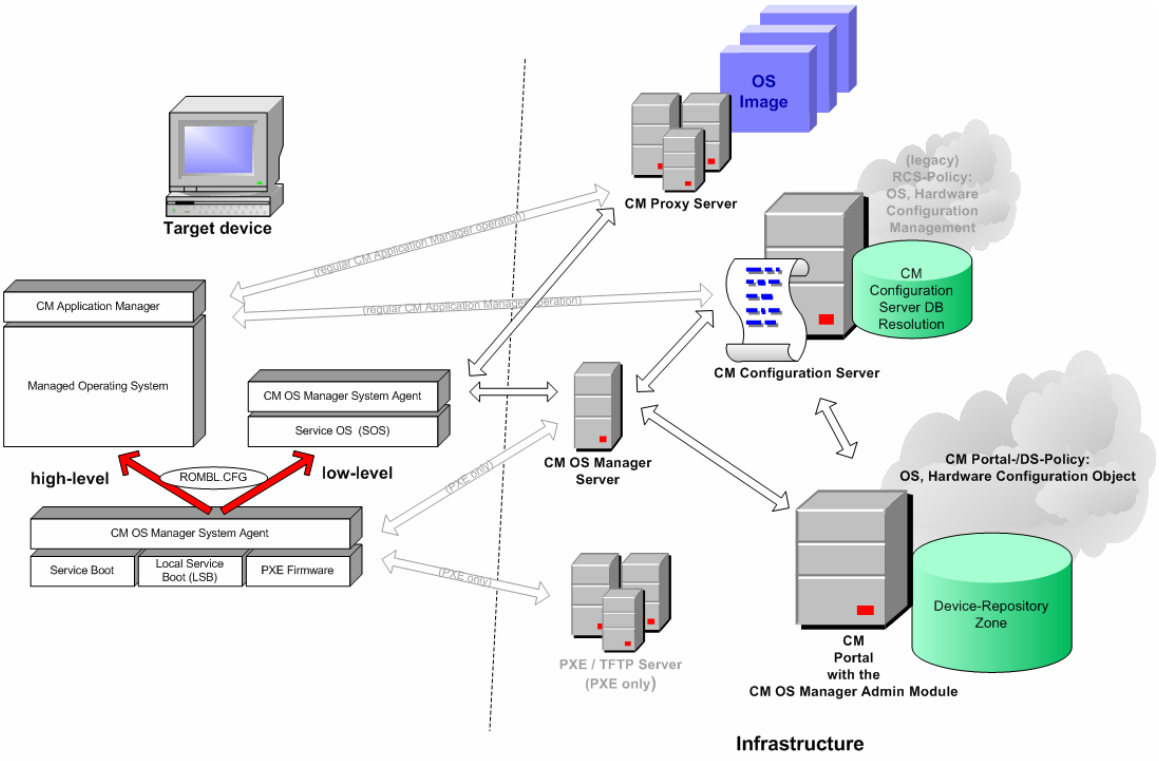
  HP recommends that you work with your network specialists to use the most appropriate PXE and TFTP server based on your network environment constraints.

- **HP OpenView Configuration Management Configuration Server (CM Configuration Server)** provides policy resolution services to determine the desired state of managed devices. The CM OS Manager runs a secondary resolution process against the HP OpenView Configuration Management Portal to determine device specific and external (directory service (DS)) policy. Refer to the *HP OpenView Configuration Management Configuration Server User Guide* on the HP OpenView support web site for more information.
- **HP OpenView Configuration Management Configuration Server Database (CM Configuration Server DB)** can store policy definition or link to an external policy store. The CM Configuration Server DB also contains OS packages for operating system images, supporting master boot record files and partition table files, which have been prepared and published with the HP OpenView Image Preparation Wizard. The CM Configuration Server DB must be updated, as described in this document, to accommodate the CM OS Manager.
- **Local Service Boot (LSB)**
  The Local Service Boot is a typical service, stored in PRIMARY.OS.ZSERVICE, that is deployed by the CM Application Manager to the OS. This service must be deployed to target devices that will use Local Service Boot for OS management.
- **HP OpenView Configuration Management Portal (CM Portal)** stores information about the target devices in your environment. CM OS Manager-specific information is stored in the ROMS object in the target device's object. For general information on how to use the CM Portal refer to the *HP OpenView Configuration Management Portal Installation and Configuration Guide, Version 5.00 for Windows*.
- **HP OpenView Configuration Management Proxy Server (CM Proxy Server)** is an NVDKIT-based web server that serves OS deployment resources (primarily the image files) to the CM OS Manager System Agent. CM Proxy Servers can be strategically located within your network infrastructure to optimize bandwidth utilization. Refer to the *HP OpenView Configuration Management Proxy Server Installation and Configuration Guide* on the HP OpenView support web site.
- **PXE**
  PXE is a network boot technology that initiates the CM OS Manager System Agent over the network.
- **HP OpenView Configuration Management OS Manager System Agent (CM OS Manager System Agent)** is a low-level agent running in the SOS that initiates policy resolution on the CM Configuration

Server through the CM OS Manager Server, and determines which operating systems qualify for installation on the managed device.

- **HP OpenView Configuration Management OS Manager Admin Module (CM OS Manager Admin Module)**
  CM OS Manager Admin Module is the graphical user interface for the CM OS Manager that is accessed through the CM Portal.
- **HP OpenView Configuration Management OS Manager Boot Loader (CM OS Manager Boot Loader)** receives control when the managed device boots from the network via PXE. It then determines how to continue the boot process. It can either continue to boot to a currently in-state operating system located on the managed device's system drive or it can continue the boot procedure by loading the CM OS Manager System Agent from the Boot Server's TFTP server.
- **ROMBL.CFG**
  A configuration file in which the CM OS Manager Boot Loader stores state information. If this file exists on the target device, it indicates that the device is under OS management and a CM agent connect has occurred.
- **HP OpenView Configuration Management OS Manager Server (CM OS Manager Server)** is an NVDKIT-based web server that communicates with the CM Configuration Server through TCP/IP. It mediates between the CM OS Manager and the CM Configuration Server to resolve policy for the correct operating systems for the managed device.
- **Service Boot**
  The Service Boot CD initiates the CM OS Manager System Agent if you encounter a non-PXE, bare-metal, disaster-recovery situation.
- **Service OS (SOS)**
  Boots as an "in memory only" service OS without any dependency on persistent storage configuration or availability.

Figure 1 CM OS Manager Components



Terminology

You should be familiar with the following OS management terms.

bare metal machine

A device that does not have a local OS installed.

Configuration Management agent (CM agent)

The software that runs on a target device and communicates with the CM Configuration Server.

Configuration Management OS Connect (CM OS Connect)

A CM agent connect that is performed for the CM OS Manager. The dname parameter in the Run Once command is set to OS to specify that this connection is being performed for the CM OS Manager.

device object

An object stored in the CM Portal that contains information about a target device.

discovery

The process when a target device boots and communicates with the infrastructure to determine whether a ROM object exists.

gold image

A snapshot of an installed OS, created with the HP OpenView Configuration Management Image Preparation Wizard (CM Image Preparation Wizard). You use the CM OS Manager to deploy a clone of a gold image (referred to as an image) to qualifying target devices.

managed device

A device recognized and managed by the CM OS Manager.

native install

An installation in which an operating system is set up using the standard vendor-provided method. For example, for Windows, the setup program from the Windows distribution media is used to perform the installation. This type of installation can be completely unattended, using `unattend.txt`.

OS state

The actual state of the OS, such as invalid, installed, or desired.

reference machine

A workstation or server used to build the OS image to be cloned.

ROM object

An object that is stored below the device object, which contains information specific to the CM OS Manager.

target device

A workstation or server on which you want to install, replace, or update an OS.

unmanaged OS

A target device that has been discovered by the CM OS Manager, but policy has not assigned an OS for the target device; or policy *is* assigned, however you are not ready to overwrite the existing OS. The current OS for the device is considered unmanaged.

_UNMANAGED_OS_ is also the name of the service in OS.ZSERVICE that is installed by the CM Application Manager on the target device.

About the Product Architecture

CM OS Manager uses several tools to prepare operating system images and then a group of Configuration Management servers to deploy these images to target devices. Its architecture can be divided into three areas – target devices, image preparation and image deployment.

Target Devices

Target devices are machines on which you want to install, replace, or update an operating system.

Image Preparation Architecture

Before preparing an image, you must determine how you want to create the image of your operating system. HP provides two tools from which to choose.

Configuration Management Image Preparation Wizard (CM Image Preparation Wizard)
Use the CM Image Preparation Wizard to prepare a gold image on the reference device. When you run the wizard, it creates an image that is sent to the CM OS Manager's `\upload` directory (by default *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\upload`). Then, you can use the CM Admin Publisher to promote the image to the CM Configuration Server DB.

or

Configuration Management Windows Native Install Packager (CM Windows Native Install Packager)
Use the CM Windows Native Install Packager to create an image of the install media for an operating system on a hard drive on the reference machine. The resulting image has completed the file copy phase of a Windows installation and contains the CM Application Manager. The image is sent to the CM OS Manager's `\upload` directory (by default *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\upload`) and you can use the CM Admin Publisher to promote the image to the CM Configuration Server DB.

See Preparing and Capturing OS Images on page 49.

Then, you can use the CM Administrator Publisher to store the image in the CM Configuration Server DB.

CM Administrator Publisher (CM Admin Publisher)
Use the CM Admin Publisher to store the gold image and its associated files in the CM Configuration Server DB. You can also use the CM Admin Publisher to publish other files, such as override `Sysprep.inf` files or `unattend.txt` files, to the SYSPREP class in the CM Configuration Server DB. See Preparing and Capturing OS Images on page 49.

After publishing the image, you can prepare to deploy the image to your target devices.

Image Deployment Server Architecture

The CM OS Manager's deployment architecture involves a set of servers designed to manage and deploy operating systems for target devices based on a set of criteria. Typically, you will need three server machines.

Machine 1

- DHCP Server

The target device uses a DHCP server to obtain an IP address. You can easily implement CM OS Manager in an existing DHCP-enabled network. There is no need to install additional DHCP servers.

Machine 2

- CM OS Manager Server

It is strongly recommended that you install the CM OS Manager Server on a separate machine from the CM Portal in order to obtain the best performance because both rely on the CM Integration Server. It is always better to have a single server on a machine to avoid networking and performance issues.

- CM Configuration Server
- CM Proxy Server
- CM Portal

You can also install the CM Admin Publisher on this machine.

See Installing and Configuring the Server Architecture on page 33.

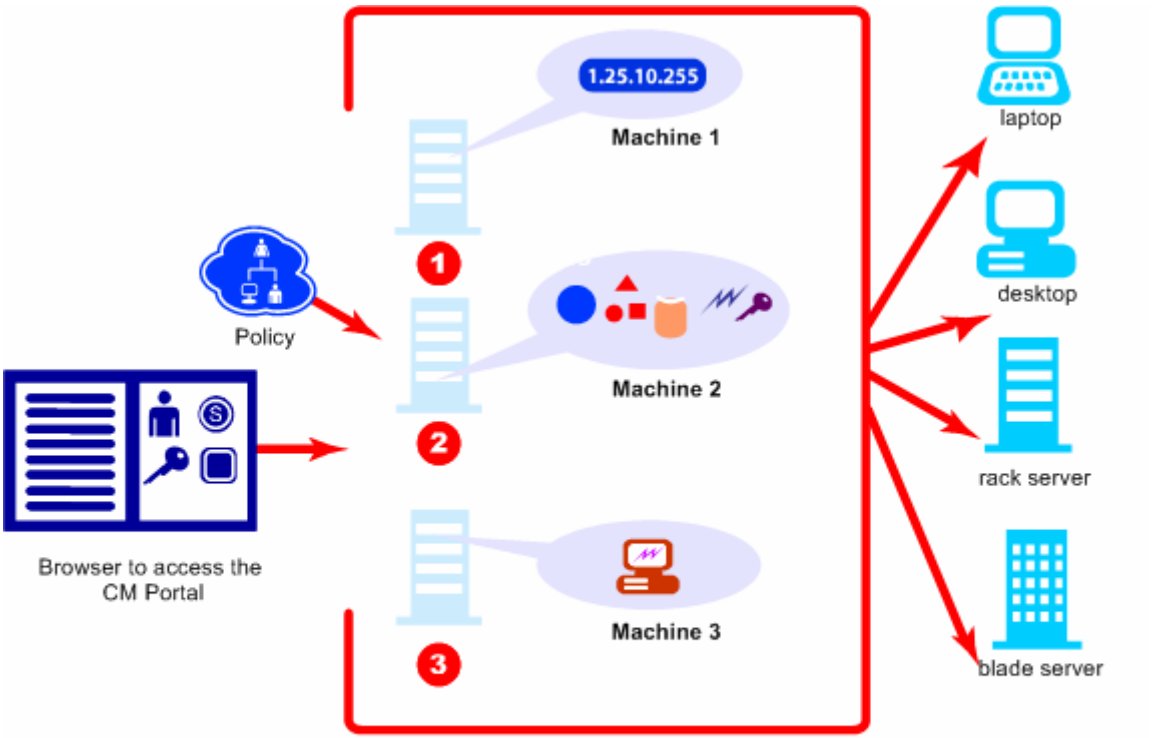
Machine 3

- Boot Server (PXE/TFTP servers)

  Do not install the Boot Server on the same machine as your DHCP server. See About the Boot Server on page 40.

Figure 2 below illustrates the deployment architecture.

Figure 2 Configuration Management OS Manager deployment architecture



Using the CM OS Manager

Below is a simple, high-level description of how you will use the CM OS Manager to deploy operating systems.

1. Decide whether you will use the CM Image Preparation Wizard to create a gold image or the CM Windows Native Install Packager to prepare the image.
2. If you are going to use the CM Image Preparation Wizard to create a gold image, install the operating system from the original product media and the CM Application Manager on the reference machine and perform any necessary customizations.
3. After you create the image, it is stored on the CM OS Manager Server.
4. Use the CM Admin Publisher to publish the image files from the CM OS Manager Server to the CM Configuration Server DB.
5. Use the CM Portal to perform administrative tasks and define policy in preparation for deploying gold images to your target devices.
6. After deploying images to the target devices, use the CM Portal to review the state of your OS deployment.

Chapter Summary

Chapter 2, Target Device Requirements

This chapter describes requirements for your target devices.

Chapter 3, Installing and Configuring the Server Architecture

This chapter describes how to install and configure the various components for operating system management.

Chapter 4, Preparing and Capturing OS Images

This chapter describes how to prepare and capture operating system images to be deployed to devices in your environment.

Chapter 5, Publishing to the CM Configuration Server DB

This chapter describes how to publish your image to the CM Configuration Server DB.

Chapter 6, Operational Overview

This chapter provides information on how to use the CM OS Manager and CM Portal to prepare your operating system (OS) images for deployment to the appropriate target devices.

Chapter 7, Implementing CM OS Manager Server in your Environment

This chapter describes for implementing the CM OS Manager Server in your environment.

Chapter 8, About OS Manager Support for HP Blades

This chapter describes how to assign policy based on enclosures, racks, slots or enclosure configurations.

Chapter 9, About Multicast and the CM OS Manager

This chapter describes how the CM OS Manager supports reliable delivery multicast so that you can rollout large numbers of OS images concurrently with improved performance.

Chapter 10, Advanced Features

This chapter describes several advanced features available with the CM OS Manager.

Chapter 11, About Double Byte Character Support

This chapter discusses the changes made to the CM OS Manager for internationalization.

Chapter 12, Troubleshooting

This chapter provides information about the logs, various tests that you can run and other information used for troubleshooting.

Appendix A, AppEvents

This appendix describes the AppEvents stored in the ROM object.

Appendix B, User Messages

This appendix lists the messages that may be displayed to a user.

Appendix C, Storing Multiple Logs

This appendix describes how to store multiple logs per machine on the CM OS Manager Server.

Related Documents

HP Configuration Management OS Manager Hardware Configuration Management System Administrator Guide

2 Target Device Requirements

At the end of this chapter, you will:

- Be familiar with the requirements for the target devices in your environment.

This chapter describes requirements for your target devices. A target device is a workstation or server on which you want to install, replace, or update an operating system. The following requirements must be met.

- Target devices with existing operating systems should have the CM Application Manager already installed.
- Target devices must meet the minimum hardware and BIOS requirements published by Microsoft (or Windows operating systems) and/or the machine manufacturer for running the operating system to be deployed by the CM OS Manager.
- If you want to report on, or make use of the device's make, manufacturer, and unique identifier for policy, the BIOS must support SMBIOS (for systems management) specification. If a target device lacks SMBIOS support, the only criterion available for specifying policy on that device will be the MAC address.
- Have an English, French, or German keyboard.
- Have 128 MB of RAM or more.
- May have multiple CPUs. CPU must be an Intel 386 or higher, or AMD Athlon or Duron.
- If you are using a network (PXE) boot, you must:
  - Be able to boot from the Boot Server. To do this, make sure that the BIOS is set to boot from the network before the hard drive.
  - Have a network interface card (NIC) that supports PXE, manufactured by Intel or 3Com. Some older network cards are PXE capable, but only actually support PXE with the addition of a network boot ROM. These cards must have the network boot ROM installed. Some older 3Com cards require a firmware upgrade to MBA 4.3 and PXE stack version 2.2.
  - Be sure that the target devices have the same or a compatible HAL (Hardware Abstraction Layer) as the reference device in order to use Microsoft Sysprep. Devices with the same version of HAL.DLL share the same Hardware Abstraction Layer. For more information on determining a device's HAL, see

    http://support.microsoft.com/?kbid=237556.

    If you cannot check the `HAL.DLL`, consider deploying the image on a target device in a lab environment to confirm success of the deployment.

- Match the reference device's ACPI characteristics (i.e., ACPI vs. non-ACPI, which is represented in the HAL) and boot drive interface.
- Be compatible with the programmable interrupt controller capabilities represented in the HAL captured on the reference machine (i.e., an Advanced Programmable Interrupt Controller (APIC) HAL will not run on a device that does not have an APIC; however a PIC (standard on-board Programmable Interrupt Controller) HAL will run on a device that has an APIC). Newer HP/Compaq computers often come with an APIC.
- Support NTFS and FAT32 file systems.

3 Installing and Configuring the Server Architecture

At the end of this chapter, you will:

- Understand the prerequisites for installing and configuring the server architecture.
- Be able to install the CM OS Manager Server.
- Be able to configure the CM Portal.
- Be able to configure the CM Proxy Server.
- Be able to install the Boot Server.

This chapter describes how to install and configure the various components for operating system management.

It is helpful to have your license strings accessible.

Prerequisites

Before installing and configuring these components, you must have a CM Management Infrastructure for Windows set up on a server *with a static IP address* that includes the following:

- HP OpenView Configuration Management Configuration Server for Windows version 5.00 or higher. During the installation, you must have selected the CM OS Manager check box on the Select Products to be installed and supported by CM Configuration Server.

  To check the version of your CM Configuration Server, go to the bin directory and open `version.nvd`.

- HP OpenView Configuration Management Configuration Server Database version 5.00 or higher

  To check the version of your CM Configuration Server DB, use the CM Admin CSDB Editor to view the PRIMARY.SYSTEM.DBVER class. The DBVER attribute specifies the current version of your database.

  To check the version of your CM Configuration Server, go to the bin directory and open `version.nvd`.

- HP OpenView Configuration Management Administrator version 5.00 or higher
- HP OpenView Configuration Management Proxy Server version 5.00 or higher
- HP OpenView Configuration Management Portal for Windows version 5.00 or higher

  The security for the Microsoft Internet Explorer browser must be set no higher than medium.

Before installing the CM OS Manager components in a production environment, be sure to backup the configuration files for the entire CM

infrastructure. Backup the files in the following default locations (and any other \ Program Files\Hewlett-Packard\CM directories under which the CM Integration Server may be installed).

- *SystemDrive*:\ Program Files\Hewlett-Packard\CM\IntegrationServer\etc
- *SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementPortal

  Note that it is recommended that you use the Backup Directory task in the CM Portal to backup operational data that is stored in the CM Portal's OpenLDAP database.
- *SystemDrive*:\ Program Files\Hewlett-Packard\CM\ConfigurationServer\modules
- SystemDrive:\ Program Files\Hewlett-Packard\CM\ConfigurationServer\bin\edmprof.dat

You must create the CM OS Manager installation media from the .iso image stored in the \OS_Manager folder on the Configuration Management 5.00 media.

Installation Checklist

We suggest that you do the installation in the following order:

Table 2 Installation Checklist

- ❑ 1 Install the CM OS Manager Server.
- ❑ 2 (Optional) Enable Communication between the CM OS Manager and the CM Configuration Server
- ❑ 3 Configure the CM Portal.
- ❑ 4 Configure the CM Proxy Server.
- ❑ 5 Install the Boot Server.

Check the HP OpenView support web site for product updates and release notes.

About the CM OS Manager Server

The CM OS Manager Server handles requests for operating system images obtained from the CM Configuration Server. The CM OS Manager Server performs a low level exchange with the CM OS Manager System Agent and the CM OS Manager Boot Loader.

CM OS Manager System Agent
The CM OS Manager System Agent is low-level agent running in the SOS that initiates policy resolution on the CM Configuration Server through the CM OS Manager Server, and determines which operating systems qualify for installation on the managed device.

CM OS Manager Boot Loader
The CM OS Manager Boot Loader receives control when the managed device boots from the network via PXE. It then determines how to continue the boot process. It can either continue to boot to a currently in-state operating system located on the managed device's system drive or it can continue the boot procedure by loading the CM OS Manager System Agent from the Boot Server's TFTP server.

Every time a target device boots, the CM OS Manager Boot Loader connects with the CM OS Manager Server; which then accesses the CM Portal to verify that the device exists. In cases of policy changes or OS reinstallation, the CM OS Manager Boot Loader will load CM OS Manager System Agent, which will perform resolution and manage the operating system.

The CM OS Manager Server is capable of handling large numbers of target devices with modest requirements for disk space and memory. It is well suited to be co-resident with the CM Proxy Server.

System Requirements

- Static IP address and port.
- Must have connectivity to the CM Configuration Server.

Installing the CM OS Manager Server

This section provides instructions for installing the OS Manager Server. Later, you must configure the CM Portal so that you can use the CM OS Manager administrative tasks. See Configuring the CM Portal on page 42.

To install the CM OS Manager Server

If you have already installed a CM-IS product such as the CM Proxy Server, some of the dialog boxes may not appear during this installation and the previously entered information will be used. For example, you may not be asked to provide your license file again.

1. From the CM OS Manager media, go to `\os_manager_server\win32`.
2. Double-click **setup.exe**.

   The Welcome to CM OS Manager Server Setup window opens.
3. Click **Next**.

   The End User License Agreement window opens.
4. Click **Accept**.

   The Installation Directory window opens.
5. Click **Next**.

   The License File window opens.
6. Click **Browse** to navigate to your license file.

   The license file is installed in *SystemDrive*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\modules`.

   To check that your license string is valid, open *SystemDrive*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\logs\ httpd-port.log` and search for "License is expired". If you find this string, you must update your license file. See CM OS Manager Server Logs on page 184 for information about this log.
7. Click **Next**.

   The CM OS Manager Server port window opens.
8. If necessary, type the port for the CM OS Manager server.
9. Click **Next**.

   The CM Configuration Server Location window opens.
10. Specify the address and port for the CM Configuration Server. You may include the company name and domain, but it is not required.
11. Click **Next**.

    The CM Proxy Server Location window opens.

12 Specify the address and port for the CM Proxy Server. You may include the company name and domain, but it is not required.

Do not type **`localhost`** or **`127.0.0.1`** in this field, because the target device will be unable to locate the appropriate server.

The CM Proxy Server can be co-located with the CM Configuration Server. Refer to the *HP OpenView Configuration Management Proxy Server Installation and Configuration Guide* for more information about installing this server and how to co-locate it with the CM Configuration Server.

13 Click **Next**.

The CM Portal Location window opens.

14 Specify the address and port number for the CM Portal. You may include the company name and domain, but it is not required.

15 Click **Next**.

The CM Portal Zone Name window opens.

16 Type the name of the CM Portal Zone.

The Zone name that you enter *must* be the same name that you specified when you installed the CM Configuration Server. If you cannot recall this value, go to `edmprof.dat` in the CM Configuration Server's `bin` directory. Go to the MGR_ROM section and check the value of the PORTAL_ZONE attribute.

The Zone name can be a maximum of 64 characters long using only letters (a-z and A-Z), numbers (0-9) and the space character. It cannot have special characters, such as underscores, commas, or periods.

Refer to the *HP OpenView Configuration Management Portal Installation and Configuration Guide* for information about zones.

17 Click **Next**.

The User ID and Password for CM Portal window opens.

18 Type the User ID for the CM Portal.

19 Type the Password for the CM Portal and then confirm the Password.

20 Click **Next**.

The Select Attribute window opens.

21 Select an attribute to be used to name the ROM object. If you do not make a selection, the default attribute, Computer Name, will be used. This name appears in the CM Portal.

If, during a CM OS Manager Server installation, you select one of the SMBIOS parameters for the ROM object display, these values may not be present or unique on all devices.

- If the value is not present, the machine ID will be used.
- If the value is not unique, multiple devices will be displayed with the same name.

22 Click **Next**.

The Summary window opens.

23 Click **Install** to begin the installation.

24 Click **Finish** when the installation is finished.

If you are using Microsoft Windows Server 2003, when you open the CM Portal, you may be prompted to add it to the Trusted sites zone. Also, in order to ensure that the CM Portal works properly, the Security settings for your browser must be set no higher than medium.

Enabling Communication between the CM OS Manager and the CM Configuration Server

You must perform the following steps to enable communication between the CM OS Manager Server and the CM Configuration Server *if you are using a password to access your CM Configuration Server*.

If you are using a password to access your CM Configuration Server

1 Shut down the HP OVCM Integration Server service.

2 From a command prompt switch to the CM Integration Server installation directory (typically *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer).

3 Type nvdkit and press **ENTER**.

4 Type the following command:

password encrypt *your password* **aes**

your password represents your existing password for your CM Configuration Server DB. This is case sensitive.

Your password will be encrypted and will look something like:

```
<AES256>kITMqDenvFUpdpBaYt8XBg==
```

5 Cut the encrypted password from the nvdkit command line and paste it into *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\roms.cfg as the value for the ADMINPWD entry.

> The equal signs (==) and the literal string <AES256> must be included

6 Restart the HP OVCM Integration Server service.

About the Boot Server

The Boot Server is the Windows-based PXE (Pre-execution environment) and TFTP (Trivial File Transfer Protocol) server for the OS Manager environment. Note that the TFTP daemon is run in secure mode.

> PXE uses DHCP broadcast, multicast, or UDP protocols and receives broadcasts. This means that if broadcast traffic is restricted between subnets, you must place PXE severs in each subnet, enable broadcasts (which may not be an option), or use a DHCP helper function to pass DHCP broadcast traffic. This situation is similar to that of standard DHCP servers and is probably well understood by your network administrator.

The PXE server is a low volume server. The TFTP server volume is slightly higher, but should only be transferring the CM OS Manager Boot Loader (less than 64 KB) on every target device boot and the intermediate Linux Service OS (approximately 11 MB) *only* when a state change is required (i.e., initial discovery, installation, or change of OS). This transfer will *not* occur for devices in desired state. Therefore, a few strategically placed PXE/TFTP servers should be able to support many clients. They should be accessible, however, on a relatively high-speed connection.

> Do *not* configure your DHCP server to preclude the use of the Boot Server.

Pre-requisites

- PXE Client version 2.2 or higher.
- Install the Boot Server on a machine separate from your DHCP server. You must do this because both the PXE server and the DHCP server listen on the same DHCP port by default.
- If you have more than one PXE server in your environment, each server must be on a separate segment and the PXE packets should not pass between segments. You can use the Discover Boot Server utility to determine if there are PXE servers in your environment. See Using the Discover Boot Server Utility on page 195.
- A static IP address for the Boot Server.

  If the CM OS Manager IP address or port is ever changed, then the Boot Server ISVR value and the ISVRPORT value in the Boot Server default file must be updated. The default file is typically located in *SystemDrive*:\Program Files\Hewlett-Packard\CM\BootServer\X86PC\UNDI\linux-boot\linux.cfg directory.

- Remember that target devices must contain a PXE-compliant NIC card and be set to boot from the network. To determine whether a device contains a PXE-compliant NIC card; refer to the card's specifications.

  Enabling PXE in your network environment:

  In some network environments (such as those containing Cisco), the client may fail to PXE boot and you may need to modify the network port configuration. For the Cisco switch, use the following:

  ```
  set port channel off
  set spantree port fast enable
  ```

  For all other vendors, consult their documentation.

Installing the Boot Server

To install the Boot Server

1 On the OS Manager media, go to \boot_server\win32.

2 Double-click `setup.exe`.

3 The Boot Server Setup window opens.

4 Click **Next**.

The Boot Server Root folder window opens.

5 Click **Next** to accept the default directory of *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\bootserver`.

The CM OS Manager Server information window opens.

6 Type the IP address and port number for the CM OS Manager Server. This must be specified in the following format: *`xxx.xxx.xxx.xxx`*`:`*`port`*. You can enter this information even if the CM OS Manager Server is not yet installed or running. This information is written to a configuration file.

7 Click **Next**.

The Summary window opens.

8 Review the installation summary, and then click **Install**.

A window opens to indicate that the Boot Server has been successfully installed.

9 Click **Finish**.

If you want to check that the installation was successful:

- Press **Ctrl + Alt+ Delete**, go to Task Manager, and review the list of processes. `PXE.exe` and `Inetd.exe` should be running.

or

- Go to the Event Viewer and check the application events. You will see when the process starts. Entries for problems will appear soon after the event starts.

Configuring the CM Portal

Make the following changes to configure the CM Portal to support the CM OS Manager.

Be sure that you have the CM Portal 5.00 or higher installed on your machine. Note that the following changes have occurred in the CM Portal 5.00:

- The default port has changed from 3466 to 3471.
- The CM Portal's service has changed to HP OVCM Portal.
- The default location of the CM Portal has changed from *SystemDrive*:\ Program Files\Hewlett-Packard\CM\IntegrationServer\ to C:\Program Files\Hewlett-Packard\CM\ManagementPortal.
- The service name `httpd` has been changed to httpd-managementportal.

To update the modules

1. Stop the HP OVCM Portal service.
2. From the CM OS Manager media, copy the files in the`\os_administrator` folder to the`\ManagementPortal\modules` directory. The default location is *SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementPortal\modules.
3. Restart the HP OVCM Portal service.

To update the `edmprof.dat` file

1. Open `edmprof.dat` in the CM Configuration Server's `bin` directory.
2. In the [MGR ROM] section
   - Set the PORTAL_HOST to point to the IP address for the CM Portal.
   - Set the PORTAL_PORT to point to the port for the CM Portal.
   - The PORTAL_ZONE contains the value that you specified when you installed the CM Configuration Server.
   - Set DISPLAYNAME to the same value as the DISPLAYNAME attribute in *SystemDrive*:\ Program Files\Hewlett-Packard\CM\IntegrationServer\etc\roms.cfg. This ensures that the display name for the device will be updated when the CM OS Manager Server interfaces with CM Portal. If you chose the default during the installation, set this to **compname**.
   - The PORTAL_UID is the ID of a CM Portal user who can update a device or the ROM object.

— The PORTAL_PASS is the password for the CM Portal user who can update a device or the ROM object.

```
*-------------------------------------------------------------------*
* Manager CM OS Manager                                             *
*  PORTAL_HOST  = Host name or IP address for the CM Portal         *
*  PORTAL_PORT  = Port number for the CM Portal                     *
*  PORTAL_ZONE  = Zone name in the CM Portal                        *
*  DISPLAYNAME  = Display name used in the CM Portal for the device *
*  PORTAL_UID   = ID of a CM Portal user who can update a device    *
*                 or the ROM object                                 *
*  PORTAL_PASS  = Password of a CM Portal user who can update       *
*                 a device or the ROM object                        *
*                                                                   *
*  PORTAL_ZONE and DISPLAYNAME parameters should match the ZONE and *
*  DISPLAYNAME parameters in roms.cfg file                          *
*-------------------------------------------------------------------*
```

```
[MGR_ROM]
PORTAL_HOST = 192.168.1.9
PORTAL_PORT = 3471
PORTAL_ZONE = cn=Home,cn=radia
DISPLAYNAME = compname
PORTAL_UID  = romadmin
PORTAL_PASS = secret
```

3 Save and close the `edmprof.dat` file.

Adding a Directory Service

You must define a CM Configuration Server directory service in the CM Portal before you can use the CM OS Manager administrative tasks. You only need to perform these steps one time.

To add the directory service

1 Open your web browser and go to the CM Portal (`http://`*`ipaddressORhostname`*`:3471`).

2 Login as the CM Portal administrator (by default, the user id is `admin` and the password is `secret`).

3 In the workspace, click the appropriate Zone. For detailed information about zones and directory services, refer to the *HP OpenView Configuration Management Portal Installation and Configuration Guide*.

4 In the workspace, go to **Configuration** and click **Directory Services**.

5 From the Model Administration task group, click **Add Directory Service**.

6 From the Type list, select **ds-rcs**.

7 In the URL text box, change the value of `localhost` to the IP address of the CM Configuration Server that you want to use for CM OS Manager administration.

For details on setting the user ID and password for the CM Configuration Server, see the *HP OpenView Configuration Management Portal Installation and Configuration Guide*.

8 If necessary change the Display Name. For example, CM Database.

9 Click **Submit**.

The CM Database is available in Zone, Configuration, Configuration Servers.

10 Log out of the CM Portal.

Assigning CM OS Manager Views to New Users

If you add a new user to the CM OS Manager, you may want to allow the user to have access to the CM OS Manager administrative tasks. To create new users see the *HP OpenView Configuration Management Portal Installation and Configuration Guide*. After the CM OS Manager Views are assigned, the appropriate classes for the CM OS Manager will appear when the user logs in and connects to the CM Configuration Server.

1 Open your web browser and go to the CM Portal **(http://ipaddressORhostname:3471)**.

2 Login as the CM Portal Administrator (by default, the user ID is admin and the password is secret).

3 Click the appropriate Zone.

4 Click **Administrators and Operators**.

5 Click on the OS Manager user to whom you want to assign CM OS Manager Views.

6 In the Group of Tasks, click **Assign OS Manager Views**.

The Modify Person window opens.

7 Click ✓ to confirm that you want to assign ROM Views to this user.

OR

Click ✗ to indicate that you do not want assign ROM Views to this user.

The Properties window opens, showing that the modification is complete.

Configuring the Default Behaviors Instance

You must modify the default Run Once parameter string in the Default Behavior instance to specify the IP address for your CM Configuration Server. If you do not modify this parameter, your target device will not be able to successfully run an CM OS connect. For more information on the Behaviors class, see Setting Behaviors on page 92.

To configure the default Behaviors instance

1 If necessary, log on to the CM Portal as the CM OS Manager administrator. See Logging On on page 82 for more information.

2 In the workspace, click **Configuration**, **Configuration Servers**, and select the appropriate CM Configuration Server.

3 Click **Behavior**.

The Behavior instances appear in the workspace.

4 Click **Defaults**.

5 In the CM OS Manager Administration task group, click **Modify Instance**.

6 In the RunOnce Parameter String change `IP=RCSSERVER` to reference the appropriate CM Configuration Server for your environment.

7 Click **Modify** to save the changes.

Now, the CM OS Manager Server is ready to use CM Portal.

About the CM Proxy Server

The CM Proxy Server is a web server used to deploy the service containing the operating system image to the target devices.

We recommend that you pre-load images on the CM Proxy Server before deploying them to the target devices. Do not download your OS images dynamically because the target devices will experience timeouts indefinitely until the image is downloaded. Where appropriate, separate CM Proxy Servers may be used for applications and OS file serving.

We recommend that you install the CM Proxy Server after installing the OS Manager Server to ensure that the module load statements in the `httpd.rc` file are in the correct order.

If you are prompted to overwrite files during the CM Proxy Server installation, make sure you choose to keep the latest files.

Refer to the *HP OpenView Configuration Management Proxy Server Installation and Configuration Guide* for more information about installing this server and how to co-locate it with the CM Configuration Server.

Configuring the CM Proxy Server

If you wish to deploy operating system images from a CM Configuration Server, you must co-locate a CM Proxy Server with the CM Configuration Server. To do this, make the following changes to the `rps.cfg`, stored by default in *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\etc`:

1. Stop the CM Integration Server service.
2. `Open` *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\etc\rps.cfg.`
3. Change the `-static-root` parameter (which is the source location) to the location of the CM Configuration Server DB (such as `C:/ Program Files/Hewlett-Packard/CM/ConfigurationServer/DB`). Be sure to use forward slashes.
4. Change the `-static-type` parameter from agent to server.
5. Save the file.
6. Restart the CM Integration Server service.

These changes are shown in bold in the excerpt below.

```
rps.cfg example:  (top portion excluded)
rps::init {
    -stager         0
    -stager-port    3461
    -stager-trace   0
    -httpd          1
    -httpd-prefix   "/RESOURCE"
    -static-root    "C:/Program Files/Hewlett-
Packard/CM/ConfigurationServer/DB"
    -static-trace   0
    -static-type    server
```

About the CM Admin Publisher

Use the CM Admin Publisher to publish the operating system image and its associated files, or other files such as `Sysprep.inf` or `Unattend.txt`, to the CM Configuration Server DB. The CM Admin Publisher is part of the HP OpenView Configuration Management Administrator (CM Administrator) and is a prerequisite for configuring the server architecture.

4 Preparing and Capturing OS Images

At the end of this chapter, you will:

- Be able to prepare and capture operating system images.
- Be able to use the CM Image Preparation Wizard.
- Be able to use the CM Windows Native Install Packager.

In this chapter, you will learn how to prepare and capture operating system images to be deployed to devices in your environment. After an image is captured, it is uploaded to the `\upload` directory on the CM OS Manager Server. Next, you must use the CM Admin Publisher to store the image in the CM Configuration Server DB and later you can use the CM OS Manager Admin Module in the CM Portal to deploy the operating systems to qualifying target devices.

Preparation and capture steps vary depending on the type of image you want to create. For specific instructions, see the appropriate section.

- For Creating Windows Images with the CM Image Preparation Wizard see page 51.
- For Creating Windows Images with the CM Windows Native Install Packager see page 63.

Windows OS Images

There are two ways that you can create a Windows OS image.

- **CM Image Preparation Wizard**
  Use the CM Image Preparation Wizard to prepare an operating system image. The advantage is that deploying the operating system image to the target device is quicker because a complete image has been prepared prior to deployment. Using the CM Image Preparation Wizard to prepare your image is especially useful when deploying the image to workstations, because often you want these images to be identical.
- **CM Windows Native Install Packager**
  Use the CM Windows Native Install Packager to publish the *installation media* for the operating system. The installation of the operating system is then automated through the combined use of answer files and policy. Although CM Windows Native Install Packages may take a bit longer to create, the advantages are:
  - — You can use the CM Windows Native Install Packager to prepare your install media image on any device regardless of the hardware configuration because the media only contains the installation files and not an already installed operating system.
  - — You only need to create one install media image for each version of Windows and service pack because you can customize installations through the use of answer files and policy.

— The operating system media image takes up less room on the server and downloads faster when deployed.

Using the CM Windows Native Install Packager to prepare your install media image is especially useful when provisioning servers, which may have varying hardware, configurations, and so forth.

Creating Windows Images with the CM Image Preparation Wizard

Use the CM Image Preparation Wizard to prepare an OS image on a reference machine.

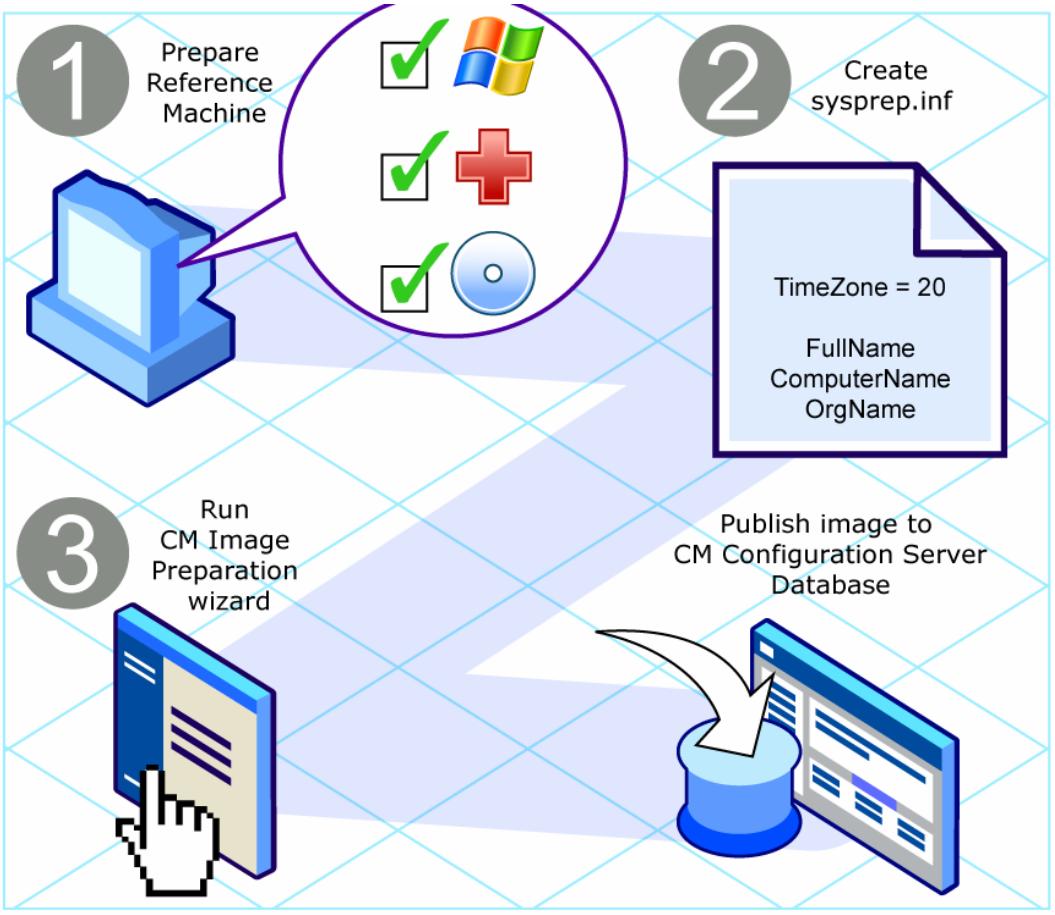
When you run the wizard, it collects inventory information associated with the image, and runs the Microsoft Sysprep utility. The image is sent to the CM OS Manager's `\upload` directory and you can use the CM Admin Publisher on your administrator machine to publish the image to the CM Configuration Server DB.

Images should be sent to a CM OS Manager Server in a non-production lab environment to prevent performance issues.

The following sections explain how to prepare and capture a Windows operating system image:

- Task 1 - Prepare the Reference Machine on page 52.
- Task 2 – Create Sysprep.inf on page 55.
- Task 3 - Run the CM Image Preparation Wizard on page 58.

Figure 3 OS image creation process



Task 1 - Prepare the Reference Machine

The image created on the reference machine (the machine used to create an image of the operating system) is deployed to target devices. Before using the CM Image Preparation Wizard to create the image, do the following:

1 Run the installation from the original product media for the OS on the reference machine. Make sure the reference machine is using DHCP.

The OS must be stored on the C: drive because only the C: drive will be captured.

2 Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service pack for the OS and applications. Be sure to include all required drivers for all device configurations to which you will be deploying the image. The following Microsoft KB article contains information for including OEM drivers for Windows OS installations:

http://support.microsoft.com/default.aspx?scid=kb;en-us;314479

Windows XP images require Service Pack 1 at a minimum.

3 From the CM agent media, install the CM Application Manager 5.00 for Windows with the OS Manager feature. The CM Application Manager is required so that when the OS image is deployed, the device can connect to the CM OS Manager Server.

Additional Recommendations

1 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the CM OS Manager Server is finished.

2 Keep the image file size as small as possible. The ideal configuration would be a partition just large enough to fit the operating system, plus additional space for the CM Application Manager.

HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see Adding Partitions on page 111.

The CM Image Preparation Wizard offers several options to assist in keeping the image file size down as described below.

a If you want to resize the partition to a smaller size, select the Resize partition before OS upload check box.

b If you want to zero free space at the end of the system drive partition, select the appropriate option in the CM Image Preparation Wizard.

This increases the compressibility of the captured image, reducing its size. Smaller image files require less disk space to store and less bandwidth to move across the network.

c **Spanning image files.**
If you want to span your images, select the appropriate option in the CM Image Preparation Wizard. This means that the image file is

broken into smaller segments. Each segment of a spanned image is restricted to 4 GB. This is helpful so that you can comply with the restriction of whole images needing to be less than 4 GB so that they can be stored in the Configuration Server. If you choose not to use the spanned image option, your images must be less than 4 GB.

If you do not plan on having the CM Image Preparation Wizard do this for you, consider:

a **Using the minimum partition size.**
When partitioning the drive on your reference machine for OS installation, use the minimal amount of space required.

- Windows 2000 Professional requires an 800 MB partition for installation.
- Windows 2000 Server requires 1 GB.
- Windows XP with SP1 requires 1.5 GB.
- Windows Server 2003 requires 1.5 GB

The additional disk space required for the CM Application Manager install varies, depending on the OS.

- For Windows 2000, the client requires 50 MB.
- For Windows XP, the client requires 100 MB.
- For Windows 2003, the client requires 50 MB.

b **Disabling hibernation if you are using a laptop.**

c **Making the page file as small as possible while preserving OS performance.**

For Windows XP or Windows 2003, you may want to:

- Turn off System Restore to stop tracking changes.
- Disable the paging file.

For Windows XP Professional with Service Pack 1 and Windows Server 2003, Standard Edition, the page file will be enabled on the target device if the KeepPageFile parameter is set to the default value (null) in the Sysprep file. See **http://support.microsoft.com/?kbid=813138** for more information on KeepPageFile.

- Turn off hibernation. The file is deleted.

For Windows Server 2003 and Windows XP SP1, you can use `powercfg.exe` to turn the hibernation file on from a command line. See **http://support.microsoft.com/default.aspx?scid=kb;en-us;q324347.**

For Windows 2000, you may want to:

- Disable the paging file by setting it to 0.
- Turn off hibernation.

d **Creating free space.**
We recommend that once you have created the smallest partition with the least amount of free disk space as possible, set the ExtendOemPartition = 1 in the [Unattended] section of `Sysprep.inf`, to allow for the small image to be installed on a target device with a much larger drive. When the ExtendOemPartition is set to 1, the Microsoft Mini-Setup Wizard will extend the OS installation partition into any available non-partitioned space that physically follows on the disk. The CM Application Manager can then use the free space on the volume for application installations. See Task 2 – Create Sysprep.inf on page 55.

Task 2 – Create Sysprep.inf

Download Microsoft Sysprep to distribute Microsoft operating systems using cloned images.

Review Microsoft's documentation for information about how to use Sysprep, how to create a `Sysprep.inf`, as well as the available parameters. For information on Microsoft Sysprep for Windows XP and Windows 2000, go to `\support\tools\deploy.cab` on the installation media. `Deploy.cab` contains three help files (`Deploy.chm` contains detailed Sysprep information).

In the last step of gold image creation, the CM Image Preparation Wizard runs Microsoft Sysprep for you. It strips out all of the security identifiers in the gold image and resets the image.

After the operating system image is delivered to the target device, the Microsoft Mini-Wizard will run automatically when the target device is started. After using the answers provided by `Sysprep.inf`, the Microsoft Mini-Wizard deletes the Sysprep directory on the target device.

To set up Sysprep

1. Go to `DEPLOY.CAB` in the `SUPPORT\TOOLS` folder of the Microsoft operating system installation media. See Microsoft's documentation for details.
2. Extract the Microsoft Sysprep files from the Deploy.cab file using the appropriate operating system media. Copy these files to `C:\SysPrep` on the reference machine and make sure the directory and files are not set to read-only.

   Be sure that you are using Sysprep version 5.02195.2104r or higher. If you use an older version, you may receive the following error:

   ```
   Invalid Sysprep version error. Please install Sysprep
   version 5.02195.2104r and re-run the Wizard. Click OK
   to terminate.
   ```

   If you do not have the appropriate version of Sysprep, you can download it from the Microsoft web site.

   Even if you have administrator rights, make sure that you have the appropriate user rights set to run Sysprep. See the article *#270032 "User Rights Required to Run the Sysprep.exe Program"* on the Microsoft web site. If you do not have the appropriate user rights, when Sysprep runs, you will receive the following error:

   ```
   You must be an administrator to run this
   application.
   ```

   The CM Image Preparation Wizard will exit and once you set up the appropriate user rights you will need to run the wizard again.
3. Be sure that the reference machine is part of a WORKGROUP and not a domain in order to use the Microsoft Sysprep.
4. Create a `Sysprep.inf` and save it to `C:\Sysprep`.

To create Sysprep.inf

The `Sysprep.inf` file can be delivered with the operating system image or it can be delivered as a package that is connected to the operating system image (known as an override sysprep file). If the sysprep.inf file is published separately, it will be merged with the Sysprep.inf file in the image's NTFS into a single, combined sysprep.inf.

`Sysprep.inf` files are prioritized in the following order, from lowest to highest:

1. Sysprep embedded in the image (lowest priority). If there is no separately published sysprep.inf (override sysprep), just the sysprep.inf in the image will be used.
2. Override Sysprep (a Sysprep file that is separate from the gold image. See Connecting a Sysprep File on page 117 for details).

   Only one override `Sysprep.inf` will be resolved.

3. Sysprep attached to policy criteria (highest priority).

   To attach a Sysprep file to policy, you must publish the Sysprep file to the CM Configuration Server DB and then use the CM Admin CSDB Editor to manually connect the Sysprep instance to the appropriate Policy instance.

   Even if you override the Sysprep.inf, the ComputerName (COMPNAME) and JoinDomain (COMPDOMN) are still updated by the CM OS Manager based on the Computer Name and Domain stored in the CM Portal device repository.

Either way, you must create the file. You can create the file manually or use the Microsoft Setup Manager (`Setupmgr.exe`) to create Sysprep files. The Setup Manager can be found in the `Deploy.cab` file in the `SUPPORT\TOOLS` folder of a Microsoft OS distribution media. See Microsoft's documentation for more information.

Sample `Sysprep.inf` files are available on the CM OS Manager product media in `\samples\sysprep\`.

The `Sysprep.inf` file should not be greater than 800 KB in size.

Below are a few tips to consider when creating the `Sysprep.inf` file:

- Adjust the TimeZone value for your enterprise.
- Set up the AdminPassword.
- Make sure to include a product key so that the user will not need to enter this at the target device.
- In order to have an unattended installation, you must include UnattendMode = FullUnattended in the [Unattended] section.
- Set ExtendOemPartition to 1, so that Microsoft Sysprep will extend the OS partition into any available non-partitioned space that physically follows on the disk.

- If JoinDomain is present in `Sysprep.inf`, then `Sysprep.inf` has to have the Admin User ID and Password of an account in the domain that has the rights to join the computer to the domain. Note that JoinDomain is case sensitive.
- ComputerName is also case sensitive.

Task 3 - Run the CM Image Preparation Wizard

The CM Image Preparation Wizard performs the following tasks:

1. Checks if there is enough free disk space on the device and verifies that the CM Application Manager is installed. See Task 1 - Prepare the Reference Machine on page 52. If there is not enough free disk space, the CM Image Preparation Wizard displays a message and terminates.
2. Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
3. Runs Microsoft Sysprep on supported operating systems (e.g., Windows XPe does not support Sysprep).
4. Restarts the reference machine into the Service OS (booted from the CM OS Manager media). The Linux-based portion of the CM Image Preparation Wizard runs to collect the image and its associated files.
5. Creates and copies the following files to *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\IntegrationServer\UPLOAD` on the CM OS Manager Server.

   — `ImageName.IMG`
   This file contains the gold image. This is a compressed, sector-by-sector copy of the boot partition from the hard drive system that may be very large. The file contains an embedded file system that will be accessible when the image is installed.

   — `ImageName.MBR`
   This file contains the master boot record file of the reference machine.

   — `ImageName.PAR`
   The file contains the partition table file of the reference machine.

   — `ImageName.EDM`
   This file contains the object containing inventory information.

While these files are transferred, network speed will be less than optimal as the operating system image is compressed during transfer.

A comprehensive log (*machineID*.log) is also available in *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer\UPLOAD after the image is deployed.

To use the CM Image Preparation Wizard

Before continuing, set the reference machine to boot from the CD-ROM drive. You must do this because the CM Image Preparation Wizard CD-ROM is bootable. When you run the CM Image Preparation Wizard, it reboots the device to the memory-resident Linux environment that boots from the CD-ROM in order to capture the image.

1. Insert the CM OS Manager media into the reference machine.
2. Go to \os_manager_image_preparation_wizard\win32 and double-click **prepwiz.exe**. The CM Image Preparation Wizard verifies that the C:\Sysprep folder exists and that CM Application Manager is installed before continuing.

   The CM Image Preparation Wizard opens.
3. Click **Next**.

   The End User License Agreement window opens.
4. Click **Accept**.

   The Identify the CM OS Manager Server window opens.
5. Type the IP address or host name and port for the CM OS Manager Server. This must be specified in the following format: *xxx.xxx.xxx.xxx*:*port*. The CM OS Manager Server port reserved for OS imaging is 3466.

   If the CM Image Preparation Wizard cannot connect to the CM OS Manager Server, a message opens and you must:

   — Click **Yes** to continue anyway.

   — Click **No** to modify the host name or IP address.

   — Click **Cancel** to exit the CM Image Preparation Wizard.
6. Click **Next**.

The Image Name window opens.

7 Type a name for the image file. This is the image name that will be stored in the `/upload` directory on the CM OS Manager Server.

8 Click **Next**.

The Span Disk Image window opens.

9 Type the amount of the total uncompressed disk space (in MB) to use for each image file. Type `0` (zero) if you do not want to create a spanned image.

Use spanned images to break the image file into smaller segments. This is helpful so that you do not have to be concerned with your images being less than 4 GB so that they can be stored in the Configuration Server. If you choose not to use the spanned image option (by typing zero) your images must be less than 4 GB.

10 Click **Next**.

A window opens so you can enter a description for the image.

11 Type a description for the image file.

12 Click **Next.**

The Options window opens.

If you do not have the CM Application Manager installed, you will not see the **Perform client connect after OS install** check box. However, please remember that it is important to have this agent installed.

13 Select the appropriate options.

— **Build Mass Storage Section in Sysprep.inf**.
Select this check box to build a list of the Mass Storage drivers in the [SysprepMassStorage] section of the `Sysprep.inf` for Windows 2000 and above.

The list of Mass Storage Drivers is installed in the registry. This takes about 15-20 minutes, but provides fundamental mass storage device drivers to ensure success of image deployment across machine models and manufacturers.

If there are any errors in these entries, subsequent Sysprep execution can fail.

— **Optimize compression of unused disk space**
Select this check box to optimize compression of unused disk space.

This adds zeroes up to the end of the disk. Note that this may take some time depending on the size of the hard drive.

— **Resize partition before OS upload**
Select this check box to resize the partition to make it as small as possible. If you do not select this check box, make sure that your partition is sized appropriately. See Using the minimum partition size on page 54.

— **Perform client connect after OS install**
Select this check box to connect to the CM OS Manager Server after the OS is installed. If this is not selected, the CM OS connect will not occur after the OS is installed.

14 Click **Next**.

The Summary window opens.

15 Click **Start**.

16 Click **Finish**.

If you are working with an APIC device, the Make image compatible with PIC window opens.

17 If necessary, select the **Make image compatible with machine with PIC** check box.

Microsoft does not recommend this. Be sure to see their web site for more information before making this selection.

18 Click **Next**.

If you selected the check box in the figure above, the Select Windows CD window opens.

19 Browse to the Windows CD-ROM.

20 Click **Next**.

Click **Finish** to run Sysprep. The CM Image Preparation Wizard will start Sysprep; this can take 15-20 minutes to complete. Sysprep will reboot the device when complete. Click **OK** to restart the device.

If you are using Windows 2000, Sysprep may take some time to run even if you don't see any activity on the screen.

After Sysprep restarts, the image must be uploaded to the server.

- If your device has a CD-ROM and the CM OS Manager media is loaded, the device will boot to the CD-ROM.

When the device restarts, you will notice that the screen says Fedora Core and looks similar to the following:

```
To specify options manually, type sos opt1=xxx
opt2=xxx enter
Some quick boot specifications with preset options
are
SOS for PREPWIZ or ROMA, default after a few seconds
TESTMODE - TESTMODE=1
DEBUG - runs in debug mode, SOSDEBUG=1 (no drivers
loaded)
```

Wait a few seconds to continue or press **Enter**, causing the device to boot.

The options mentioned on screen should typically be used only if instructed by Technical Support.

- If your device does not have a CD-ROM, you must have a PXE environment and the device must be set to boot from the network first. Then, during the network boot you can press **F5** on your keyboard to capture the image using PXE. A menu appears and you must select Remote Boot Linux (Image Upload).

Then, the device will connect to the network, and store the gold image on the CM OS Manager Server.

The upload of the gold image may seem to take a long time. However, it is not the upload that is taking a long time, but rather the compression of the image and the optimization for compression of the unused disk space (especially if there is a lot of free disk space). This happens during the transfer of the image and therefore, the network pipe is not a bottleneck. Transfer speeds will be approximately 30-400 Kbps but may vary depending upon processor speeds and your network environment.

You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

The CM Image Preparation Wizard connects to the network, and stores the image on the CM OS Manager Server in the `/upload` directory.

When the upload process is complete, you will see the following message:

```
**** OS image was successfully sent to the CM OS Manager
Server.
```

Next, you will want to publish your image to the CM Configuration Server DB. See Chapter 5, Publishing to the CM Configuration Server DB.

Creating Windows Images with the CM Windows Native Install Packager

Use the CM Windows Native Install Packager to prepare an image of the installation media for an operating system on a hard drive on the reference machine. The resulting image has completed the file copy phase of a Windows installation and contains the CM Application Manager source. The image is sent to the CM OS Manager's `\upload` directory and then you will use the CM Admin Publisher to publish the image to the CM Configuration Server DB.

When the image is deployed to a target device, the target device reboots and the Windows Native Install setup continues with the text mode setup phase, followed by the GUI phase. These two phases are controlled by `Unattend.txt`, and allow for a completely unattended setup.

The following sections explain how to prepare and capture a Windows operating system image:

Task 1 – Prepare the Reference Machine

The image of the original installation media created on the reference machine is deployed to target devices. Before using the CM Windows Native Install Packager to create the image, ensure that you have the CM OS Manager media and that the reference machine meets the following requirements:

1 Connectivity to a CM OS Manager Server.

2 A target drive, recommended being on an extended partition, that:

— Will be used as if the target drive is currently formatted and empty (has no data). If the target drive is not formatted or it is formatted and contains data, the user will be prompted to format the drive.

— A user can pre-format the drive with FAT32 if they format the drive and ensure that there is no data on the drive.

Note that FAT32 cannot be expanded once deployed. NTFS can be expanded and is the default.

— Is at least 1.5 GB. If the target drive is larger, it will take more processing time when the drive is imaged or the image may be larger than necessary depending on how the "Optimize Compression of Unused Disk Space" check box is set in the CM Image Preparation Wizard.

All data on the target drive will be lost.

3 A separate drive (to increase speed), such as the C: drive, with the CM Windows Native Install Packager software already installed. See Task 3 - Install the CM Windows Native Install Packager on page 66.

4 You must also have access to the following items; specify their location when using the CM Windows Native Install Packager:

— The setup files for the CM Application Manager.

— The i386 directory from your operating system media.
You can slipstream any necessary service packs into this directory. See the `readme.txt` file associated with each service pack for more information about how to do this.

Windows setup will not let you run the setup for an older version of Windows. For example:

- If your device is running Windows XP, you cannot use the i386 directory for Windows 2000
- If your device is running Windows 2003, you cannot use the i386 directory for Windows 2000 or Windows XP.

— `Unattend.txt`
You can create the file manually or use Windows Setup Manager on your Windows media. Sample files are available on the product media in `\samples`.

Task 2 – Create Unattend.txt

`Unattend.txt` automates the installation of the OS so that no user input is necessary. The `unattend.txt` file *must* match the release of Windows specified in the i386 directory. These files may vary slightly depending on the version of Windows being installed.

The `Unattend.txt` file should not be larger than 800 KB.

The following are some tips about creating the `unattend.txt` file to be stored with the image:

- The settings in the file should be as generic as possible so that the file can be used with any device in your environment.
- Include the statements AutoLogon=YES and AutoLogonCount=1 in the [GuiRunOnce] section of this file.

  You must use the [GuiUnattended] section, rather than `$OEM$\cmdlines.txt`, because the CM Application Manager setup uses Windows installer to install the CM Application Manager on the target device and `$OEM$\cmdlines.txt` cannot run the Windows Installer. The AutoLogon and AutoLogonCount statements ensure that the CM Application Manager is installed during the first user logon after the operating system is installed.
- Include the statement Extendoempartition=1 in the [Unattended] section of this file. This causes Windows to extend the file system and partition to include any unused space that follows the partition. If the target partition is too small, it is possible that the copy phase of the installation will work (the phase run on the reference machine), but when the image is deployed the text mode phase will fail or install the OS on some other partition.

  If you use a large target partition, the process that zeroes unused space on the file runs for a long time.
- You can also create separate `unattend.txt` files for any necessary customizations. You can use the CM Admin Publisher to publish these files to the SYSPREP class in the CM Configuration Server DB and then you can connect them to the appropriate OS image. Use the Connect Sysprep File task in the CM OS Manager Administration task group. When the image is deployed, the customized unattend.txt will be merged with the original file.

See Using the CM Admin Publisher on page 72 for information about the CM Admin Publisher. When publishing `Unattend.txt` files, follow the instructions as if you were publishing a `Sysprep.inf` file.

Task 3 - Install the CM Windows Native Install Packager

1. On the product media, go to `\windows_native_install\win32` and double-click **setup.exe**.

   The Welcome window opens.

2. Click **Next**.

   The End User License Agreement window opens.

3. Review the terms and click **Accept**.

   The Directory to install the product window opens.

4. Select the appropriate directory and then click **Next**.

   The Summary window opens.

5. Click **Install**.

When the installation is done, click **Finish**.

Task 4 - Run the CM Windows Native Install Packager

To run the CM Windows Native Install Packager

1. Double-click the CM Windows Native Install Packager icon on the desktop.

   The Configure Options window opens.

   You must complete the information on each of the three windows – CM, Windows Setup, and Package.

   a. The CM area contains options used to set up options related to CM products.

   b. The Windows Setup area gathers information needed to perform the OS installation.

   c. The Package area gathers information needed by CM about the package that you are creating.

If you click **Next** before completing the required fields on each of these windows, you will receive a message prompting you to complete the fields.

2 In the CM Client Source Directory field, enter the path for the CM Application Manager.

3 Select the check boxes for the CM products that you want installed.

4 Select the Run first connect after install check box to perform a CM OS connect after the OS is installed. If this is not selected, the CM OS connect will not occur automatically after the OS is installed.

5 In the Optional Packager Command Line Arguments box, type parameters to be used by the WNI application. The options can be placed all on one line or on several lines. Specify the options in the keyword-value format, such as

```
-trace_level  9
```

The keyword must always begin with a dash (-).

Usually you will use the Optional Packager Command Line Arguments text box only when directed by Technical Support.

There are many parameters that can be used to create logs. The following example describes how to create a file called `C:\temp\nvdwni.log`.

- `-trace_level  99`
- `-trace_dir  c:\temp`

If you want to create a log with a different name, you can use the following:

- `-trace_file filename.log`

6 Click **Next**.

The Windows Setup window opens.

7 In the **unattend.txt File** box, browse to the appropriate `unattend.txt` file.

Select a generic `unattend.txt` file to be stored in the image. This file should contain options that are applicable for all devices that the image may be applied to. Later, you can attach a separate unattend.txt file to the image to make any necessary customizations.

The `Unattend.txt` file must match the release of Windows specified in the i386 directory. These files may vary slightly depending on the version of Windows being installed.

8 In the i386 Directory text box, select the Windows source distribution directory provided by Microsoft on its distribution media. You can use the Microsoft slipstream process to incorporate service packs and other fixes. See the `readme.txt` file associated with the service pack for more information about how to do this.

Be sure to copy the i386 from the Windows CD-ROM to another location. If you use the CD-ROM, Windows setup assumes you will have the CD-ROM loaded on the target device and will not copy all of the necessary files.

9 In the Target drive drop-down list, select the drive where the native install package will be created. We recommend that this drive is on an extended partition.

All existing data found on this drive will be lost.

10 In the Extra Command Line Parameters text box, type any parameters that you want to pass to the Windows Setup program when it is run. See the Microsoft web site for more information about the parameters.

11 Click **Next**.

The Package window opens.

12 In the Image Name text box, type the name of the package that will be stored in the `\upload` directory on the CM OS Manager Server. This name has a maximum length of eight characters and should be composed of alphanumeric characters only.

13 In the Image Description text box, type a description of the image (up to 255 characters).

14 In the CM OS Manager Server text box, specify the IP address or host name for the CM OS Manager Server where the image should be uploaded.

15 In the CM OS Manager Port text box, specify the port for the CM OS Manager Server.

16 Select the Optimize Compression of Unused Disk Space check box to null all unused disk space on the target drive before imaging it. This reduces

the size of the image but causes the CM Image Preparation Wizard to run longer.

17 Click **Next**.

18 Review the Summary and then click **Create**.

After you click **Create on a Windows 2000 machine**, Windows Setup may prompt you to reboot the system. Click **Cancel** to avoid the reboot. The reboot is not necessary; however nothing will be harmed if the reboot does happen.

Windows Setup runs and then returns to the CM Windows Native Install Package.

19 When the CM Windows Native Install Package is done, a message prompts you to reboot using the Linux CD-ROM. This refers to the CM OS Manager media.

Remember the boot order must be set to boot from the CD-ROM first.

20 Insert the CM OS Manager media, and then click **OK**.

21 Click **Finish**.

22 Reboot the device and the image is uploaded to your CM OS Manager Server's `\upload` directory.

23 When a message appears that the OS Image has been successfully sent to the CM OS Manager Server, you can remove the media from the drive and reboot your device.

Next, you must use the CM Admin Publisher to publish the image to the CM Configuration Server DB.

5 Publishing to the CM Configuration Server DB

At the end of this chapter, you will:

- Be able to use the CM Admin Publisher to publish your operating system image to the CM Configuration Server DB.

After you have created your image, you must use the CM Admin Publisher to publish it to the CM Configuration Server DB.

Publishing is an administrative task that should be done in a non-production lab environment.

For more information about the CM Admin Publisher, see the *CM Admin Publisher Guide*.

Using the CM Admin Publisher

To use the CM Admin Publisher

1. Double-click the CM Admin Publisher icon on your desktop.

   The Logon screen opens.

2. In the User ID text box, type your CM Administrator user ID.
3. In the Password text box, type your CM Administrator password.
4. From the Type of data to Publish drop-down list, select OS Image if you are publishing an operating system image, `Sysprep.inf` file, or `Unattend.txt` file.
5. Click **OK**.

   The Select window opens.

6. Use the Select window to find and select the file you want to publish (typically stored in the `\upload` directory on the CM Integration Server). Only supported file types appear in the window.

   If you select a `sysprep.inf` file or a `unattended.txt` file, a field appears where you must type the instance name. When you click Next, you will skip directly to the final step because you will not be creating a service for these files. Sysprep and unattended text files are published to the SYSPREP class in the OS domain of the CM Configuration Server DB. Use the CM Portal to view your published instances and then connect them to the appropriate OSs.

7. Use the information in the Description box to verify that you have selected the correct file before you continue. You can also add information to the description if you choose.

8 Click **Next**.

The Configure – Package Information window opens.

9 Use the Package Information section to enter the CM package information. Note that the Limit package to systems with section is not available when publishing OS images.

10 Click **Next**.

The Configure – Service Information window opens.

11 Select **Create new**.

12 Enter the appropriate information in the rest of the fields.

13 In the Assignment type group box, select whether the service is mandatory or optional. By default, Mandatory is selected, which will distribute this service to all available subscribers.

Optional services are only available if you are using the CM Application Self-service Manager. Refer to the *CM Application Manager Guide* or the *CM Application Self-service Manager Guide* for more information about mandatory versus optional services.

14 Click **Next**.

The Publish window opens.

15 Review the Summary section to verify the package and service information you provided during the previous steps. When you are satisfied, click **Publish**.

16 Click **Finish** to exit the CM Admin Publisher.

Use the CM Portal to view your service. In the image below, the new service is V22_W2K.

Remember, Sysprep files are published to the SYSPREP class in the OS domain of the CM Configuration Server DB. Use the CM Portal to view your published Sysprep files.

6 Operational Overview

At the end of this chapter, you will:

- Understand how a target device is discovered.
- Understand how to bring a device to its desired state.
- Understand the policy classes used for OS management.
- Understand how to determine policy assignments.
- Understand how to handle ambiguities in policy resolution.
- Use the CM OS Manager Admin module to prepare and deploy operating systems to target devices.

This chapter provides information on how to use the CM OS Manager and CM Portal to prepare your operating system (OS) images for deployment to the appropriate target devices. The OS Manager allows for OS installations on bare metal devices, migration of existing OSs, and disaster recovery of devices.

About Discovery

When a target device boots, it communicates with the CM OS Manager Server to determine whether a ROM object exists. This process is called **discovery**. If a ROM object does not exist, one will be created the first time the target device communicates with the CM OS Manager Server. After a ROM object is established in the CM Portal, the CM OS Manager Server and the target device can communicate. Use the CM Portal to view the ROM object, which is stored below the target device in the Devices container. See About the CM OS Manager Administration Classes on page 82.

If a ROM object *does* exist, what happens depends on several factors, such as whether the device has an OS installed, how policy is defined and so on. The following table provides several scenarios and the results that you can expect under varying conditions.

In order to implement any changes to your operating system based on policy, a CM OS agent connect must run before the target device reboots.

Table 3 Expected Results on target device

If the target device...	then...
is a bare metal machine and no policy is assigned	nothing will happen until policy is assigned. Note: The default behavior is to prompt the user for workstation or role. However, if no policy is assigned, no OS can be installed. The user will be informed of this and instructed to press **Enter**. The device shuts down.
is a bare metal machine and policy is assigned	the appropriate OS is installed, a ROM object is created and the device is considered to be under CM management.

If the target device...	then...
has an OS that was not installed by the CM OS Manager and no policy is assigned	the CM OS Manager discovers the device but considers it *unmanaged* and a ROM object is created; however, the installed OS remains on the machine.
has an OS that was not installed by the CM OS Manager and the CM OS Manager User Agent, and policy is defined	after the next CM OS agent connect a ROM object will be created. The behavior settings will determine how and when the installation will take place (e.g., whether the resolved OS is installed or not, whether a user is prompted or not).
has a corrupted partition table and PMDISCRV=_CONFIRM_	the target device shuts down so that the administrator can recover data from the target device.
has a corrupted partition table and PMDISCRV=_AUTO_	the appropriate OS is re-installed.

After devices are under CM management, the OS will be changed if a device is not in the desired state. A device may not be in the desired state due to one of the following issues:

- There is a change in policy.
  When policy is modified, the current OS on a device may no longer be applicable. In other words, the list of OS services returned as a result of policy resolution does not include the currently installed OS. This will trigger installation of an OS so that the device's OS is in the desired state.

  You typically use policy to manage your OSs.

  An example of this occurs during an upgrade where the desired OS changes from Windows 2000 to Windows XP.
- It doesn't have a local OS (bare metal).
- There is administrator intervention.
  In some cases, you may wish to install an OS regardless of what is currently on the device e.g., when a device has a corrupted local hard drive which can no longer successfully boot the local OS.

About Policy

The CM OS Manager introduces several policy classes — machine manufacturers (MANUFACT), machine models (MODEL), machine roles (ROLE), and machine subnets (SUBNET)—which are resolved in the following order: ROLE, MANUFACTURER, MODEL, SUBNET. *This order is subject to change.* See Determining Policy Assignments below for important information about implementing policy,

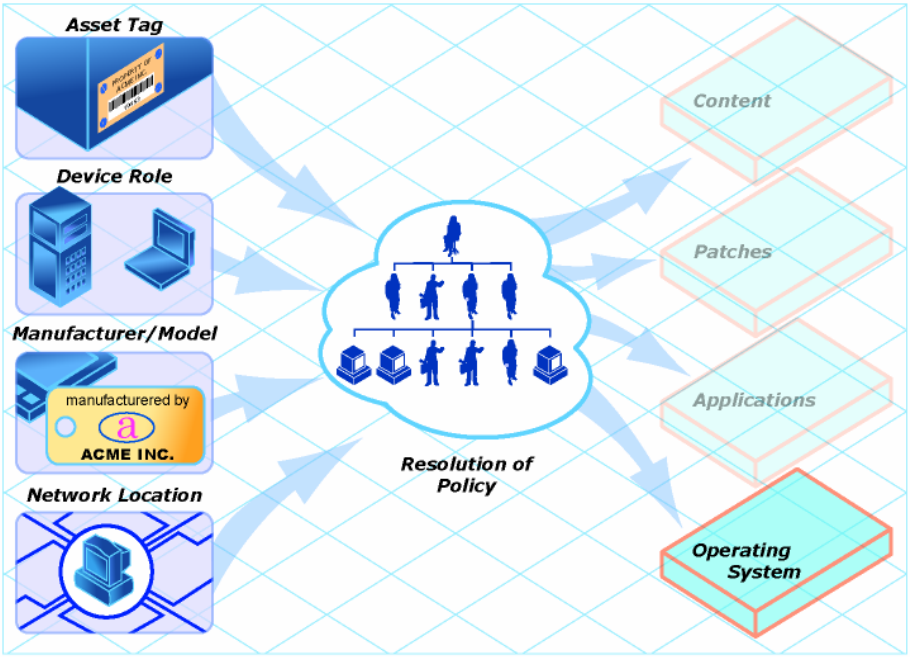
Manufacturer, model, and subnet are based on attributes related to a device. Role is *not* based on a device's attributes. It is simply a grouping of devices, similar to how you might assign policy based on departments. You can set policy based on a device's assigned role—such as server or workstation.

Role is the only criterion that you can use to allow a user to determine the OS that is installed on the device. Note that to allow a user selection of an OS, you need to set the system behaviors accordingly (see Setting Behaviors on page 92). After a role is selected by the user, only you, the administrator, can reset it to a different value, or to empty, so that the end user may select the role again.

Determining Policy Assignments

We recommend that you select a single criterion for policy.

Figure 4 Resolution of Policy



In order to determine which criterion to use, look at your overall environment. In general, you will probably most often assign policy by subnet or role.

- If your environment is divided by subnets, you may choose to use the SUBNET criterion. For example, server farms are typically defined by subnets.
- If your environment is a build center, it may make sense to use the ROLE criterion so that end users can select what OS should be installed.
- If your environment is standardized by hardware, then you may choose to use the MANUFACTURER or MODEL criterion. For example, one vendor makes all the laptops in your environment and a different vendor makes all of the workstations in your environment, you may decide to use the manufacturer class. These criteria will probably be used less often than the others because it may be unusual to use a certain model or manufacturer throughout your environment.

In general, you should use policy to determine the OS to be installed. Occasionally, you may want to assign a specific OS directly to a device. This can be useful for testing purposes; however it should be considered the exception to the rule. This is not recommended. Remember—policy rules.

If you have followed the recommendation to use one criterion to determine policy, your OSs will deploy as expected.

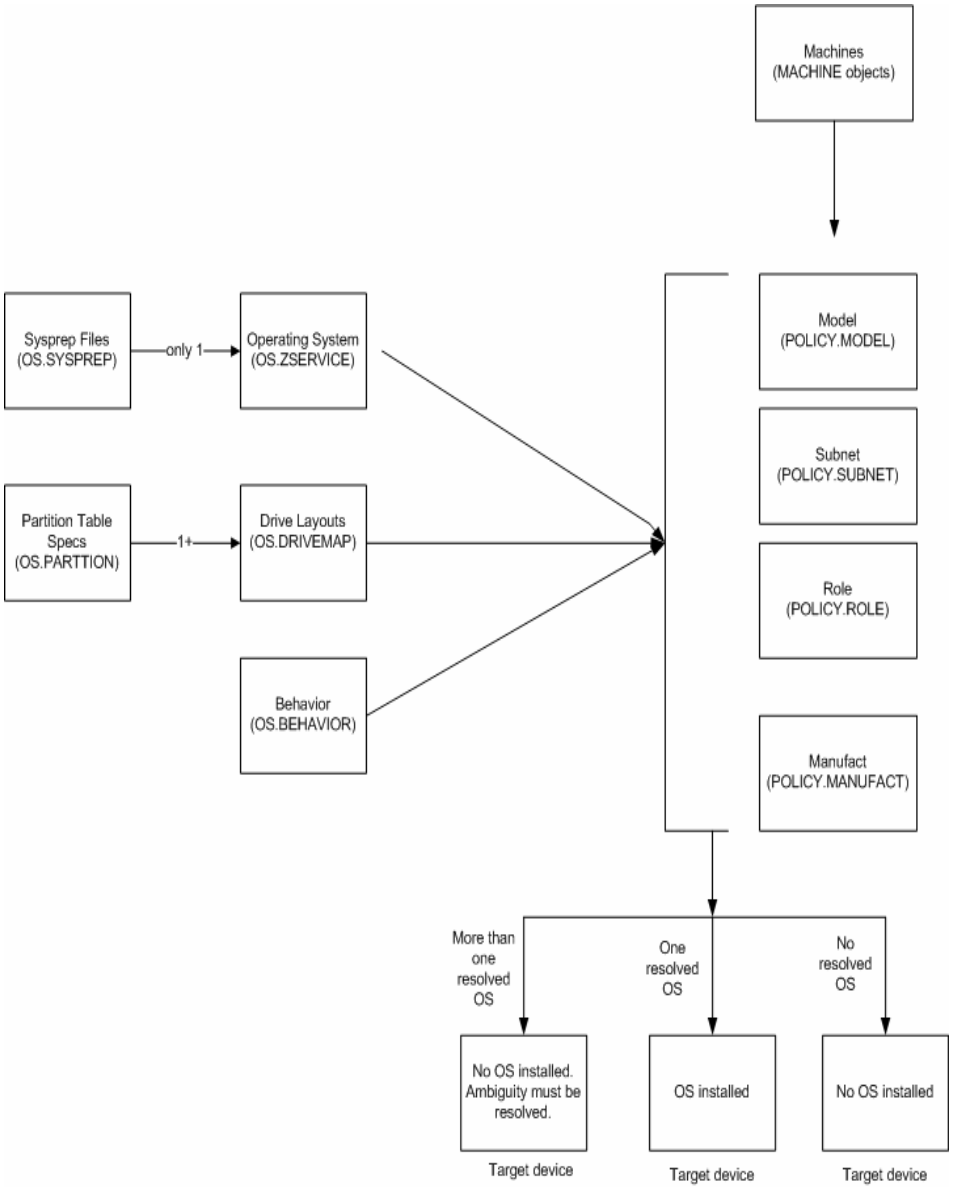
Ambiguities in Policy Resolution

At times, you may find that more than one OS has been resolved for a device. We call this an **ambiguity**. You may need to use the behavior settings to arbitrate the ambiguity if more than one criterion was used to determine policy. See Setting Behaviors on page 92 for more information about determining who is responsible for selecting the appropriate OS.

In some situations, you may intend to cause an ambiguity. An example of this would be if you have a test lab that is on its own subnet, yet you want end users to have the option to rebuild the devices frequently, choosing from one of three OSs. You would assign policy by subnet and role, but you would also have to set the behavior to prompt the end user to select the role.

Below is an overview of how the classes relate in order to determine what OS is installed on a target device.

Figure 5 Class relationships



Performing CM OS Manager administrative tasks in the CM Portal

Use the CM OS Manager Administration tasks in the CM Portal to prepare your OSs and initiate deployment. Remember, you must be familiar with the CM Portal to complete these tasks.

Logging On

To log on to the CM Portal as a CM OS Manager Administrator

1. Open your web browser.
2. In the Address bar, type **`http://IP_AddressForCMPortal:3471.`**
3. In the User Name box, type **`ROMADMIN`** to log in as the CM OS Manager administrator.
4. In the Password box, type a password. The password is case-sensitive.

   The pre-defined password is *secret*.

   Be sure to change your password before moving the CM Portal with the CM OS Manager administrative tasks into your production environment.
5. Click **Login** or press **Enter**.

About the CM OS Manager Administration Classes

To access the CM OS Manager Administration classes

1. Go to Desktop, Zone: *`ZoneName`*, Configuration, Configuration Servers and select the appropriate CM Configuration Server service for the CM OS Manager.
2. In the workspace, the following icons appear.
   - Behaviors
     Lists the settings for how the CM OS Manager behaves. You can assign different system behaviors to different targets. See Setting Behaviors on page 92.

— Drive Layouts
Lists the types of partitions that you can add or copy, and allows you to configure new partitions. See Defining Drive Layouts on page 109.

— HW Config

Stores objects that contain the information about how a target device's hardware must be configured in order for it to be ready for operating system installation. See the *HP Configuration Management OS Manager Hardware Configuration Management System Administrator Guide*.

— HW Config Element

Stores the objects that contain information about the resources required for a Hardware Configuration Management operation, the sequencing of operations, and how the operation is to be carried out. See the *HP Configuration Management OS Manager Hardware Configuration Management System Administrator Guide*.

— Machine Manufacturers
Used to set policy based on the device's manufacturer.

— Machine Models
Used to set policy based on the device's model.

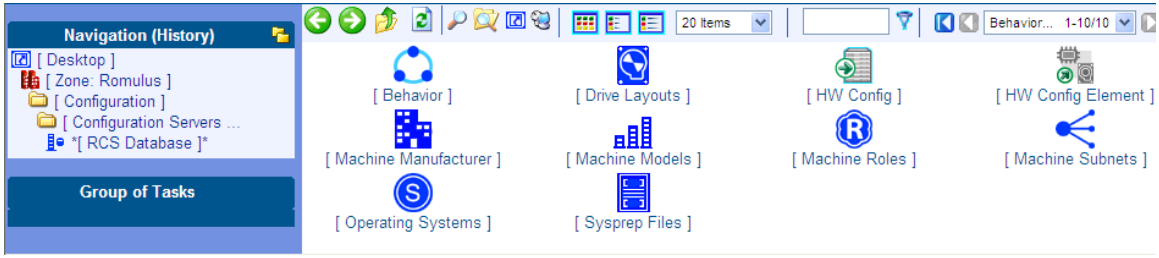
— Machine Roles
Used to set policy based on the device's role.

— Machine Subnets
Used to set policy based on the device's subnet.

— Operating Systems
Stores the OS services to be deployed to your target devices.

— Sysprep Files
Lists the Sysprep files and unattend.txt files stored in your database. See Connecting a Sysprep File on page 117.

Figure 6 CM OS Manager Administration classes



Using the CM OS Manager Administration tasks

Use the CM OS Manager Administration task group to manage the various criteria as well as define policy structures.

Before you begin using the individual tasks, it is recommended that you review some typical scenarios and the procedures that you might follow when preparing to deploy OSs to your target devices. The table below provides sample scenarios and a summary of the tasks that you can use in each of these situations. See the referenced descriptions listed with the individual tasks to learn how to use the CM OS Manager Admin Module to complete the tasks.

To use the scenarios below, you must be logged into the CM Portal as a CM OS Manager administrator.

Table 4 Administrative Procedures

If you want to...	Then...
Install an OS on a bare metal machine Note: This does not apply to Local Service Boot implementations.	1 Create any necessary policy instances, such as subnet or role. See Creating an Instance on page 99. 2 Connect the policy instances to the OS service. See Connecting Operating Systems on page 101. 3 If you do not want to use the default behavior (the Undefined instance in the Behavior class), you can modify the behaviors. See Setting Behaviors on page 92. 4 Boot the target device. When the device boots up, the appropriate OS (according to policy) is installed and a ROM object is created.

If you want to...	Then...
Bring an unmanaged machine with an installed OS under CM management and install the appropriate OS as per policy. Reminder: The target device must have the CM Application Manager with the CM OS Manager feature installed.	1 Boot the target devices so that discovery occurs. Note that the OS State is set to Desired and the Current OS and Selected OS are Unmanaged. 2 If necessary, use the Filter Machines task to determine which devices are unmanaged. See Filtering Machines on page 103. 3 If necessary, create policy instances, such as department, machine, model, or subnet. See Creating an Instance on page 99. 4 Connect the policy instances to the OS service. See Connecting Operating Systems on page 101. 5 Run a CM OS connect (via Notifying Target devices) and select the Bringing Machines under Management task which initiates a reboot of the device and starts the migration process.
Force a re-installation of the current OS without retaining any existing data.	1 Use the Force OS Install task. See Forcing an OS Installation on page 105. 2 Reboot the target device.
Force the installation of a valid OS that you choose without retaining any existing data.	1 Assign policy so that the new OS that you want to install is the *only* OS connected to policy. 2 Use the Force OS Install task. See Forcing an OS Installation on page 105. 3 Reboot the target device. 4 Run a CM OS connect. 5 Reboot the target device.

If you want to...	Then...
Initiate the installation of a different OS.	1 Set the Select OS (PMSLCTOS) behavior to _CENTRAL_ to give the administrator control over policy. See Setting Behaviors on page 92. 2 Assign policy so that the new OS that you want to install is the *only* OS connected to policy. 3 Run a CM OS connect. 4 Use the Re-evaluate/install OS task to re-evaluate the state of the OS and install a new one based on policy. See Re-evaluating the Operating System on page 104. 5 Run another CM OS connect and the device will reboot and install the new OS. Note that if you do not set the Behavior to CENTRAL, the user will be prompted to confirm whether they want to reinstall the OS.
Allow the user to decide which OS to install.	1 Verify that your policy will result in more than one OS available for the target devices. 2 Set the Select OS (PMSLCTOS) behavior in the Undefined behavior to _LOCAL_. See Setting Behaviors on page 92. 3 Run a CM OS connect. 4 Use the Re-evaluate/install OS task to re-evaluate the state of the OS and install a new one based on policy. See Re-evaluating the Operating System on page 104. 5 Reboot the target device.
View a list of devices that have more than one resolved OS and then select the OS to be installed.	• Use the Select OS for pending machines task. See Selecting an Operating System on page 102.
The following are additional options that can be used in many scenarios	
Use an override Sysprep file.	• Connect a Sysprep instance to the operating system instance. See Connecting a Sysprep File on page 117. When the OS is deployed to the target device, the override Sysprep file will be merged with the Sysprep file that is embedded in the OS.

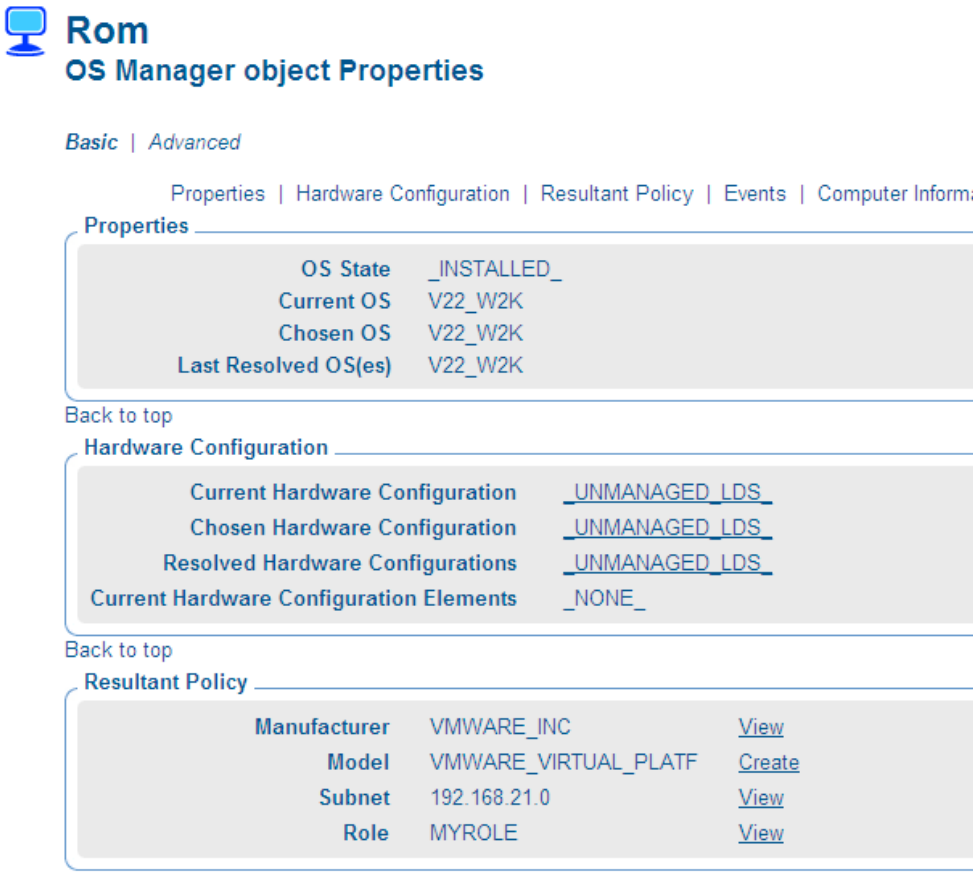
If you want to...	Then...
Add partitions.	1 Use the Drive Layouts class to specify the type of partition. See Defining Drive Layouts on page 109. 2 Add a partition. See Adding Partitions on page 111. All existing data will be lost. 3 Assign the appropriate drive layouts to your target devices. See Connecting Drive Layouts on page 111.
Create a replace, cache, or merge type partition.	1 Use the Drive Layouts class to specify the type of partition. See Defining Drive Layouts on page 109. 2 Assign the appropriate drive layouts to your target devices. See Connecting Drive Layouts on page 115.

Viewing the ROM Object

Earlier you learned that the ROM object is created in the CM Portal when a device is discovered by the CM OS Manager Server. For more information review the topic About Discovery on page 76. In order to perform many of the tasks to prepare an OS for deployment, you must have a ROM object.

To view a ROM object, select the appropriate Zone from the desktop and click on Devices. Then select the managed device you want to view and click the ROM object. The Properties window opens.

Figure 7 ROM Object Properties window



This window is separated into several sections: The Properties section displays the CM OS Manager-specific attributes for the device.

Table 5 ROM Object Attributes - Properties

Field	Description
OS State	Indicates the state of the OS on the target device. • _INVALID_ – CM OS Manager will install a valid, managed OS. • _DESIRED_ – The device is already managed and has a valid OS. • _INCONSISTENT_ – The machine is managed, but the OS must be repaired. • _INSTALLED_ – A temporary state after the gold image has been installed and before a connection with the CM OS Manager Server. After the CM OS connect, the correct OS will be installed and the OS state will change to _DESIRED_. Default: _INVALID_
Current OS	Indicates the OS that is successfully installed on the device. This represents the ZSERVICE instance in the OS class. Default: _NONE_
Chosen OS	Indicates the OS to be installed on this device. Default: _NONE_
Last Resolved OSs	Indicates the OSs resolved for this device. Default: _NONE_

- The Hardware Configuration section displays information about the current hardware configuration, including the Hardware Configuration Elements that have been successfully applied. See the *HP OpenView Configuration Management OS Manager Hardware Configuration Management Guide* for more information.
- The Resultant Policy section displays policy for the device. If policy does not already exist, you can click **Create** to create a policy instance. If policy does exist, you can click **View** to see the existing policy assignments.

Table 6 ROM object Attributes – Resultant Policy

Field	Description
Manufacturer	Manufacturer reported by SMBIOS.

Field	Description
Model	Model reported by SMBIOS.
Subnet	Current subnet.
Role	Specifies the role selected for this device by the local user or the administrator (depending on the PMROLE setting in the BEHAVIOR class of the OS domain). Default: _NONE_

The Events section displays the last five events that have been reported.

The Computer Information section displays all of the MACHINE attributes that contain values. These values are stored in the CM Configuration Server.

Table 7 ROM Object Attributes - Computer Information

Field	Description
Computer Name	Computer Name. If the ROM object exists and there is a successful CM OS connect, this attribute will be updated with the computer's current information.
Display Name	The friendly name for the ROM object.
DNS Host Name	The host name of the machine.
Enclosure Manufacturer	Manufacturer of the enclosure.
Enclosure Serial Number	Serial number for the enclosure.
Enclosure Type	Type of the enclosure.
IP Address	The target device's IP address.
ACPI BIOS?	Indicates whether the device has ACPI BIOS. • Y – indicates the device is ACPI-compliant. • N – indicates the device is not ACPI-compliant.
APIC	Indicates whether the device has an Advanced Programmable Interrupt Controller.
Mass Storage Interface	Indicates the mass storage interface - IDE or SCSI.

Field	Description
Boot drive disk space (MB)	Disk space on the boot drive in MB.
Number of CPUs	Number of CPUs in the target device.
CPU Speed (MHz)	CPU speed in MHz.
Current IP Address	Current IP address.
MAC Address	MAC address is a unique identifier derived from the NIC card.
Memory (MB)	Computer's total memory.
Subnet	The current subnet.
Sys Locator Enclosure Name	(Compaq-specific) EnclosureName field from the SMBIOS Locator structure. For HP-Compaq blades, this might be the user-defined enclosure name.
Sys Locn Enclosure Sys Bay	(Compaq-specific) EnclosureSystemBay field from the SMBIOS Locator structure. For Compaq blades, the relative location of this blade is in the enclosure.
Baseboard Location in Chassis	LocationInChassis field from the SMBIOS BaseBoardInformation structure. Note: For Dell and IBM blades, this stores the relative location of this blade inside the enclosure. Also for Dell and IBM blades, the enclosure name might be found in the SerialNumber field of the SMBIOS SystemEnclosure structure; it will be in SMINFO under the name SNENCLOS. The format of all of those four raw information fields is entirely manufacturer/model specific.
Manufacturer Derived from SMBIOS	Manufacturer reported by SMBIOS.
Model Derived from SMBIOS	Model reported by SMBIOS.
Current Subnet Mask	Current subnet mask.

Field	Description
Device Architecture	The processor architecture (CPU).
Baseboard Serial Number	The serial number for the baseboard.
Enclosure Asset Tag	The asset tag for the enclosure.
SMBIOS Enclosure S/N	System Enclosure Serial Number from the SMBIOS.
Number of Processors	The number of processors in the device.
Processor Family	The processor family.
Processor Type	The type of processor.
SMBIOS Manufacturer	Manufacturer.
SMBIOS Product	System Product (model number) from the SMBIOS.
SMBIOS System S/N	System Serial Number.
SMBIOS Machine Unique UID	Machine Unique ID from the SMBIOS.

Setting Behaviors

You can assign system behaviors to your target devices based on policy. If you do not assign a behavior to policy, the Undefined Behavior (_NULL_) instance is the default.

For example, you may want to configure some managed devices to require that the user acknowledge that this OS is about to change, while others may not require user acknowledgement.

You must be very careful if you are using more than one Behavior instance, because these instances determine the behavior of the system. You may have unintended consequences if this is not performed properly. For example, if you set the wrong policy, you may inadvertently allow users to make policy changes, or an unattended device may become stuck at a prompt.

It is highly recommended that you connect one Behavior instance to one Policy instance only.

One potential way to prevent errors would be to connect Behavior instances to mutually exclusive instances of different policies.

To set the behaviors

1. Use the navigation aid to select the appropriate CM Configuration Server.
2. In the workspace, click **Behavior**.
3. Create a new instance.

   or

   Click an instance in the workspace and then click **Modify** to make changes to an existing instance.

If you do not know how to create or modify instances, refer to the *CM Portal Guide* or follow the steps in Creating an Instance on page 99 or Modifying Instances on page 109.

Table 8 describes the attributes for the Behavior class.

Table 8 Attributes of the BEHAVIOR class

Field	Attribute in CM Configuration Server Database	Description
Instance	BHVRINST	Instance Name

Field	Attribute in CM Configuration Server Database	Description
Select ROLE	PMROLE	Indicate whether the user is allowed to select a machine role. • _LOCAL_ displays a user interface so a user at the target device can select a role for the device. The list of available roles, determined from the instances in the POLICY.ROLE class in the CM Configuration Server DB, is displayed. • _CENTRAL_ does not display the user interface. The administrator can assign a role, if necessary. A role selection remains in effect until you (the administrator) void or overrule the selection. Default: _LOCAL_
Select OS	PMSLCTOS	Indicates whether the user or administrator is responsible for action if policy resolves more than one OS for the target device. • _LOCAL_ displays a choice of OSs so the user can make a selection. Note: If a device prompts the user to make a selection even though it already contains a managed OS, it will also give the user the option to use the existing OS. For example, this would occur if a device is managed, but the ROM object was deleted from the CM Configuration Server DB. This option allows the user to preserve the existing data and applications.

Field	Attribute in CM Configuration Server Database	Description
		• _CENTRAL_ delays installation until the administrator specifies the Chosen OS. (SLCTDOS). An OS selection remains in effect until you (the administrator) void or overrule the selection or policy changes. Default: _LOCAL_
OS Overwrite Prompt	PMACKOVW	Indicates whether to prompt the user before overwriting or modifying the OS. If the prompt is displayed, it will ask the user to select "install," "use," or in some cases (where you have a valid OS with minor changes), "refresh." • "Install" creates a ROM object and installs the OS on the device. • "Use" creates a ROM object, does not install the OS and considers the device to be unmanaged. • "Refresh" reinstalls the existing OS, but includes updates to the OS made using the CM OS Manager Admin Module. Use one of the following to set PMACKOVW. • _ALWAYS_ (Default) Prompts the user only if there is a valid file system (including a valid Master Boot Record) on the machine. • _NEVER_ Does not prompt the user, but installs the OS. — Caution: NEVER is designed for use in bare metal machines or kiosk situations.

Field	Attribute in CM Configuration Server Database	Description
		Use this option with caution, as the user will not be prompted before the OS is overwritten. • _VALID_ Prompts the user only if the current installation is valid. If there is a valid OS on the device where an OS is to be installed, the user will be prompted to overwrite the OS. IF there is no valid OS, the user will not be prompted and the OS will be installed without user intervention.
Timeout for user response (seconds)	USERTO	Specifies how long a message displays to the user before continuing. • Set USERTO = -1 to wait indefinitely for input by the user. • Set USERTO = *number of seconds* to wait the specified length of time before continuing.
Download: # bytes/sec (opt K/M/G)	BANDWITH	The bandwidth throttle used by each target device. For example, 1000K. • If this attribute is left empty, the download process will run at the maximum speed of the network interface. • You can specify bandwidth throttle in Kbs (K), MB/sec (M), or GB/sec (G). The default definition is in bytes/sec. The default value is blank (no bandwidth limitation).

Field	Attribute in CM Configuration Server Database	Description
RunOnce parameter string	RUNPARAM	You must modify this parameter to specify the IP address for your CM Configuration Server. If you do not modify this parameter, your target device will not be able to successfully run a CM OS connect. Specifies the parameters that are appended to the radskman command line. This command line will run after the OS has been installed, and will install the target device's applications. For additional parameters, refer to the *HP OpenView Configuration Management Application Manager Installation and Configuration Guide* and the HP OpenView support web site. • For the IP parameter value, enter your CM Configuration Server IP address or DNS name. • The cop=y parameter must included to meet the requirement that COP must be enabled to use the CM OS Manager.
Action on existing OS upon Machine Discovery	PMINITL	Specifies whether an OS should be installed over an existing file system on a recently discovered, but unmanaged device. • _LOCAL_ Prompts the user. • _KEEP_ Does not prompt the user and keeps the current OS if the device has a valid operating system. If the device does not have a valid operating system and there is a resolved OS, it will be installed.

Field	Attribute in CM Configuration Server Database	Description
		• _REINSTALL_ (default) Does not prompt the user and reinstalls the operating system, regardless of what exists. The installation occurs only if there is no `rombl.cfg` on the device. If there is a `rombl.cfg`, this indicates that the device is already under management and nothing will happen.
Ack Timout ROLE/OS (seconds)	ACKTMOUT	Specifies how long ACKTMOUT waits before assigning the default AUTOROLE. • Set ACKTMOUT = 0 to disable the timeout. • Set ACKTMOUT = *`number of seconds`* to wait the specified length of time before continuing.
Default value for ROLE	AUTOROLE	The ROLE that is assigned if a timeout occurs.
Disaster Recovery	PMDISRCV	Specifies the action to be taken when the master boot record is found to be damaged. If PMDISRCV _CONFIRM_ then the target device shuts down so that the administrator can recover data from the target device. If PMDISRCV = _AUTO_ then the appropriate OS is re-installed.
Keybd Language Support	KBDMAP	Sets the keyboard mappings: • en (default) – loads English keyboard mappings • fr – loads French keyboard mappings • de – loads German keyboard mappings

Field	Attribute in CM Configuration Server Database	Description
ROMA Parameters	ROMAPARM	This field has several uses. Typically, you should use this only if instructed by Technical Support. Also used in conjunction with the TESTMODE flag.
Send AppEvent To	EVNTDEST	Indicates where to send the AppEvent objects. Options are: • OPS – For future use. • RIM – This option sends the AppEvent to the CM Inventory Manager. • RMP– This option sends the AppEvent to the CM Portal.
System Language	LANG	Specifies the language to be supported. • en_US = English • zh_CN = Simplified Chinese • ja_JP = Japanese • ko_KR = Korean

4 When you are done making changes, click **Modify**.

The Defaults for the Behavior Properties window opens again.

Creating an Instance

The following is an example of how to create a subnet instance. Use these steps to create an instance in any class over which you have the appropriate authority.

Note that if you want to create an instance for a machine manufacturer or machine model, you should use the manufacturer or model information that is stored in the ROM object that was created when the device was discovered.

The reason for this is that the instance name must correspond with the data derived from SMBIOS. For example, Hewlett-Packard would be HEWLETT_PA. You cannot use spaces and are restricted to ten characters.

Also, remember that you can create policy instances directly from the MACHINE instance, as described in Viewing the ROM Object on page 87.

To create a subnet instance

1. Use the navigation aid to select the appropriate CM Configuration Server.
2. In the workspace, select the appropriate class, such as Machine Subnets.
3. In the CM OS Administration task group, click **Create Instance**.

   The Create window opens.
4. In the Instance box, type the name of the instance that represents the subnet. Remember that when specifying the subnet, you must use underscores (_), not periods (.).
5. In the Friendly name box, type a friendly name.
6. Click **Create**.

   The Subnet Properties window opens.

Assigning Roles

Use the Assign Role task to assign the appropriate role to the target device. HP includes the following sample roles – SERVER and WORKSTATION.

To assign roles

1. Use the navigation aid to go to the appropriate device.
2. In the workspace, click **ROM**.
3. In the CM OS Manager Administration task group, click **Assign Role**.

   The Assign Role window opens.

4 Select a role from the list of Available Roles.

5 Click **Submit**.

The Properties window opens.

Removing Roles

Use the Remove Role task to remove the assigned role from the target device.

To remove a role

1 Use the navigation aid to go to the appropriate ROM object.

2 In the CM OS Manager Administration task group, click **Remove Role**.

The Remove Role window opens.

3 Click ✓ to confirm that you want to remove the role.

or

Click ✗ to indicate that you do not want to remove the role.

Connecting Operating Systems

Use the Connect Operating Systems task to assign the appropriate OSs to your target devices based on policy such as machine type, manufacturer, model, role or subnet.

To connect operating systems

1 Use the navigation aid to go to the appropriate POLICY instance, such as a SUBNET instance.

2 In the CM OS Manager Administration task group, click **Connect Operating Systems**.

The Add Services window opens.

3 From the Available list, select the OSs that you want to assign to the POLICY instance and then click ▶▶ to add your selections to the Selected list.

4 Click **Next**.

The Summary window opens.

5 Click **Commit**.

The Properties window for the selected POLICY instance opens.

Disconnecting Operating Systems

Use the Disconnect Operating Systems task to remove assignments between OSs and the target devices based on the selected criteria.

To disconnect operating systems

1. Use the navigation aid to go to the appropriate POLICY instance.
2. In the CM OS Manager Administration task group, click **Disconnect Operating Systems**.
3. From the Available list, select the images that you want to disconnect.
4. Click  .
5. Click **Next**.
6. The Summary window opens.
7. Click **Commit**.

   The Properties window for the selected POLICY instance opens.

Selecting an Operating System

Use the Select OS task to assign the appropriate OS to the selected target device. This task may be useful if:

- a device has more than one resolved OS (for example, if the MACHINE attribute Last Resolved OS(es) (RSLVDOS) = WIN2K WINXP).
- the user was offered a list of OSs to choose from, and selected the wrong one. To resolve this situation, you (the administrator) must set the current OS to NONE. Then, you can use the Re-evaluate/install OS task to allow the user to select the appropriate OS. Of course, you can also change the behavior settings so that the user no longer receives a list of options, and the OS of your choice is installed.

Note that:

- The Chosen OS (SLCTDOS) must be in a pending state (_SLCTOS_PENDING_).
- This task does not initiate the installation of the OS; it simply allows you to select the OS that you want to install.

To use the Select OS task

1. Use the navigation aid to go to the appropriate Zone.
2. Click **Devices** and select the appropriate device.
3. Click the ROM object.
4. In the CM OS Manager Administration task group, click **Select OS**.
5. Select the operating system that you want to install from the list.
6. Click **Submit**. The Chosen OS (SLCTDOS) attribute contains the name of the OS that you selected. You may use this task in conjunction with the Force OS Install task to force the installation of the selected OS.

Filtering Machines

Use the Filter Machines task to query for devices with an invalid OS state, unmanaged devices with no resolved OS, or devices that have more than one eligible OS.

To use the Filter Machines task

1. Use the navigation aid to go to the appropriate zone.
2. Click **Devices**.
3. In the CM OS Manager Administration task group, click **Filter Machines**.

   The Query Selection window opens.
4. Select the type of query that you want to perform.
   - Select **Invalid OS** state to find devices whose current OS is invalid. The OS State (OSSTATE) is set to _INVALID_.
   - Select **Unmanaged OS** to find devices with an OS installed, but which the CM OS Manager does not manage. An unmanaged device is a device whose Current OS (CURROS) is set to _UNMANAGED_OS_.
   - Select **Pending OS selection** to find devices that have no OS currently installed, but also have more than one eligible OS and are waiting for you (the administrator) to make a selection. A device is pending OS selection if the Chosen OS (SLCTDOS) is _SLCTOS_PENDING.
   - Select **No resolved OS** to find devices that have no resolved OSs; in other words, no policy has been assigned to the device. A device has no resolved OS if Last Resolved OS(es) (RSLVDOS) is empty.

— Select **Pending Hardware Configuration Selection** to find devices that have no hardware configuration currently applied, but also have more than one eligible hardware configuration and are waiting for you (the administrator) to make a selection. A device is pending OS selection if the Chosen LDS (SLCTDLDS) is SLCTLDS_PENDING.

Re-evaluating the Operating System

Use the Re-evaluate/install OS task to change the currently installed operating system (Chosen OS) to a different operating system. The list of potential operating systems is stored in the Last Resolved OSes field in the ROM object. See Viewing the ROM Object on page 87. Depending on your behavior settings, the user will be prompted to select an operating system or you (the administrator) will use the Select OS for Pending Machines task to make the selection.

Use of this task requires that the target device is already under management and has the ability to perform a CM OS connect. After selecting this task, you must perform a CM OS connect in order to initiate the policy change.

When the CM OS connect occurs, the data capture exit point is executed so that any user data or settings can be captured. The device then reboots and resolution continues as normal. If the behavior is set to prompt the user, he will select the appropriate OS from the list displayed. The new OS is installed and the data restore exit point will be executed so that any user data or settings can be restored. See Addressing Requirements for Capturing, Recovering, and Migrating Data on page 173.

If you want to completely re-evaluate the existing installation, and the Select Role attribute in the Behavior Properties is set to LOCAL, you may consider setting the Role assigned to the device to NONE so that the user is prompted for a role on the next reboot. See Assigning Roles on page 100 for information about how to set the role for a device.

To use the re-evaluate/install OS task

1. Use the navigation aid to go to the appropriate Zone.
2. Click **Devices** and select the appropriate device.
3. Click the ROM object.
4. In the CM OS Manager Administration task group, click **Re-evaluate/install OS**.

5 Click ✓ to continue.

or

Click ✗ to cancel this procedure.

6 If you click ✓, Chosen OS (SLCTDOS) is set to NONE and Current OS (CURROS) is set to NONE until the new OS is installed.

Forcing an OS Installation

Use the Force OS Install task to force the installation of the resolved OS over any previously existing operating system.

Use this task only in situations where you have no other choice, such as if something unrecoverable happened to a drive.

Data capture/restore exit points will *not* be executed. All data and settings will be lost. See Addressing Requirements for Capturing, Recovering, and Migrating Data on page 173.

Typically, you should modify policy to change a device's OS.

Note that if a cached partition exists, the image will be obtained from the partition. See Defining Drive Layouts on page 109.

To force an OS installation

1 Use the navigation aid to go to the appropriate Zone.

2 Click **Devices** and select the appropriate device.

3 Click the ROM object.

4 In the CM OS Manager Administration task group, click **Force OS Install**.

5 Click ✓ to continue.

or

Click ✗ to cancel this procedure.

6 If you click ✓, the OS State (OSSTATE) is set to INVALID, which is to be used as a last resort option. The OS will be re-installed on the next boot. If the next boot happens before the next CM OS connect data/restore capture, backups and so on will not be executed.

Selecting the OS for Pending Machines

Use the Select OS for Pending Machines task to return a list of devices that have more than one resolved OS and then select the OS to be installed.

To return a list of devices in pending state

1. Use the navigation aid to go to the appropriate Zone.
2. Click **Devices**.
3. In the CM OS Manager Administration task group, click **Select OS for Pending Machines**.

   A list of devices opens. A device is in pending state if Chosen OS (SLCTDOS) is set to _SLCTOS_PENDING_.
4. From the Available list, select the devices whose OSs you want to set, and then click  to add your selections to the Selected list.
5. Click **Next**.

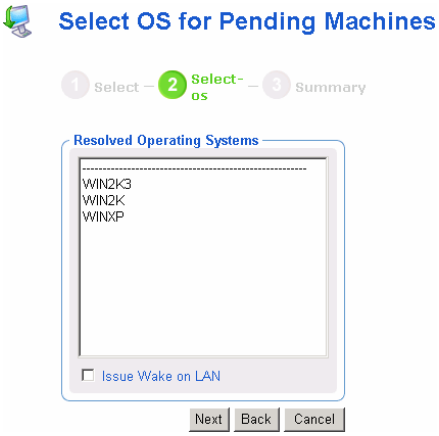
   A list of the resolved OSs opens. Note that if you select multiple devices, this list is limited to the OSs that are eligible for all of the selected devices.

   For example, if you have two devices:

   — Device A's eligible OSs are Win2k and WinXP, and

   — Device B's eligible OS is Win2k.

   The list in this window will only contain Win2k.



6 From the Resolved Operating Systems list, select the OS that you want to specify for the selected devices.

7 If you want to "wake" the target devices, select the Issue Wake on LAN check box.

8 Click **Next**.

The Summary window opens.

9 Click **Submit**. The Chosen OS (SLCTDOS) is set according to your selection.

Selecting HW Configuration for Pending Machines

Use the Select HW Configuration for Pending Machines task to return a list of devices that have more than one resolved hardware configuration and then select the hardware configuration to be applied.

To return a list of devices in pending state

1 Use the navigation aid to go to the appropriate Zone.

2 Click **Devices**.

3 In the CM OS Manager Administration task group, click **Select Hardware Configuration for Pending Machines**.

A list of devices opens. A devices is in pending state if Chosen LDS (SLCTDLDS) is set to _SLCTLDS_PENDING_.

4 From the Available list, select the devices whose hardware configurations you want to set, and then click  to add your selections to the Selected list.

5 Click **Next**.

A list of the resolved hardware configurations opens. Note that if you select multiple devices, this list is limited to the hardware configurations that are eligible for all of the selected devices.

6 From the Resolved Hardware Configurations list, select the hardware configuration that you want to specify for the selected devices.

7 If you want to "wake" the target devices, select the Issue Wake on LAN check box.

8 Click **Next**.

The Summary window opens.

9 Click **Submit**. The Chosen LDS (SLCTLDS) is set according to your selection.

Bringing Machines under Management

If there is an existing OS on a device when it is discovered, the Current OS will be set to indicate that the device is unmanaged (_UNMANAGED_OS_). You must assign policy and then use the Bring Machines Under Management task. Note that the Current OS will be set to _NONE_ until another CM OS connect occurs and the resolved OS is installed.

A typical scenario would be to filter the machine to find all of the unmanaged machines, assign policy, and then use the Bring Machines Under Management task to remove the unmanaged OS and install the new, resolved, OS. If you have not set policy, no change will occur. Note that the data capture/restore exit points will be executed so that any user data or settings can be captured and restored. See Addressing Requirements for Capturing, Recovering, and Migrating Data on page 173.

This task should not be used as the way to change OSs on a daily basis. Typically, you should modify policy to change a device's OS.

To bring machines under management

1 Use the navigation aid to go to the Devices.

2 In the CM OS Manager Administration task group, click **Bring machines under management**.

3 From the Available list, select the machines that you want to bring under management, and then click  to add your selections to the Selected list.

4 Click **Next**.

The Summary window opens.

5 Click **Submit**.

The workspace displays a list of the devices that are under management. The next time the target devices boot, they will follow the typical boot process and the appropriate OS will be installed. Until the devices boot, the value of Current OS remains set to _NONE_.

Removing Instances

Use the Remove task to remove the selected object.

To remove an object

1. Use the navigation aid to go to the appropriate instance, such as a Manufacturer instance.
2. In the CM OS Manager Administration task group, click **Remove**.
3. Click ✓ to confirm that you want to remove the instance.

   or

   Click ✗ to indicate that you do not want to remove the instance.

Modifying Instances

Use the Modify Instance task to change the selected object.

To modify an object

1. Use the navigation aid to go to the appropriate instance.
2. In the CM OS Manager Administration task group, click **Modify Instance**.
3. Make any necessary changes.
4. Click **Modify Instance**.

   The Properties window for the selected instance opens.

Defining Drive Layouts

The CM OS Manager Server supports the ability to:

- Create one or more data partitions in addition to the boot partition.

  or

- Create a copy of your new OS image and its supporting files on a hidden partition to be used for recovery.

Use the Drive Layouts class to specify the type of partition. Partitioning is supported for the boot drive only.

We strongly recommend that you connect a Drive Layout instance to only one Operating System or Policy instance to prevent conflicting definitions. Doing otherwise may cause unpredictable results.

It is possible that multiple Drive Layout instances may be resolved for an installation. Only the first resolved instance will be used. Any other instances will be ignored.

To specify a drive layout

1. Use the navigation aid to go to the appropriate CM Configuration Server.
2. Click **Drive Layouts**.
3. In the CM OS Manager Administration task group, click **Create Instance**.
4. In the Instance name box, type the name of the instance.
5. In the Friendly name box, type a friendly name.
6. In the Type drop-down list, select the type of partition you want to create.

Table 9 Types of Partitions

Type	Description
Add	Creates one or more extended partitions at the end of the hard disk.
Replace (default)	Replaces the current mappings on the target device with the partition that is defined with the OS image being installed. If there are no DRIVEMAP instances connected to the OS being installed, this is the default method. Important: If you use Replace, *all existing data will be lost.*

Type	Description
Cache	Creates a hidden back-up partition at the end of the target drive. The size of the partition will be dynamically determined by the size of the OS installation image. All files necessary to reinstall the OS will be saved (in compressed form) in this partition. Note that during the reinstallation, the name and size of the image are confirmed. Important: If you use the Cache type, *all existing data will be lost.* See Restoring Operating Systems on page 170 for information about restoring this image.
Merge	Use for migration purposes. Replaces or updates an OS on a machine where existing data needs to be preserved. Merge will overlay only the existing boot partition and will not touch data on any other partitions. • If the boot partition to be installed is larger than the space already defined for the partition, the installation will fail. The starting point of the existing partition will be used and the boot partition will be placed at the beginning of the drive segment defined in the partition. • If the target drive does not contain existing partitions, the boot partition definition will be used to partition the target drive.

7 Click **Create**.

The Drive Layout Properties window opens.

Adding Partitions

You can create a new layout that contains a boot partition and one or more logical data partitions at the end of the hard disk in a single, extended partition. These partitions are in addition to the OS boot partition. Partitions are added from the "back" of the disk to the "front."

All existing data will be lost.

There is a limit of four *physical* partitions on a hard drive and only one partition may be an extended partition (which may contain any number of logical drives).

Also, if you start with a single physical drive such as:

PARTITION	LOGICAL DRIVE
Primary	C
Extended	D
	E
	F

and then add a second hard drive, the drive letter mappings are reassigned so that the primary partitions are in alphabetical sequence. See the example below.

Drive 1

PARTITION	LOGICAL DRIVE
Primary	C
Extended	E
	F
	G

Drive 2

Primary	D
Extended	H
	I
	J

The partition will be added after the boot partition. Make sure you allow enough space for the OS. Note that if the total requested space would exceed the capacity of the drive where the OS is being installed, the installation will fail.

To add partitions

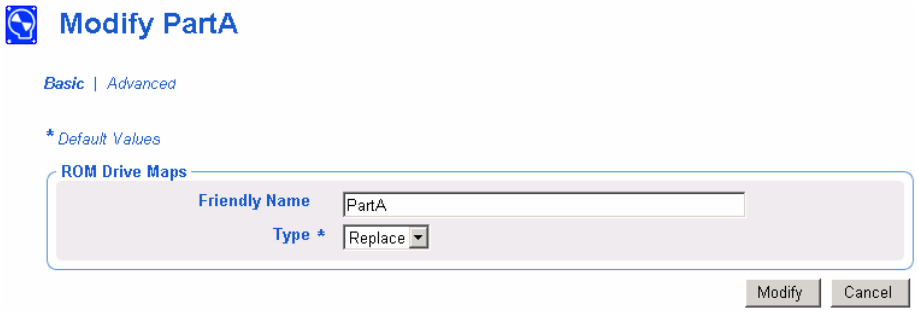
1 Use the navigation aid to go to the appropriate Zone.

2 Click **Drive Layouts.**

3 Select the appropriate drive layout instance.

4 Make sure the type is set to Add. Remember, *all existing data will be lost*.

5 If you need to modify the partition type, use the Modify Instance task, otherwise, skip to step 8.

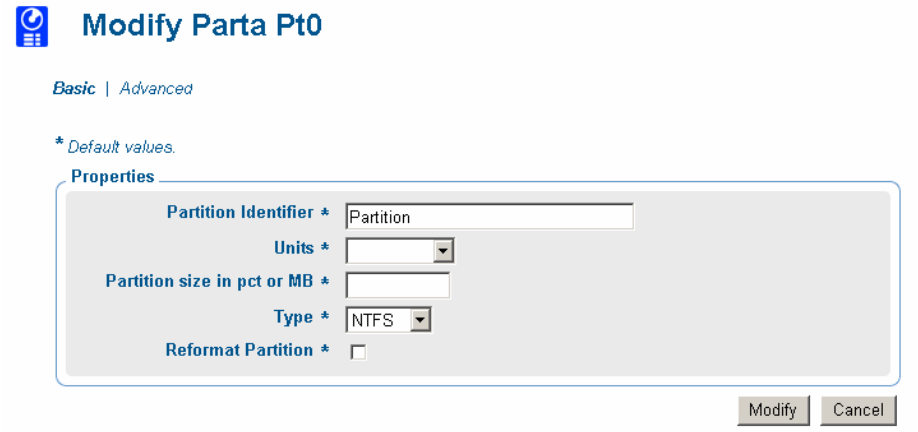


6 From the Type drop-down list, select **Add**. See Table 10 on page 114.

7 When you are done making changes, click **Modify**.

8 In the CM OS Manager Administration task group, click **Add Partition**.

The Modify window opens.



9 Specify the options in the Properties area. Note that an instance is created in the OS.PARTTION class for each partition that you add.

Table 10 PARTTION Class Attributes

Field	Attribute in the Database	Description
Partition Identifier	PARINFO	Identifies the name of the partition.
Units	UNITS	Indicates whether the partition size is being specified as a percentage or in megabytes.
Partition Size in pct or MB	SIZE	Specifies the partition size specified as a percentage of the hard drive or in MB. These values equal the total hard drive space.
Type	PARTYPE	Indicates the type of partition – NTFS, FAT32, EXT2, EXT3, or QNTFS. Note that QNTFS performs a quick format without zeroing out the partition.
Reformat drive	FORMAT	Specifies whether to format the drive.

10 Click **Modify** when you are done defining the partition information.

The Drive Layout Properties window opens.

11 In the Partition Information area, you can use the Modify or Delete hyperlinks to make changes to the defined partition. If you make changes to the partition, you will be returned to this window when you are done.

Connecting Drive Layouts

Use the Connect Drive Layout task to assign the appropriate drive layouts to your target devices based on policy such as machine manufacturer, model, role, or subnet.

To connect drive layouts

1. Use the navigation aid to go to the appropriate POLICY instance, such as a SUBNET instance.
2. In the CM OS Manager Administration task group, click **Connect Drive Layout**.

   The Connect Drive Layout to window opens.
3. From the Available Drive Layouts list, select the appropriate drive layouts, and then click Submit.

   Remember that you can add partitions *or* merge, replace, or cache partitions. You cannot do both.

   The Properties window opens.

Disconnecting Drive Layouts

Use the Disconnect Drive Layouts task to remove assignments between drive layouts and the target devices based on the selected criteria.

To disconnect drive layouts

1. Use the navigation aid to go to the appropriate POLICY instance.
2. In the CM OS Manager Administration task group, click **Disconnect Drive Layout**.
3. When prompted, click ✓ to accept to continue.

   or

   Click ✗ to cancel this procedure.

   The Properties window for the selected POLICY instance opens.

Connecting Behaviors

Use the Connect Behavior task to assign the appropriate behaviors to your target devices based on policy. Connect only one behavior instance per policy instance.

A behavior instance defines system behaviors that can be assigned to targets based on policy.

To connect behaviors

1. Use the navigation aid to go to the appropriate POLICY instance, such as a SUBNET instance.
2. In the CM OS Manager Administration task group, click **Connect Behavior**.

   The Available Behaviors window opens.
3. From the Available OS Behaviors list, select the appropriate behavior.
4. Click **Submit**.

   The Properties window opens.

Disconnecting Behaviors

Use the Disconnect Behaviors task to remove the behavior assignment.

To disconnect behaviors

1. Use the navigation aid to go to the appropriate POLICY instance.
2. In the CM OS Manager Administration task group, click **Disconnect Behavior**.
3. When asked if you are sure that you want to disconnect the behavior, click ✓ to continue.

   or

   Click ✗ to cancel this procedure.

   The Properties window for the selected POLICY instance opens.

Connecting a Sysprep File

Use the Connect Sysprep File task to assign a `Sysprep.inf` that is separate from the gold image to allow the same image to be set up differently on target devices. The override `Sysprep.inf` will be merged with the embedded `Sysprep.inf`. Therefore, the values in the override `Sysprep.inf` will take priority; however any values not specified in the override file will remain as is in the original file.

Each Sysprep can only be connected to one OS service. At this time OS services cannot share Sysprep instances.

The `Sysprep.inf` file should not be greater than 800 KB in size.

To create an override Sysprep.inf

1. Modify `Sysprep.inf` to contain the appropriate information.
2. Use the CM Admin Publisher to publish the new `Sysprep.inf` file to the OS domain, Sysprep Files (SYSPREP) class.

   In the CM Admin Publisher, from the Type of Data to Publish drop-down list, you must select **OS Image**. Then, you can select the appropriate `Sysprep.inf` file that you want to use. See Using the CM Admin Publisher on page 72.

3. Use the Connect Sysprep File in the CM OS Manager Administration task group to connect the Sysprep file to the appropriate OS. You can only attach one Sysprep file to an OS. If the OS does not have this connection, the embedded `Sysprep.inf` file will be used.

   Currently, the COMPNAME and DOMAIN from the ROM object will be used in `Sysprep.inf`, whether `Sysprep.inf` was embedded in the image or published separately.

   Consider running a manual test of `Sysprep.inf` to verify the accuracy of the file prior to using the CM Image Preparation Wizard. Remember that if you run Sysprep and have extendoempartition = 1, the partition will be extended after Sysprep runs.

   If you want to deliver the same OS with varying setup behaviors, you can create multiple OS services. Each OS service can contain the same OS image, yet each may have a different `Sysprep.inf` attached to it.

To connect a Sysprep file to an OS instance

1. Use the navigation aid to go to the appropriate OS instance.
2. In the CM OS Manager Administration task group, click **Connect Sysprep File**.

   The Select Sysprep File window opens.
3. From the Available OS Sysprep list, select the appropriate Sysprep file.
4. Click **Submit**.

   The Properties window opens.

Disconnecting a Sysprep File

Use the Disconnect Sysprep File task to remove an assignment between OSs and a Sysprep file. If you disconnect the override Sysprep file, the next time that the OS is installed, the Sysprep file that is embedded in the OS image will be used.

To disconnect a Sysprep file

1. Use the navigation aid to go to the appropriate operating system instance.
2. In the CM OS Manager Administration task group, click **Disconnect Sysprep File**.
3. When asked if you are sure that you want to disconnect the Sysprep file, click ✓ to continue.

   or

   Click ✗ to cancel this procedure.

   The Properties window for the selected OS opens.

Adding Devices

By default the CM OS Manager will use the serial number as the ComputerName in order to ensure that the device is given a unique name. However, you may prefer to have more control over the machine name.

Use the Add Device task to specify network setting information manually in a ROM object. This information will be injected into the Sysprep.inf during OS deployment. For example, you can specify the computer name, static IP addresses, subnet, subnet mask and gateway information for a machine.

The Add Device task is most useful when provisioning servers. For example, if you want to install Windows 2003 Server on a machine, you may not want to have the machine discovered so that you have some control over identifying parameters. Therefore, you can add the device in the CM Portal and assign a unique computer name. When the device boots for the first time, it will be provisioned with the information that you specified.

This task is useful for a small number of devices. If you have many devices and want to specify their identifying parameters (via an algorithm or mapping), you would use the exit point called `getmachinename.tcl`, located on the CM OS Manager Server, to configure devices dynamically. This exit point can interact with existing servers, such as Web servers or SQL servers. See the engineering note, *Assigning unique Machine Names with OS Management* for more information about this exit point.

To add a device

1. Use the navigation aid to select the appropriate Zone.
   a. In the workspace, click **Groups**.
   b. Select a group and from the CM OS Manager Administration task group, click **Add Device**.
2. In the Common Name field, type the machine ID.
3. In the Computer Name field, type the computer name with a maximum of 15 characters.
4. In the Sysprep Data field, type the Sysprep data that you want to inject in the following format:
   `section/key=value,section/key=value,section/key=value,...`

   You cannot use blanks except as part of a value. You cannot use a forward slash (/), equal sign (=), or comma (,) in the section, key or value.
5. Click **Submit**.

Modifying Devices

Use the Modify Device task to modify Sysprep data that you manually added to a device using the Add Device task.

To modify a device

1. Use the navigation aid to select the appropriate Zone.
2. In the workspace, click **Devices**.

3 Select the device that you want to modify and then select its ROM object.

If you want to see the Sysprep Data that was added to the device, click **Advanced** in the workspace. Scroll to the Advanced section and you will see a Sysprep Data field that shows the current settings.

2 From the CM OS Manager Administration task group, click **Modify Device**.

3 Make the necessary changes and click **Submit**.

Downloading Resources

Use the Download Resources task to save the resource files for OS services or Sysprep files to a directory on the CM OS Manager Server. Then, you can burn a CD-ROM or DVD-ROM with this data. Do not span your resources over multiple CD-ROMs or DVD-ROMs. Typically, this is meant for use with DVDs to store multiple images.

You must use Client Operations Profiles (COP) to specify where CM OS Manager Server should retrieve the image. See the *CM OS Manager Server Release Notes* on the HP OpenView web site for more information about the capabilities and limitations of the CM OS Manager Server-specific extension before proceeding.

Your CD-ROM must be in Joliet format.

To download resources to a target directory

1 Use the navigation aid to go to the appropriate class — Operating Systems or SysPrep Files.

2 In the CM OS Manager Administration task group, click **Download Resources**.

The Select window opens.

3 From the Available list, select the operating system services that you want to download.

4 Click **Next**.

The Download Options window opens.

5 If you changed the port number for the Proxy Server, type the new port number in the **Please specify the port number of your Proxy Server on localhost** text box.

6 Type the name of the directory on your CM OS Manager Server to which you want to download your resources. If the directory does not exist, it will be created.

If your browser is not running on the CM OS Manager Server, specify a UNC path to the target directory.

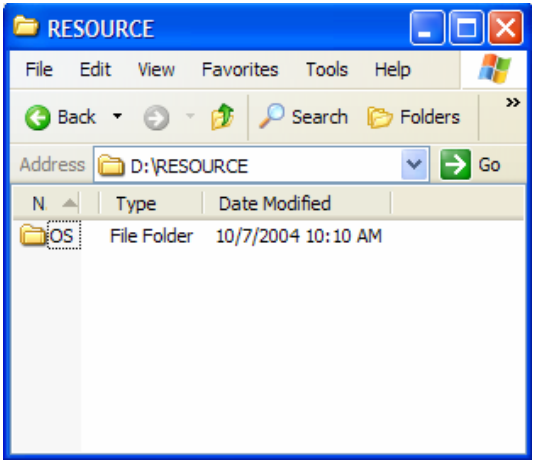
7 Click **Next**.

The Summary window opens.

8 Click **Submit**.

The workspace returns to the class you were viewing. However, if you use Windows Explorer, you will notice that your files have been downloaded to the target directory that you specified.

Be sure that your CD writer software does not change the case of the directories or files that you are copying. If it does, then be sure to change it back to match the file structure that was created using this task.



9 Be sure to copy the entire RESOURCE directory to the CD-ROM or DVD-ROM.

Now that you have the RESOURCE directory stored appropriately, use CM Client Operations Profiles to specify where the CM OS Manager Server should retrieve the image. See the *CM OS Manager Server Release Notes* on the HP OpenView web site for more information about the

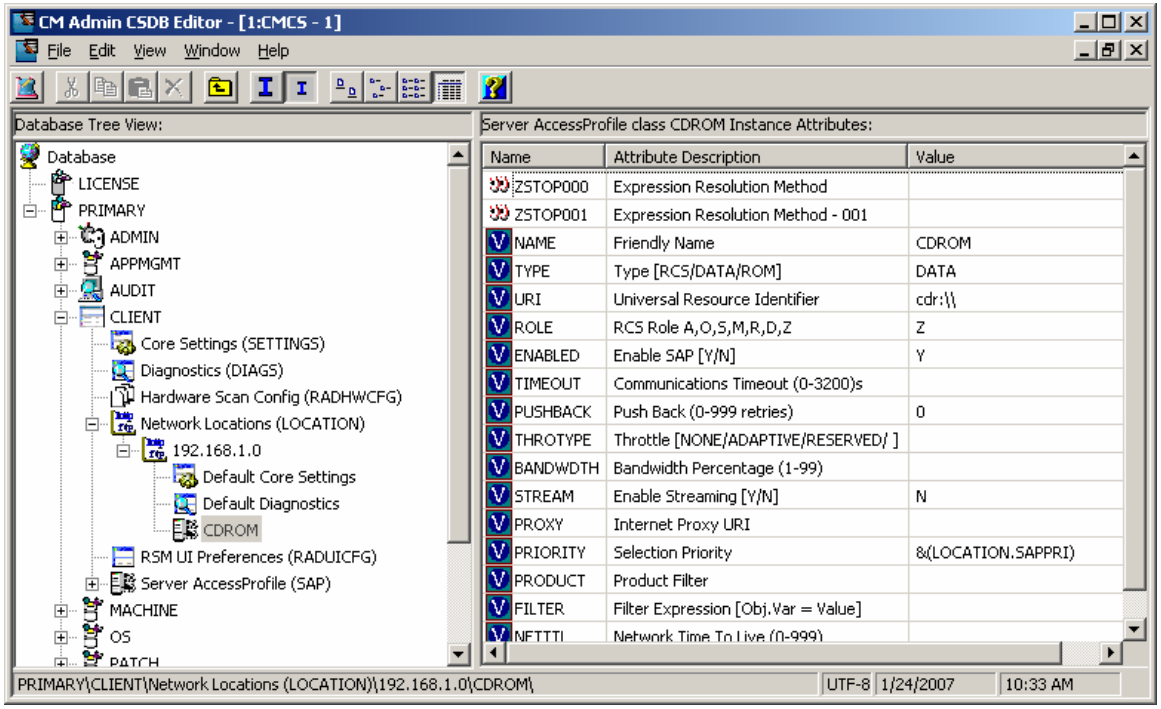
capabilities and limitations of the CM OS Manager Server-specific extension before proceeding.

Retrieving the OS image from a CD-ROM

If you used the Download Resources task, the following is an example of how to use a CD-ROM or a DVD-ROM to install an OS to a target device.

See *Configuring Client Operations Profiles* in the *CM Application Self-Service Manager Guide* and then see the *CM OS Manager Server Release Notes* for details on how to use CM Client Operation Profiles with ROM.

1. Create a CLIENT.LOCATION instance to specify your network.
2. Create a CLIENT.SAP instance for the CD-ROM. Be sure to:
   - Set `TYPE` to `DATA`.
   - Set `URI` to `cdr://`
   - Set `ROLE` to `Z`.
3. Use the CM Admin CSDB Editor to connect the SAP instance to the LOCATION instance. Be sure to use the _ALWAYS_ connection with the Connect To Attribute description.



4 Insert the CD-ROM or the DVD-ROM into the target device.

5 Boot the machine. When the machine boots, it does a CM Client Operations Profiles resolution and installs the OS image from the CD-ROM or the DVD-ROM.

Notifying Target devices

Use the Notify task to perform an action on a target device that you select. For more information, see the *CM Portal Guide for Windows*.

To notify a target device

1 Use the navigation aid to go to the Device class under the appropriate Zone.

2 In the CM OS Manager Administration task group, click **Notify**.

The Select CM OS Manager Task window opens.

3 Select the CM OS Manager task type.

— No CM OS Manager Task Selected

Select this option to perform a standard notify operation.

— Assign Role

A list box appears and you must select a role. See Assigning Roles on page 100.

— Bring Machines Under Management

See Bringing Machines under Management on page 108.

— Force OS Install

See Forcing an OS Installation on page 105.

— Re-evaluate/install OS

See Re-evaluating the Operating System on page 104.

— Remove Role

The selected role is removed. See Removing Roles on page 101.

4 Click **Next**.

The Select window opens.

5 Select the devices that you want to Notify.

6 Click **Next**.

The Notify Options window opens.

7 From the Notify Type drop-down list, select **OS Connect** to indicate that this connection is being performed for the CM OS Manager.

The parameters in the Command box change, based on your selection.

8 In the Command box, modify the command line as necessary. For example, the Command box is pre-filled with the following command line:

```
radskman ip=|mgr_ip|,
port=|mgr_port|,dname=OS,cat=prompt,ulogon=n,context=m,ask=
n,cop=y,catexp=ZOBJDOMN:OS,ver=y
```

You must replace information between the pipes (|) with the necessary information to perform the notification. For example, you might modify the command line above to read:

```
Radskman ip=10.10.10.1,port=3464,
dname=OS,cat=prompt,ulogon=n,context=m,ask=n,
cop=y,catexp=ZOBJDOMN:OS,ver=y
```

If you repeat a Notify operation often, you may want to modify the appropriate Notify task so that it has default options that pertain to your organization. Refer to the *CM Portal Guide*.

9 In the Port number box, type the port number that the Notify daemon will be listening on. By default, the port number is 3465.

10 If necessary, in the User box, type the user name for the target device.

11 If necessary, in the User Password box, type the password for the target device.

12 Click **Next**.

The Schedule dialog box opens.

13 In the Schedule dialog box, specify when you want this job to run.

14 Click **Next**.

The Summary dialog box opens.

15 Click **Submit**.

The Job Status dialog box opens with list of the jobs. This dialog box automatically refreshes every 60 seconds.

— Click  to refresh the dialog box to display the latest status.

— Click  to view detailed information, such as the status of the installation.

16 When you are done viewing the job status, click  to close the Job Status dialog box, and return to the CM Portal.

7 Implementing CM OS Manager Server in your Environment

At the end of this chapter, you will:

- Be able to initiate an installation via the network.
- Be able to initiate an installation locally.

After you have successfully installed your CM OS Manager infrastructure, consider how you want to implement the CM OS Manager in your environment. We recommend that you work with Professional Services to determine what is best for your unique situation. This chapter is intended to help you understand your options. They are:

- Installations initiated by the network
  This refers to the PXE-based environment. The CM OS Manager can assume management of the operating system on target devices that are booted from the network.
- Installations initiated locally
  This refers to the Local Service Boot (LSB). The CM OS Manager can assume management of the OS on target devices that are not booted from the network.

We strongly recommend that you choose one method for a particular target device. If you have a bare metal machine or a machine that needs disaster recovery, you *must* use PXE.

About the PXE-Based Environment

The PXE-based environment allows the CM OS Manager to assume management of the OS on target devices that are booted from the network. Typically, we recommend that you use the PXE-based environment because it provides a fully automated solution for all scenarios.

Best Practices for PXE-Based Implementations

If you already have CM implemented in your environment and want to use a PXE-based environment for the CM OS Manager, we recommend the following:

1. Install the CM OS Manager Server infrastructure before making any changes to your target devices. See Chapter 3, Installing and Configuring the Server Architecture.
2. CM agents that exist on your target devices will continue running any previously scheduled CM agent connects. The CM OS Manager will not make any changes to the device until you assign policy.

3 After your infrastructure is installed and stable, set the network boot as the primary boot device on your target devices.

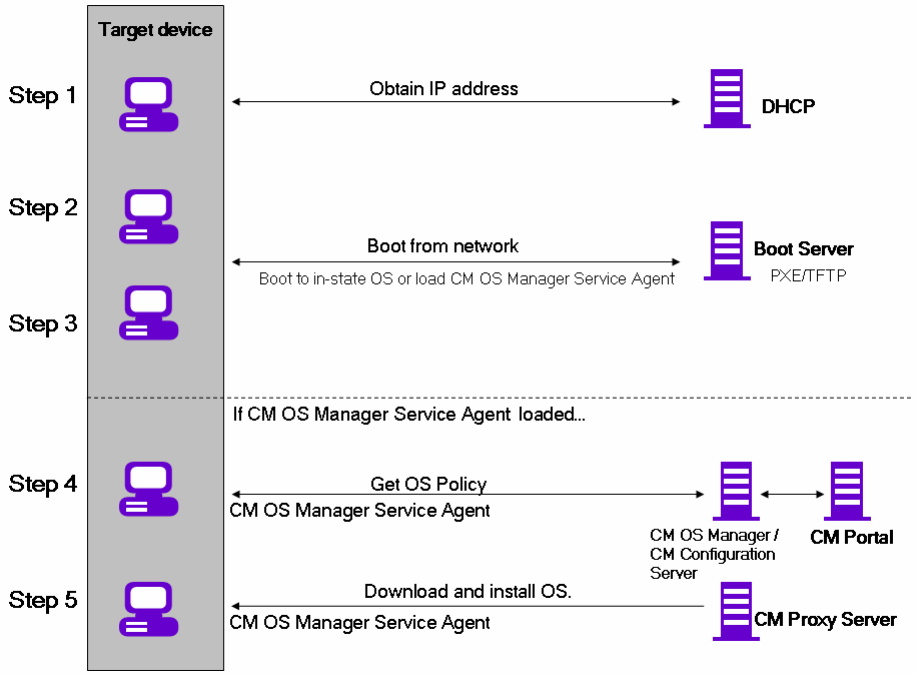
4 The next time the device boots, a ROM object will be created in the CM Portal. The CM OS Manager Server and the target device use the ROM object to communicate.

At this point, the CM OS Manager has discovered the target device, but its OS is likely considered unmanaged unless you assigned policy prior to booting the target device. The target device will continue to boot into its existing OS until you assign policy.

Networking Boot with PXE

Figure 8 below and the text following it give an overview of the boot process.

Figure 8 Networking boot with PXE process flow



1 The target device obtains an IP address from a DHCP server.

2 The (managed) target device boots from the network (via the PXE server), and the TFTP server delivers the CM OS Manager Boot Loader to the target device.

3 The CM OS Manager Boot Loader looks at the CM Portal to see if a ROM object exists.

   — If there is no ROM object, an object is created in the CM Portal.

   — If there is a ROM object, it must be decided whether there is a valid OS or not.

4 If there is a valid OS on the machine, it boots to the existing OS located on the device's system drive.

   or

   If there is not a valid OS on the device, the boot process continues by loading the CM OS Manager System Agent from the TFTP server to the target device.

5 The CM OS Manager System Agent and the CM Configuration Server communicate through the CM OS Manager Server to handle policy resolution of the correct OSs for the target device.

6 The CM OS Manager System Agent downloads the appropriate images from the CM Proxy Server and installs them on the target device.

Check the HP OpenView support web site for product updates and release notes.

About Local Service Boot

The Local Service Boot allows the CM OS Manager to assume management of existing OSs on devices that are not booted from the network.

The advantages of Local Service Boot are that existing machines do not need to be PXE-enabled and the boot order does not need to be configured locally in the BIOS for each target device. This option is also less network-intensive because the CM OS Manager System Agent is only downloaded when the LSB service is downloaded to the target device. Since this intermediate OS is local, it does not need to be downloaded again unless there is an update. In a PXE environment, the CM OS Manager System Agent is downloaded every time it is needed.

If you have a bare metal machine or a machine that needs disaster recovery, you *must* use PXE.

Prerequisites

- You must have an operating system and the CM Application Manager installed on the target device so that you can deploy the LSB service.
- You must be using CM Client Operations Profiles as configured for the CM OS Manager Server and it must be enabled. See the *CM OS Manager Server Release Notes* on the HP OpenView web site for more information about the capabilities and limitations of the CM OS Manager Server-specific extension.

  The CM OS Image Preparation Wizard sets up CM Client Operations Profiles, and when the image is deployed, CM Client Operations Profiles is enabled. However, if you want to use the Local Service Boot on a machine where the OS has not been deployed by the CM OS Manager Server, you must enable CM Client Operations Profiles. To do this, use COP=Y on the radskman command line. See *Configuring Client Operations Profiles* in the *HP OpenView Configuration Management Application Self-service Manager Installation and Configuration Guide*.

Best Practices for Using Local Service Boot

If you already have CM implemented in your environment and want to use the Local Service Boot for the CM OS Manager, we recommend that you:

1. Install the CM OS Manager Server infrastructure. See Chapter 3, Installing and Configuring the Server Architecture.
2. Use CM Client Operations Profiles to specify the IP address and port of the CM OS Manager Server in the form of a Service Access Profile (SAP) instance.

   When you set up the SAP, be sure to:

   — Set `TYPE` to `ROM` to identify this SAP as a CM OS Manager Server server.

   — Set `ROLE` to `Z`.

— Set `URI` to specify the fully qualified IP address (or hostname) and port of the CM OS Manager Server that serves the CM agents on the subnet. For example:

http://CMOSManagerServer.domain.com:3466.

The value of the URL must be in lowercase text; otherwise the Local Service Boot will fail.

You must create a LOCATION instance and an SAP instance and connect them.

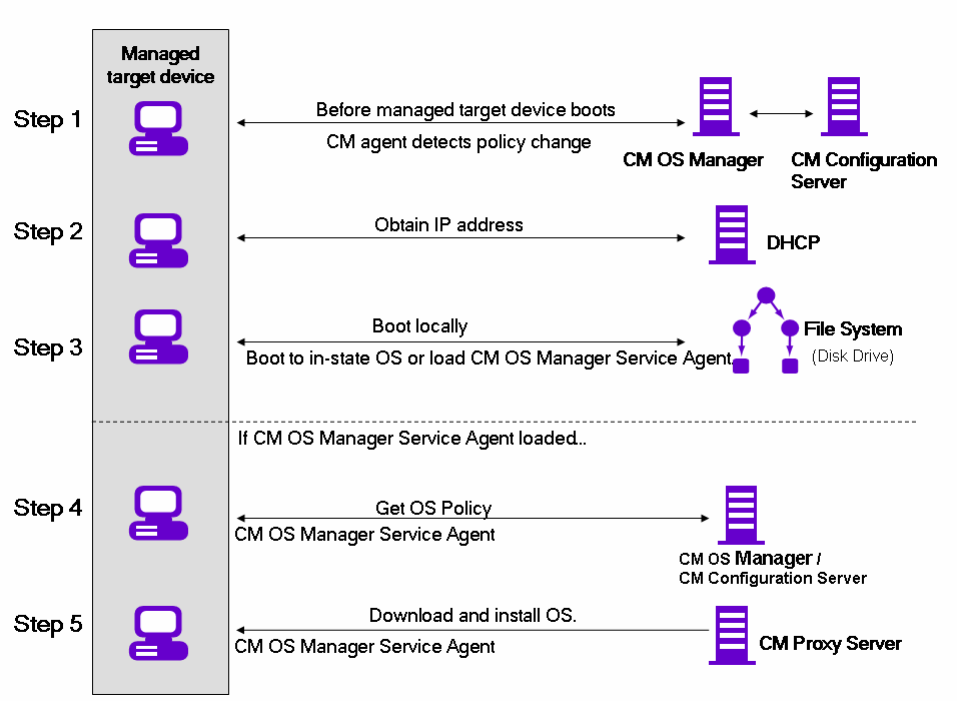
3 Set up policy to use the CM Application Manager to install the Local Service Boot service (LSB) on your target devices. Local Service Boot (LSB) must be distributed based on subnet, model or manufacturer.

After the LSB service is installed on the target devices (which creates the `Rombl.cfg` file on the root of the drive), they will reboot and be discovered. At this point, the CM OS Manager has discovered the target device, but its OS is still unmanaged. The target device will continue to boot into its existing OS until you assign policy.

Booting with Local Service Boot

Figure 9 on page 133, and the text following it give an overview of the boot process.

Figure 9 Booting with Local Service Boot



1. After the Local Service Boot service is installed on a target device, the CM Application Manager is responsible for detecting OS policy changes on the managed target device.
2. The target device obtains an IP address from a DHCP server.
3. When the device restarts, the device boots into the intermediate Linux service OS and runs the CM OS Manager System Agent.
4. During this first boot after installation of the Local Service Boot service, a ROM object for the target device is created in the CM Portal (if one does not already exist). A ROM object will exist only if the device was previously under OS management.
5. During every subsequent reboot, the CM OS Manager Boot Loader will be loaded from the local file system.

6 If the CM OS connect detected a change in OS policy before the reboot, the CM OS Manager Boot Loader will load the intermediate Linux service OS, from the local file system, containing the CM OS Manager System Agent. The CM OS Manager System Agent processes the installation of the new OS, according to policy.

7 If no OS policy exists for this device, the CM OS Manager System Agent will install the _UNMANAGED_OS_ service (located in PRIMARY.OS.ZSERVICE). This special OS instance indicates that the device is under OS management, but that no OS has been selected for the device by policy.

Check the HP OpenView support web site for product updates and release notes.

Managing Your Devices

Whether your devices are in a PXE-based environment or Local Service boot environment, once your existing devices are discovered and set to be unmanaged, nothing will happen until you take action.

If you want to change the OS, you must:

1 Specify policy.

2 Select the appropriate devices and use the Bring Machines under OS Management task.

3 This removes the unmanaged service (which was connected to your devices) and the device is considered managed.

4 Run a CM OS connect so the target devices can detect the policy changes.

5 If necessary, reboot the target devices.

This completes the description of how to implement the CM OS Manager in your environment.

We recommend that you work with Professional Services to determine what is best for your environment.

8 About OS Manager Support for HP Blades

At the end of this chapter, you will:

- Be able to enable policy configurations for blades, enclosures and racks.
- Be able to view blade information stored in the Chassis container in the CM Portal.
- Be able to assign policy based on enclosures, racks, slots or enclosure configurations.

The CM OS Manager System Agent captures and reports all specific blade SMBIOS information to the CM Portal. Using the CM Portal, you can assign drive layouts, hardware configurations, and operating systems to your devices based on enclosures, racks, slots or enclosure configurations. To do this, you can use the CM OS Administration tasks Connect Operating System, Connect Hardware Configuration and Connect Operating System which are available for Blade.

For more information of Blade Management in CM Portal refer to the *HP OpenView Configuration Management Portal Installation and Configuration Guide*.

Enabling Policy Configurations for Blades, Enclosures and Racks

To enable resolution of policy for the objects related to blades, you must update the `rmp.cfg`.

To enable policy configurations for blades, enclosures and racks

1. Open *`SystemDrive`*`:\IntegrationServer\etc\rmp.cfg`.
2. Add the following entry:

```
rmp::init{
   LINKS{ enclosureslotnumberdn enclosuremodeldn
enclosureconfigdn rackdn osdevicearchitecturedn }
 }
```

   The specific set of links to include in the entry will vary for each enterprise, depending on which entities and containers have been used for policy. Table 11 below describes the policy link that is enabled in the entry above. For example, if you have not assigned policy to the rack instances in your Zone, you may omit `rackdn` from the entry shown above.

Table 11 Policy Resolution Links to Define in RMP.CFG

LINKS Parameter	Description
enclosureslotnumberdn	Links the blade device to the enclosure slot.
enclosuremodeldn	Links the blade device to the enclosure model.
enclosureconfigdn	Links the enclosure to its enclosure configuration.

LINKS Parameter	Description
osdevicearchitecturedn	Links the device to its device architecture (which is added by default).
rackdn	Links the enclosure to its rack (when policies are assigned to racks).

About HP Blade Discovery

Every time the target device boots, SMBIOS information (such as enclosure name and slots) from HP blades is sent to CM Portal through the CM OS Manager Server. The CM Portal will automatically create all related Blade information in the Chassis container.

To view the blade information stored in the Chassis container

1. Log into the CM Portal.
2. Navigate to the appropriate Zone.
3. Click **Chassis** and then **Blade Enclosures** to see the discovered enclosures.
4. Click an enclosure name to display the slots discovered by the CM OS Manager.
5. Click a slot to display the discovered hardware device plugged into this slot.

About HP Blade OS Policy Assignment

Using the CM Portal, you can assign operating systems, drive layouts and hardware configurations based on enclosures, racks, slots or enclosure configurations.

To assign operating systems, drive layouts or hardware configurations

1. In the CM Portal, browse to the desired enclosure, racks, slots or enclosure configurations.
2. From the CM OS Manager Administration task group, select the appropriate task such as **Connect Operating Systems**.
3. From the Available list, select the desired OS.

4 Click **Next**.

The operating system is assigned to the selected enclosure name.

5 If you want to see the operating system assigned to enclosure, go to the enclosure and click **View Properties**  .

9 About Multicast and the CM OS Manager

At the end of this chapter, you will:

- Understand the requirements for using multicast with the CM OS Manager.
- Be able to configure multicast for the CM OS Manager.
- Understand how to improve performance and reliability for multicast with the CM OS Manager.
- Understand how multicast transfers images.
- Understand the multicast parameters and their influence.
- Be able to identify, analyze and resolve multicast data transfer problems.
- Use a set of tools to manually test combinations of multicast parameters.

The CM OS Manager supports reliable delivery multicast so that you can rollout large numbers of OS images concurrently with improved performance.

In general, the same concepts apply when using the Multicast Server for the CM Application Manager or for the CM OS Manager. For a general understanding of the Multicast Server, refer to the *HP OpenView Configuration Management Multicast Server Installation and Configuration Guide* on the HP OpenView support web site.

This topic covers how to use multicast with the CM OS Manager. Refer to the *CM Multicast Server Guide* for installation instructions.

Spanned images are not supported with Multicast.

Prerequisites

- An understanding of the Multicast Server.

Requirements

- Multicast server version 3.1 or higher installed on a Windows machine.
- A reliable delivery Multicast-aware version of the CM OS Manager System Agent (supported in version 2.0 and higher of the OS Manager).
- The image will be downloaded only if the Service Multicast Eligible option is selected for the OS Service. To do this, use the CM Portal to navigate to the appropriate Operating System service.
  a. Click **Modify Instance**.
  b. In the workspace, click **Advanced**.
  d. Scroll to the bottom of the screen and make sure that Service Multicast Eligible is selected.
- Images must be a maximum of 4 GB. If they are larger than 4 GB, the image download will fail when using multicast.

Configuring Multicast for CM OS Manager

To configure multicast for use with the CM OS Manager complete the following steps.

To configure reliable delivery multicast

1. Go to the appropriate Behavior instance.
2. In the workspace, click **Advanced**.
3. Click **Modify Instance**.
4. Modify the ROMA Parameters field as follows:

```
-multicast multicastIPAddress:3463 -mcastretrycount 1
-mcastretrywait 240
```

Table 12 Description of ROMA Parameters

Parameter	Description
`multicastIPAddress`	This parameter specifies the CM Multicast Server host. You can also use the host name. 3463 is the default Multicast Server port.
`mcastretrycount`	This parameter specifies the number of times that the client will retry multicast if there is a failure. The default value is 1.
`mcastretrywait`	This parameter specifies how long to wait before the client will start the retry. The default value is 240 seconds.

5. Modify `SystemDrive:\ Program Files\Hewlett-Packard\CM\MulticastServer\etc\mcast.cfg` as needed.

   — `root`
   Specifies the root directory from which the Multicast Server will retrieve resources.

   — `address`
   Specifies a range of multicast IP addresses available for use with dynamic windows. See the *CM Multicast Server Guide* for more information about dynamic windows.

   — `Minref`
   Specifies the minimum number of clients that are required to contact the multicast server to start a multicast session. By default, `minref=2`. You may want to change this to take advantage of multicast's functionality.

   — `Cwindow`
   Specifies the length of the collection window; how long to wait for clients to register for a given OS service before finalizing the setup of

a multicast session. Change the value for this parameter based on your requirements.

Refer to the *CM Multicast Server Guide* for more information about the parameters in this file.

6 If you made changes to `mcast.cfg`, restart the Multicast Service to implement your changes.

You may notice a `multicast.rc` file in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\MulticastServer\etc`.

Do *not* make any changes to this file.

Improving Performance and Reliability for Multicast with CM OS Manager

The default values of the multicast parameters provide a good combination of reliability and performance in many environments. Optimal performance (transfer speed) is relative to your network environment. Therefore, you must determine what is optimal for your environment and then use the parameters defined in this topic to increase reliability and performance.

The fundamental problem surrounding the reliability and performance issues of the multicast transfer is packet loss. Because multicast is a UDP based protocol, delivery of packets is not guaranteed.

External factors that contribute to packet loss are:

- Network conditions. The amount of traffic on the network, the number of routers between the server and client, and faulty network connections, all can contribute to packet loss during multicast transfers.
- Agent conditions. The relative CPU, I/O and network performance of the agents can contribute to packet loss specific to the clients in question. If an agent is unable to read packets fast enough, some of those packets will be missed.

In any environment, packet loss is inevitable. The key is to find the balance between minimal packet loss and high data transfer rates in order to optimize actual throughput.

Terminology

It is important to understand of how multicast handles the transfer of images. A sender (server) sends packets to a receiver (agent). The agent receives the data. If the data has not been received in its complete form, the client sends a resend request to the server. The server resends the packets to attempt to complete the transfer successfully. Below you will be introduced to some of the terminology that you will see used throughout this topic.

actual throughput

The size of the operating system image divided by the time it takes to transfer the image.

agent (Receiver)

The agent that receives the multicast transmission.

image

The data that is transmitted from the server to its clients in a single multicast session. For the OS Manager, this is an operating system image.

multicast transfer

The process of sending data from the server to the client.

packet

A unit of information sent over a computer network.

packet loss

When the agent does not receive one or more packets sent by the server.

performance

The time it takes to transfer the image.

raw data transfer rate

The total number of packets (fixed size of data) sent over time, including packets that have been resent.

reliability

The likelihood that the multicast transfer will complete successfully.

resend block

A group of packets to be resent as a result of a resend request (NACK).

resend request /negative acknowledgment (NACK)

A message sent from the client to the server indicating the client did not receive a specific piece of data.

server (sender)

The agent that transmits the data to its clients via multicast. For the CM OS Manager, this data is an operating system image.

About the Multicast Parameters

This section describes the multicast parameters whose values may need to be modified in order to increase performance and/or reliability.

Table 13 Multicast parameters

Parameter	Used by	Definition	Default value
`gddelaybp`	Sender	Inter-packet delay. The number of milliseconds to wait after sending a packet before sending the next one.	0.0625
`lingercount`	Sender	The number of times to check for resend requests (NACKs) after the last packet has been sent before determining that the transfer is complete.	512
`lingerdelay`	Sender	The delay, in milliseconds, between checking for resend requests (NACKs) after the last packet has been	32.0

Parameter	Used by	Definition	Default value
		sent.	
lprcount	Sender	The number of times the last packet of the image is retransmitted in order to increase the probability that the receiver sees the last packet. Note that the receiver recognizes the last packet because it contains a flag indicating that it is the last packet.	4
lprdelay	Sender	The delay, in milliseconds, between each attempt to resend the last packet.	.25
maxrsndreq	Receiver	The maximum number of resend requests (NACKs) that can be issued for a given block. A block contains a number of packets. The size of a block is defined by the numpktblks parameter described below.	4098
nacdelay	Receiver	The delay, in milliseconds, between resends of a specific NACK.	0.5
nacresend	Receiver	The number of times to resend each NACK.	2

Parameter	Used by	Definition	Default value
`netinacto`	Receiver	Network inactivity time-out. The number of minutes of network inactivity allowed between received packets before the receiver fails.	5
`numpktblks`	Sender or Receiver	Defines the size of the pool from which resend requests are fulfilled.	64
`pktsperblk`	Sender or Receiver	Specifies the number of packets within a resend block. This is the minimum number of packets that will be resent as a result of a NACK. The total number of these packets is considered a resend block. This value must be a multiple of 32. If you do not follow this requirement, your value will be adjusted and noted in the `gdmcsend.log` and the CM OS Manager System Agent logs.	256

Parameter	Used by	Definition	Default value
`recvtimeout`	Receiver	The maximum time, in minutes, that is allowed for the total data transfer before it is considered a failed transfer.	45
`throtfreq`	Sender	Throttle frequency. Specifies how often to check to see if the inter-packet delay should be adjusted.	8
`throthighth`	Sender	Throttle high threshold. The number of average resends per block that will trigger an increment of the inter-packet delay.	-1 (disabled) Note: To enable this, set it to a positive number higher than 0.
`throtincr`	Sender	Throttle increment. The value, in milliseconds, that is automatically added to (or subtracted from) the current inter-packet delay each time the throttle is adjusted. See Auto Throttle on page 152 for more information.	0.01

Parameter	Used by	Definition	Default value
`throtlowth`	Sender	Throttle low threshold. The number of average resends per block that will trigger a decrement of the inter-packet delay.	-1 (disabled) Note: To enable this, set it to 0 or a positive number.
`throtmax`	Sender	Throttle maximum. The maximum inter-packet delay, in milliseconds, that can be set by the throttle.	0.5
`throtmin`	Sender	Throttle minimum. The minimum inter-packet delay, in milliseconds, that can be set by the throttle.	0.0
`ttl`	Sender	Time to live. The number of subnets that the packet will reach. Every time a packet reaches a switch the ttl value is decremented until it reaches 0. If the value is 0, the packet cannot cross the switch. This limits how far the packets can spread from the sender.	3

How the Parameters Influence Multicast Data Transfer

This section provides a more in-depth description of the parameters, including the influence they have on the multicast data transfer and their interaction with each other.

Understanding Inter-packet Delay

The raw data transfer rate of the sender is influenced by the inter-packet delay parameter (`gddelaybp`).

`Gddelaybp` represents the number of milliseconds to wait after sending a packet before sending the next.

Increasing the inter-packet delay will decrease the raw data transfer rate of the sender. In general lower transfer rates will result in less packet loss. If the transfer rate is too low, it will have a negative impact on the actual throughput.

To give you a feeling for the impact this parameter can have on the actual throughput, let's consider the example of transferring a one gigabyte image using a 1 millisecond inter-packet delay. One gigabyte is 1,073,741,824 bytes. Assuming each packet is 1024 bytes, the image can be transferred in 1,048,576 packets at best. Given a one millisecond delay for each packet, the delays alone would total more than 1048 seconds. This means that it would take over 17 minutes to transfer the image, assuming no packet loss at all. In actuality, some packets probably will be lost, requiring some of the data to be resent; each resend packet consuming at least one millisecond.

Approaching this from the other direction, say we want to be able to transfer the one gigabyte image in under five minutes. Five minutes equals 300,000 milliseconds. Dividing that by 1,048,576 packets gives us about 0.3 milliseconds per packet. So, before we can even hope to transfer the image in under five minutes, the inter-packet delay must be less than 0.3. Unfortunately, lowering this value will more than likely result in greater packet loss and in turn, more resent packets.

To what degree lowering the inter-packet delay results in greater packet loss depends on the network and client conditions. While some conditions may support very low inter-packet delay values with minimal packet loss, others may not. Normally, when the conditions can't support a given raw data transfer rate, the actual throughput will suffer due to the number of resends required to complete the transfer. In extreme cases however, the transfer may fail.

About the Buffer Settings

While the buffer settings don't have an impact on the raw data transfer rate, they can have significant impact on the reliability and actual throughput of the transfer.

The buffer, as defined by the `numpktblks` and `pktsperblk` parameters, influences the following characteristics of the multicast transfer:

- The maximum number of packets the receiver can handle before it has the opportunity to write out the packets received first. For slower clients, there may be periods during the transfer where packets are being received faster than they can be written out, or an unfulfilled resend request may prevent a buffer from being written out, causing received packets to backup. During these periods, the overall size of the buffer (`numpktblks` * `pktsperblk`) defines the number of packets that can be received before the backup is alleviated. If the buffer limit is exceeded before the backup is alleviated, the transfer will fail.
- On the sender side, the number of packet blocks (`numpktblks`) defines the size of the pool from which resend requests are fulfilled. If a resend request is made for a block that is no longer in this pool, the server will not be able to fulfill the request.
- On the receiver side, the number of packet blocks, `numpktblks`, defines the size of the pool of blocks for which resend requests can be made.
- The size of each packet block (`pktsperblk`) defines the minimum number of packets that will be resent as a result of a resend request (NACK). The optimum packet block size depends on the overall distribution of lost packets. If lost packets are few and far between, then smaller packet blocks will minimize the overhead associated with the acquisition of each lost packet. If lost packets tend to be grouped together, then larger packet blocks may minimize the number of resend requests (NACKs) required to acquire the missing packets.

Handling Special Packets

As we mentioned earlier, multicast, being a UDP based protocol, does not guarantee delivery of packets. The protocol used to send resend requests from the receivers to the sender is based on UDP as well, so delivery of resend requests isn't guaranteed. However, we are relying on the resend requests to ensure the delivery of the packets. In addition, the last packet sent from the sender is used to trigger resend requests from the receiver as needed. If the last packet is lost, receivers will not know to request resends for the missing packets, including the last one.

Because we can't rely on a resend request to ensure that a resend request is received, we must fall back on a more fundamental way to minimize the probability that these special packets will be lost. To do this, we send a fixed number duplicates for each of these types of packets, to ensure that at least one of them will be received by the clients. The parameters used to do this are:

- `nackresend` defines the number of times each NACK packet is retransmitted.
- `nackdelay` defines the delay between each retransmission.
- `lprcount` defines the number of times the last packet of the image is re-transmitted.
- `lprdelay` the delay between each retransmission.

The more clients participating in the multicast session, the lower the need for many NACK resends. Assuming many of the lost packets will be common to a large number of receivers, more often than not, multiple receivers will NACK the same blocks.

Handling the End of Image

After the multicast server has sent the last packet of the image, it needs to wait to see if there are any remaining NACKs that need to be serviced before exiting. The `lingercount` and `lingerdelay` parameters govern how this is done.

`Lingercount` - The number of times to check for resend requests (NACKs) after the last packet has been sent before determining that the transfer is complete.

`Lingerdelay` - The delay, in milliseconds, between checking for resend requests (NACKs) after the last packet has been sent.

Basically, the server checks for NACKs *`lingercount`* times and waits *`lingerdelay`* milliseconds between each check. If the server does not see a NACK in that period, it exits. If it does receive NACKs, it services them and starts checking all over again.

If these parameters are set too low, the server may exit before it receives the remaining NACKs from its clients. If this happens, the transfer to the clients with unfulfilled NACKs will fail. In the event of failure, the transfer will be retried if you have set `mcastretrycount` to a value greater than 0.

Auto Throttle

The intent of this feature is to prevent adverse network and/or client conditions from causing the actual throughput from degrading to unacceptable levels, not to optimize throughput; although, in some cases, it may accomplish just that.

This feature attempts to keep the average NACKs per block within a predefined band. This is accomplished by modifying the inter-packet delay (`gddelaybp`) whenever the average NACKs per block falls outside the band. The band is defined by high (`throthighth`) and low (`throtlowth`) throttle threshold values, where the high threshold is the maximum desired NACKs per block and the low threshold the minimum.

After each packet block is sent for the first time, the n-moving average for the last *n* packet blocks is computed, where *n* is the number of packet blocks currently configured (`numpktblks`). When the throttle is checked, this moving average is compared to the high and low throttle thresholds, and the inter-packet delay is adjusted accordingly. If the moving average is greater than the high throttle threshold, a configurable value (`throtincr`) is added to the inter-packet delay. If the moving average is less than the low throttle threshold, the same configurable value is subtracted from the inter-packet delay. High (`throtmax`) and low (`throtmin`) limits for the inter-packet delay are also defined. If a throttle adjustment would cause the inter-packet delay to exceed either of these limits, the adjustment will not be made.

The throttle is checked after every `throtfreq` packet blocks are sent. Here, `throtfreq` is the configurable throttle frequency. Actually, this is the throttle period, as it defines the number of packet blocks between throttle adjustments. The intent here is to give any previous adjustments an opportunity to influence the results, before checking the throttle again.

Analyzing Problems

This section describes haw to identify, analyze and resolve multicast data transfer problems.

About the Logs

The sender's log — `gdmcsend.log` — is typically stored in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\MulticastServer\logs`.

The receiver log is typically appended to the end of the CM OS Manager System Agent log for the device.

Poor Performance

As mentioned before, poor multicast transfer performance is usually due to poor network and/or agent conditions. Such conditions result in the generation of an excessive number of resend requests (NACKs) from one or more of the clients, slowing down the entire transfer.

Before you can resolve the performance issue, you must first determine the root cause of the problem. To do so, examine the contents of the multicast sender's log file, `gdmcsend.log`. Review the following steps to guide you in determining the cause of the problem.

1. Determine is the average number of resends per block for the transfer in question. Look for the line in the log file in the form:

   ```
   Avg resends per block = 0.00283688
   ```

   Averages less than one are very good. This indicates that most of the packet blocks were sent only once, with relatively few resends. Large values may indicate a problem. What to consider large depends on the value of the inter-packet delay, `gddelaybp`. Remember, there is a trade-off between raw data transfer rates and packet loss, so you can expect more NACKs when the inter-packet delay is small.

2. If the average resends per block indicates that there is a problem, examine the per-client statistics for the transfer. In the same log file, look for lines in the form:

   ```
   Client stats:
   Client: 16.119.237.171 (0xabed7710) NACKs = 19714
   Client: 16.119.237.207 (0xabed7710) NACKs = 102
   Client: 16.119.237.122 (0xabed7710) NACKs = 17
   Client: 16.119.237.217 (0xabed7710) NACKs = 8
   ```

   Each client is identified by its IP address. The client that has been issued the most resend requests (NACKs) appears at the top of the list.

   If there are one or more agents that top the list whose NACK count far exceed those of the other agents, it is a strong indication that the problem is specific to the agents in question. After the problematic agents have been identified, you can try to determine what sets them apart from the others. Some considerations:

   a. Are the problematic clients on a different subnet than the others? If so, the problem may be specific to that subnet. Check the routers in

the path from the server to the clients to see if any have seen a large number of errors on any of their ports. If so, it can be a router, port, or cabling problem.

b Are the agents in question slower than the others? Slow clients may be unable to keep up with high raw data transfer rates, causing them to miss more packets and in turn, NACK more often. If this is the case, you have a few options:

– Increase the inter-packet delay (`gddelaybp`) in order to lower the raw data transfer rate, so the slower agents will be better able to keep up. Even with the lower transfer rate, if the number of NACKs from these agents is significantly reduced, the actual throughput may increase.

– Whenever possible, do not include these clients in multicast sessions with faster agents. Put them in their own multicast session, or use unicast to deploy images to them.

c If the clients are of comparable speed, the local network connections or cabling may be at fault. Check the cables and connections closest to the agents to see if they are causing the problem.

3 If all of the clients show a large number of NACKs, the problem is probably more systemic.

a The network may have been especially congested during the time of the transfer. Performing the transfer when the network is less busy may yield better results.

b Check the relevant network routers, connections and cabling as described above. This time, make sure to check the cables and connections from the server to the network.

c It could be that all of the machines are just too slow to keep up with the current raw data transfer rate. Increase the inter-packet delay to see if fixes the problem.

In some cases, enabling the auto-throttle feature is a better alternative than manually increasing the inter-packet delay. After the proper threshold values are set, the auto-throttle will adjust the inter-packet delay as needed.

Client Time-out

Agents can time out for one of two reasons:

1. **Total image transfer time-out** occurs when the total time it takes to transfer the image exceeds the value of the recvtimeout parameter.
2. **Network inactivity time-out** occurs when the time between received packets exceeds the value of the `netinacto` parameter.

When a client times out, the type of time-out can be determined by examining the client's log file.

Total Image Transfer Time-out

In the log file, a total image transfer time-out is indicated by a message in the form:

```
Module has timed out (timeout = nnn)
```

where *nnn* is the time-out value that has been exceeded.

Extreme cases of poor performance can lead to this type of failure, when the performance degrades to the point where the image cannot be transferred in the time defined by the recvtimeout parameter. When this is the case, the same techniques described in Poor Performance on page 153, can be used to identify and resolve the problem.

Network Inactivity Time-out

A log file message in the form:

```
Inactivity timeout has been exceeded.
```

is indicative of a network inactivity time-out.

This type of failure can be caused by almost anything that disrupts the flow of data from the server to the client. Premature termination of the multicast sender and various network problems can occasionally be at fault.

In some cases, it can result from the loss of one or more strategic packets. For example, the client in question may not have seen the last packet of the image. If this is the case, it will not know it needs to NACK the missing data. Having sent the last block and not seeing any NACKs, the server will not send more data. Expecting more data, the client will wait for the next packet until `netinacto` has been exceeded.

We can determine if the client missed the last packet of the image by examining the log files. In the sender's log file, `gdmcsend.log`, look for two lines in the form:

```
Last block: 3524
```

```
Packets in last block: 54
```

If they exist, then you know the sender sent the last packet.

Now, in the client's log file, look for a line like:

```
Last buffer size = nnn
```

If this line isn't there, then you know the client didn't see the last packet.

To remedy this problem, increase the value of the `lprcount` parameter. This will cause the last packet of the image to be retransmitted more times, increasing the probability that the client will see at least one of the redundant packets.

Buffer Overflow

The primary causes of buffer overflow are slow clients and missing data.

Slow Client

If the client is too slow, it may not be able to write out data fast enough, causing its buffer capacity to be exceeded. To determine if this is the case, look to the client's log file.

First, look for a line in the form:

```
Current block: 3289, High block: 3353
```

In this example, the value of the `numpktblks` parameter is 64. The fact that the difference between the current block (3289) and the high block (3353) is 64 indicates that all the buffers are in use.

Following this line are entries for every block that isn't full. If there are no such entries or just a few near the high block range, it shows that most of the buffers are full, but the agent has not had the chance to write them out yet. For example, if the following line is:

```
Block: 3353, 32 packets of 256
```

It shows that all but the high block are full. This indicates that the agent may be too slow for the current raw data transfer rate. Here, you may want to consider increasing the inter-packet delay to see if the agent can better keep up with the lower raw data transfer rate.

Missing Data

On the client, if a block is missing data, it cannot be written out. After that block becomes current, writing will stop and won't resume until the missing data is filled in. In the meantime, the remaining buffers are used to hold the incoming data. If the missing data is not filled in soon enough, the buffers may overflow. Normally, the client will NACK the missing data and the holes will be filled in long before this happens.

In the client's log file, the indicators of this condition are similar to those of the slow client case. The line:

```
Current block: 3289, High block: 3353
```

should look essentially the same, showing all of the buffers in use.

In this case however, the following line will show that the current buffer is not full:

```
Block: 3289, 32 packets of 256
```

Now the question becomes, why is this data missing? The agent should have sent a NACK requesting that this block be resent and the data should have been resent by the server.

There are two possibilities: the NACK was never sent or the server never received it.

First, let's see if the block was indeed NACK'ed. In the client's log file, look for the statistics associated with the block in question:

```
Block: 3289, 32 packets of 256
Resends requested: 1
```

Here you see one NACK was sent for the block.

Now, see if all of the NACKs the client sent got through to the server. In the client log file, there should be a line in the form:

```
Total resend requests = 8
```

Here, you see that the agent sent eight NACKs to the server. In the server log file, look at the per- agent data. After the line:

```
Client stats:
```

is a list of agents and the number of NACKs the server has received from each. Using the agent's IP address, find the line associated with the client in question. It should look something like this:

```
Client: 16.119.237.171 (0xabed7710) NACKs = 8
```

Here you can see that the server did receive all the NACKs the client sent. If these numbers were not the same, it would indicate that one or more NACKs had been lost. In that case, you should increase the value of the `nackresend` parameter. This will cause each NACK packet to be retransmitted more times, increasing the probability that the client will see at least one of the redundant packets.

For the case where the server has seen all the NACKs sent from the client, it probably indicates that the client didn't issue a NACK when it needed to.

In the agent log file, look for the following line:

```
Max resend hits = n
```

Here, `n` is the number of times the client didn't issue a NACK because the value of the `maxresendreq` parameter had been exceeded. If you can't remedy the cause of the excessive number of NACKs, you may want to increase the value of `maxresendreq`, thus enabling the client to NACK a given block more times.

Test Modules

The following commands are provided as test tools that you can use to manually test different combinations of parameters, rather than running tests in the full CM OS Manager environment.

Using gdmcsend

The `gdmcsend` command can be run from a Windows environment only.

`gdmcsend` is the server side multicast send command.

On the CM 5.00 media in Infrastructure`\extended_infrastructure \multicast_server\multicast_test_modules\` there is a script called `gdmsend.cmd` that can be used for testing.

To start the multicast test sender module

1 Copy the multicast test send modules (`gdmcsend.exe`, `gdmcsend.cmd`, and `TESTDATA0004`) from the `extended_infrastructure\multicast_server\multicast_test_modules` directory on the infrastructure CD to a temporary directory.

2 Rename `TESTDATA0004` to `GDMCTESTDATA`.

3 Edit `gdmsend.cmd` and change `DP` on line 19 from `0.0` to `0.5`.

4 Edit `gdmsend.cmd` and change `OFFSET` on line 49 from `60` to `0`.

5 Run `gdmsend`.

If you want to modify the script, use a text editor to open the file and modify the parameters. Then, you can run this file to test the changes you made. See Example of Using the Test Modules on page 167.

When setting values for parameters that apply to both `gdmcsend` and `gdmrecv`, the values must match.

Below are two forms of the command and the valid options for each. Explanations of the parameters follow.

Use this command if you are using reliable delivery resend mode.

```
gdmcsend -rm D|B -ma multicast_address -mp multicast_port -np
nac_port-f file_name -npb nblocks -ppb npackets[-dp1 delay] [-
dp delay] [-dl delay] [-lc n] [-lf log_file][-nr n] [-ttl n]
[-lpr n] [-lprd delay] [-offset n_bytes][-ni ip_address][-tf
throttle_frequency] [-ti throttle_increment][-tmax
throttle_maximum] [-tmin throttle_minimum][-tthigh
high_throttle_threshold][-ttlow low_throttle_threshold]
```

Use this command if you are using the fixed resend mode, which resends each packet block a fixed number of times.

```
gdmcsend -rm F -ma multicast_address -mp multicast_port -f
file_name-ppb npackets -nr number_of_resends[-dp1 delay] [-dp
delay] [-lf log_file] [-nr n] [-ttl n][-lpr n] [-lprd delay]
[-offset n_bytes] [-ni ip_address]
```

Table 14 gdmcsend command options

Option	Corresponding parameter in mcast.cfg	Description	Default
-dl *linger_delay*	`lingerdelay`	The delay, in milliseconds, between checking for resend requests after the last packet has been sent.	64.0

Option	Corresponding parameter in mcast.cfg	Description	Default
-dp *delay*	gddelaybp	Delay, in milliseconds, after sending each packet.	0.0625
-dp1 *delay*	N/A	Delay, in milliseconds, after sending the first packet.	5
-f *filename*	N/A	Name of the file containing the data to be sent.	N/A
-lc *n*	lingercount	Linger count. The number of times to check for resend requests (NACKs), after the last packet has been sent.	256
-lf *log_file*	N/A	The name of the log file. The log file is stored in the directory where you execute the command. You may use this parameter to change the name of the log file or provide an absolute or relative path.	gdmcsend.log
-lpr *n*	lprcount	Last packet resend. The number of times to resend the last packet.	4

Option	Corresponding parameter in mcast.cfg	Description	Default
-lprd *delay*	lprdelay	Last packet resend delay. The delay, in milliseconds, between last packet resends.	0.25
-ma *multicast_address*	N/A	Multicast address. The address to which the data is sent.	N/A
-mp *multicast_port*	N/A	Multicast port. The port to which the data is sent.	N/A
-ni *ip_address*	N/A	Network interface. The IP address identifies the specific local network interface to use when sending data.	selected automatically
-np *nac_port*	N/A	NACK port. The port from which resend requests are read.	9514
-npb *nblocks*	N/A	Number of packet blocks. The number of packet blocks available to be resent.	N/A
-nr n		The number of times to resend each packet. This option only applies when resend mode (**-rm**) is set to **F**.	0

Option	Corresponding parameter in mcast.cfg	Description	Default
-offset *n_bytes*	N/A	Skip the first *n_bytes* bytes of the file.	0
-ppb *npackets*	N/A	Packets per block. The number of packets in each packet block (must be a multiple of 32).	N/A
-rm F|B|D	N/A	Resend mode. **F = fixed** Each packet block is resent a fixed num-ber of times (as specified by the **-nr** option). **B = backup** Resend all blocks from the lowest number requested to the current block (last block sent by the sender). **D = discrete** Resend only requested blocks.	B
-tf *throttle_frequency*	throtfreq	The minimum number of packet blocks between throttle adjustments.	8

Option	Corresponding parameter in mcast.cfg	Description	Default
-ti *throttle_increment*	throtincr	The value, in milliseconds, that is added to (or subtracted from) the current inter-packet delay each time the throttle needs to be adjusted.	0.01
-tmax *throttle_maximum*	throtmax	The maximum value of the inter-packet delay before throttling will stop.	0.5
-tmin *throttle_minimum*	throtmin	The minimum value of the inter-packet delay before throttling will stop.	0.0
-tthigh *high_throttle_threshold*	throthighth	The average number of resends per block that will trigger an increment of the inter-packet delay.	-1 (throttling disabled)
-ttlow *low_throttle_threshold*	throtlowth	The average number of resends per block that will trigger a decrement of the inter-packet delay.	-1 (throttling disabled)
-ttl n	ttl	Time to live. The number of subnets that the packet will reach.	3

Using gdmcrecv

`Gdmcrecv` is the client side multicast receive command.

The gdmcrecv command can only be run from the Service Operating System as booted from the CM OS Manager CD-ROM in TESTMODE. If necessary, use a nano editor to modify the shell script, gdmrecv.sh. For an example of how this may be used, see Example of Using the Test Modules on page 167.

When setting values for parameters that apply to both gdmcsend and gdmrecv, the values must match.

Below are two sample commands and explanations of the parameters follow.

Use this command if you are using reliable delivery resend mode.

```
gdmcrecv -rm D|B -ma multicast_address -mp multicast_port -np
nac_port-na nac_address -npb nblocks -ppb npackets[-t
timeout_minutes] [-nit timeout_minutes][-mr max_resend_req] [-
nd nac_delay] [-nr nac_resends][-lf log_file] [-bt
block_threshold] [-ni ip_address][-pmf freq] [-stderr]
```

Use this command if you are using the fixed resend mode which resends each packet block a fixed number of times.

```
gdmcrecv -rm F -ma multicast_address -mp multicast_port -ppb
npackets[-t timeout_minutes] [-nit timeout_minutes][-lf
log_file] [-ni ip_address]
```

Table 15 gdmcrecv command options

Option	Corresponding parameter in mcast.cfg	Description	Default
-bt *block_threshold*	N/A	Block threshold. When the number of used blocks exceeds this value, resend requests are sent even if all data has been received in order to slow down the sender.	0

Option	Corresponding parameter in mcast.cfg	Description	Default
-lf *log_file*	N/A	Name of log file. The log file is stored in the directory where you execute the command. You may use this parameter to change the name of the log file or provide an absolute or relative path.	`gdmcrecv.log`
-ma *multicast_address*	N/A	Multicast address. The address from which data is read.	N/A
-mp *multicast_port*	N/A	Multicast port. The port from which data is read.	N/A
-mr *max_resend_req*	`maxrsndreq`	The maximum number of times a resend can be requested for each block.	128
-na *nac_address*	N/A	NACK address. The address to which resend requests are sent.	N/A
-nd *nac_delay*	`nacdelay`	The delay, in milliseconds, between sending resend requests.	0.5
-ni *ip_address*	N/A	Network interface. The IP address that identifies the specific local network interface to use to receive data.	selected automatically

Option	Corresponding parameter in mcast.cfg	Description	Default
-nit *timeout_minutes*	netinacto	The time to wait, in minutes, between received packets before failing.	5
-np *nac_port*	N/A	NACK port. The port to which resend requests are sent.	9514
-npb *nblocks*	numpktblks	Number of packet blocks. The maximum number of packet blocks that can be serviced by resend requests at any point in time.	N/A
-nr *nac_resend*	nacresend	The number of times each NACK should be resent.	4
-pmf *freq*	N/A	Progress meter frequency. The progress meter is updated after every freq packet blocks have been written out. A value of zero disables the progress meter.	0
-ppb *npackets*	pktsperblk	Packets per block. The number of packets in each packet block (must be a multiple of 32 and match the value used by the sender).	N/A

Option	Corresponding parameter in mcast.cfg	Description	Default
-rm F|B|D	N/A	Resend mode. **F = fixed** Each packet block is resent a fixed number of times (as specified by the -nr option). **B = backup** Resend all blocks from the lowest requested to the current. The receiver will only send resend requests (NACKs) for the lowest block needed. **D = discrete** Resend only requested blocks. The receiver will send resend requests (NACKs) for every block needed.	B
-stderr	N/A	Write log messages to *stderr* (standard error), as well as the log file.	FALSE
-t *timeout_minutes*	recvtimeout	The maximum time, in minutes, before the data transfer fails.	45

Example of Using the Test Modules

This is an example of how to transfer a test image from the sender to the receiver with parameters specified in `gdmsend.cmd` and `gdmrecv.sh`.

Sample Test Configuration

- A multicast server, named mserver1 with an IP address of 192.168.1.4.
- A multicast client (used for testing) mclient1 with an IP address of 192.168.1.50.
- A multicast transfer will use the multicast address 231.1.222.8 and port of 9511.

You must start the receiver before the sender.

To start the receiver on the multicast client

1 Use the OS Manager media to boot the machine named mclient1.

2 At the boot prompt, type **`testmode`** and press **Enter** on your keyboard.

When Linux is finished booting, you will see the following on screen.

Use **Alt-F1**, **Alt-F2**, and **Alt-F3** to switch between virtual terminals.

Hold down the **Alt** key and press the **F2** key.

3 At the bash prompt (#), type **`cd /work`** and press **Enter** on the keyboard.

4 Type **`./gdmrecv.sh 192.168.1.4`** and press **Enter** on the keyboard. 192.168.1.4 is the NACK IP address for mserver1.

If you want to change parameters passed to `gdmcrecv`, use a nano editor to modify the shell script.

To start the sender on the multicast server

1 If necessary, change to the directory where the `gdmsend.cmd` is located.

2 From a command prompt, type **`gdmsend.cmd`** and press **Enter**.

10 Advanced Features

At the end of this chapter, you will:

- Be able to restore operating systems in a last resort situation.
- Be able to capture, recover or migrate user data and settings.
- Be able to use Client Operation Profiles with the CM OS Manager.

This chapter discusses advanced features that are available with the CM OS Manager. These features are for use by those who are extremely comfortable with CM.

Restoring Operating Systems

The CM OS Manager allows you to restore your operating system in last resort situations. Your operating system will be reinstalled, but *you will lose all data.*

Pre-requisite

- Create a CD-ROM from the `.iso` in the `\service` cd folder on the CM OS Manager media.

To recover your operating system

1. Insert the CD-ROM that you created from the `.iso` in the `\service_cd` folder on the product CD-ROM.
2. Boot the target device.
3. A menu opens with the following choices:
   - Service OS networking (default selection if no option is chosen)
   - Install OS from cache partition
   - Install OS from CD or DVD
4. If you select:

- **Service OS Networking** you must be connected to a network.

  If DHCP is found, you will be prompted for the CM OS Manager Server's IP address and then the appropriate OS image will be installed to your device.

  or

  If DHCP is not found, you will be prompted for network information such as the following before the appropriate OS image can be installed to your machine:

  - IP address for the target device
  - Default gateway

- Subnet
- Subnet mask
- DNS address
- CM OS Manager Server IP address

You may choose to store the network information on a floppy disk. To do this, prepare the following `.ini` files:

- `romsinfo.ini`
  This includes information about the CM OS Manager Server. It should be ordered from the top down with the most-specific information to the least-specific information. When a match to the CM OS Manager Server s found on the left, the information on the right will be used.

  In the sample romsinfo.ini file below:

  ```
  [ROMSInfo]
  192.128.1.99=192.168.123.*, 192.168.124.*, 192.128.125.*
  osm.usa.hp.com=192.168.*
  osm.hp.com=*
  ```

  - The first line looks at the machine to see if it falls within one of the subnets listed (192.168.123.*, 192.168.124.*, 192.128.125.*). The asterisk is used as a wildcard. If there is a match, then the machine will use the CM OS Manager Server with the IP address specified on the left (e.g., 192.128.1.99).
  - If no match is found, then the second line of the file is used. This one looks at the machine to see if it falls within a subnet that begins with 192.168.*. If so, the machine will use osm.usa.hp.com to find the CM OS Manager Server.
  - If no match is found again, the third line of the file is used. This one indicates that osm.hp.com should be used to find the CM OS Manager to be used by the machine, no matter what subnet it is part of.

  ```
  [ServiceCD]
  source=net
  netif=eth0
  ```

  - The first line defines where to get the image. Valid values are net, cd, or cache. Use this if you want to prevent the user from being prompted for this information.

- The second line defines which NIC to use. If there are multiple NIC cards and you do not specify this parameter, then the first NIC card that is discovered will be used. Valid values are eth0 – eth3.

— `netinfo.ini`
This includes the networking information. If there is more than one section (such as a [SubnetDisplayName2], you will be prompted about which information to use.

You can use `addr` to specify a range of IP addresses. This allows you to create one floppy disk that will be useful for multiple machines.

```
[SubnetDisplayname1]
addr=192.168.123.50-192.168.123.69
gateway=192.168.123.254
subnet=192.168.1.0
netmask=255.255.255.0
dns=192.168.123.1
```

If you do not know the DNS, leave the keyword `dns=` in the `.ini` file.

Insert your recovery CD-ROM and then insert the floppy disk shortly after the device begins to boot. When configuration is complete, you will see the message "Network configuration successful."

- Install OS from cache partition.

  If you have a target device that is managed by the CM OS Manager and you created a cache type partition as described in Table 9 on page 110, select this option to restore the operating system. You will be reminded that you will lose all data in the current partition. Then, you will see a message that says "Installing OS from cache partition". This remains on screen for several minutes. When it is done, a message says to see the logs and provides you with the ability to switch consoles. Remove the Service CD and reboot the machine.

- Install OS from CD or DVD

  If you have a target device that is managed by the CM OS Manager and you used the Download Resources task to create a CD or DVD, select this option to restore the operating system.

Addressing Requirements for Capturing, Recovering, and Migrating Data

If you want to capture, recover, or migrate user data and settings (such as personality information), HP provides the ROM Client method (romclimth.tkd), which has two exit points. This method is stored in *SystemDrive*:\Program Files\Hewlett-Packard\CM\Agent.

The exit points call two optional scripts—Novapdc.cmd (data capture) and Novapdr.cmd (data restore)—that must be also stored in *SystemDrive*:\Program Files\Hewlett-Packard\CM\Agent. You can use these scripts to customize data capture, recovery, and restoration for any product that you would like to use.

Capturing, recovering and migrating data relies on the CM OS Manager User Agent because data can be captured only when the OS is running. The CM Application Manager senses the change to a device's desired state and triggers the data capture if Novapdc.cmd is available in *SystemDrive*:\Program Files\Hewlett-Packard\CM\Agent. Then, the target device reboots and the new operating system is installed. If Novapdr.cmd is available, the ROM Client method begins the restore process after the OS has been installed on the target device.

Sample Command Lines

The following is a sample of a command line used to capture data using HP OpenView Configuration Management Settings Migration Manager.

```
Path\SE.exe /autoextract /http IntegrationServer:Port
UniqueName overwrite:yes /allusers
```

The following is a sample of a command line used to restore data using HP OpenView Settings Migration Manager.

```
Path\SE.exe" /autoinject /http IntegrationServer:Port
UniqueName /allusers
```

See HP OpenView Settings Migration Manager's documentation for more details.

Return Codes for HP Exit Points

The following return codes are returned from the HP exit points `Novapdc.cmd` and `Novapdr.cmd`. The values may vary depending on the software that you are using with these exit points. If the return value of the method is not equivalent to the following, use the standard batch error level conditional processing and the exit command to make them correspond to the following:

Table 16 HP Exit Point Return Codes

Code	Description
0	Successful.
1	An error occurred and will be logged, but processing will continue. The log is located in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log`.
2	For `Novapdc.cmd` (capture): • A fatal error has occurred and will be logged. The log is located in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log`. Processing of the service has ended. For `Novapdr.cmd` (restore): • An error has occurred and will be logged. The log is located in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent\Logs\romsclimth.log`. The service is flagged but at the next CM OS Connect, the CM Application Manager will attempt to install the service again.

Using CM Client Operations Profiles with CM OS Manager

CM Client Operations Profiles allow you to dynamically assign and select a target device's available Configuration Management servers based on network location, network speed, or other criteria. For example, you may want to use this capability to assign CM Proxy Servers to your managed devices or designate fail-over CM Proxy Servers. The ability to specify Service Access Points (SAPs) so that managed devices can access alternate sources for image download is a CM OS Manager-specific extension to CM Client Operations Profiles.

When using CM Client Operations Profiles with the CM OS Manager, the CM OS Manager uses only the CM Configuration Server specified in `roms.cfg`. Therefore, fail-over for multiple CM Configuration Servers is not supported.

If you are already using CM Client Operations Profiles, you must perform the following tasks to be properly configured for the CM OS Manager Server. Note that if CM Client Operations Profiles is already being used in your production environment, the CM Client Operations Profiles objects will be updated (date and time) once you modify the SAP class template.

Requirements

If you are using CM Client Operations Profiles for the CM OS Manager Server, you must use the same CM Configuration Server for both application deployment and operating system deployment.

You must observe the following constraints:

- Name instances in PRIMARY.CLIENT.LOCATION only by subnet.
- Specify only one CM Configuration Server.
- The ROLE attribute in the PRIMARY.CLIENT.SAP instance must be set to A.
- If you are using CM Client Operations Profiles, failover for CM OS Manager is supported in the following scenarios:
  - If the first SAP is a CD but there are no valid resources on the current CD or there is no CD.

— If there is more than one SAP for a CM Proxy Server, CM OS Manager will failover from one SAP to another, respecting the connection order in the LOCATION instance. CM Client Operations Profiles can only be used to redirect the CM Application Manager and/or CM OS Manager Server to an alternate image data source.

- If the TYPE attribute in the PRIMARY.CLIENT.SAP instance is set to DATA, then the ROLE attribute in this instance must be set to Z to limit its usage exclusively to CM OS Manager.
- If you are using Local Boot Service, each CM Application Manager must resolve only one SAP with the TYPE attribute set to ROM. This SAP's URI attribute will point to the CM OS Manager Server (**http://servernameORIPAddress:port**) and must be specified in lowercase.

Editing the Server Access Profile (SAP) Class

Before configuring CM Client Operations Profiles for use with the CM OS Manager, you must edit the PRIMARY.CLIENT.SAP class template to add some CM OS Manager-specific items.

Before you make any changes, be sure to back up your CM Configuration Server DB.

To edit your class template

1. Open the CM Admin CSDB Editor.
2. Go to PRIMARY.CLIENT.SAP and right-click **SAP**.
3. Select **Edit Class**.

   Select the TYPE attribute.

   `Type` specifies the type of Configuration Management server. The value `ROM` is for use only with Local Service Boot (LSB). You must specify the URL so that Local Service Boot can locate the CM OS Manager Server.

   Additional URLs for the Universal Resource Identifier are:

   — **URI=cdr://**
   Indicates the agent's local CD/DVD drive. The first CD/DVD drive detected is used.

   — **URI=smb://username=username,password=password //romssvr/c$**

Indicates a windows share that will be mounted. SMB (Server Message Block) is the Windows protocol used to mount shares.

— **URI=nfs://hostname/directory**
Indicates a network file share.

See About Local Service Boot on page 130 for more information.

4 Select the ROLE attribute and add Z as a valid option. The description should read as follows:

```
RCS Role A,O,S,M,R,D,Z
```

This field is a free-form entry, so this change to the class template is not required, but is recommended.

Specifies the role of the SAP. The value Z has been added for ROMS-only usage. The agent process ignores any SAP that has this value in ROLE.

5 Click **OK**, and then click **Yes** to confirm the changes.

Using Local Service Boot and CM Client Operations Profiles

If you are using the Local Service Boot, create an SAP instance with the following settings:

- TYPE=ROM
- ROLE=Z

Using the CM Proxy Server with CM OS Manager Server and CM Client Operations Profiles

If you have a CM Proxy Server that contains OS images and applications, you would set up your SAP instances as follows:

- For the CM Proxy Server that contains OS images, create an SAP instance with the following settings:
  - TYPE=DATA
  - ROLE=Z
- If there is a CM Proxy Server that contains the all other data (such as applications), create the SAP instance with the following settings:
  - ROLE=D

- If there is a CM Proxy Server that contains all data, create SAP instances with the following settings
  - ROLE=DZ

11 About Double Byte Character Support

At the end of this chapter, you will:

- Know what languages are supported.
- Be able to add support for a supported language in a PXE environment.
- Be able to add support for a supported language when restoring from a CD-ROM.

This chapter discusses the changes made to the CM OS Manager for internationalization. These changes set the locale for the service operating system (SOS) and CM OS Manager System Agent messaging.

When creating an image (with the CM Image Preparation Wizard or the CM Windows Native Install Packager) the locale for your reference and target devices must match. For example, if you want to create a Simplified Chinese OS image, you must run the CM Image Preparation Wizard or the CM Windows Native Install Packager on a Simplified Chinese reference machine.

If there are no double-byte requirements, do not make any of the following changes.

Supported languages

Simplified Chinese, Japanese, and Korean

Changing the locale

To add support for Simplified Chinese, Japanese or Korean in a PXE environment

1. Use a UNIX based text editor to open `C:\Program Files\Hewlett-Packard\CM\BootServer\X86PC\UNDI\linux-boot\linux.cfg\default`. The file looks similar to the following:

   ```
   DEFAULT bzImage

   APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1 ISVRPORT=3466
   ```

   Add the LANG parameter to the end of the APPEND line and set it to LANG=CJK. As a result, the file will look similar to the following:

   ```
   DEFAULT bzImage

   APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1 ISVRPORT=3466 LANG=CJK
   ```

2. Save and close the default file.

To add support for Simplified Chinese, Japanese, or Korean when restoring from the Service CD-ROM

- Specify LANG=CJK in the ServiceCD section of the `romsinfo.ini file`.

Setting the System Language Parameter

In this section, you will set the System Language parameter in the Behavior instance. Doing so sets the locale for the service operating system and CM OS Manager System Agent messaging. This affects PXE environments, LSB environments and restoring operating systems from a CD-ROM or DVD.

To set policy to enable support for other languages

1. Log in to the CM Portal as the CM OS Manager Administrator (by default the user id is **`romadmin`** and the password is **`secret`**).
2. Use the navigation aid to select the appropriate CM Configuration Server.
3. In the workspace, click **Behavior**.
4. Click the appropriate instance in the workspace and then click **Modify** to make changes.
5. Click **Advanced** to open the Advanced Properties section.
6. Change the System Language parameter to the appropriate language.
   - en_US = English
   - zh_CN = Simplified Chinese
   - ja_JP = Japanese
   - ko_KR = Korean

7 Set policy to deploy the images to the appropriate users.

Double-byte support for Sysprep or Unattend.txt files

If using double byte char in Sysprep or unattend.txt the file must be encoded in UTF-8 coding.

12 Troubleshooting

At the end of this chapter, you will:

- Know where to find the CM OS Manager Server logs.
- Know where to find the CM Configuration Server and CM Configuration Server DB logs.
- Know where to find the CM Image Preparation Wizard log.
- Know where to find the CM agent logs and objects.
- Know where to find the logs created when capturing, migrating, or recovering data.
- Be familiar with some basic infrastructure tests to determine whether your environment is configured properly.
- Understand what to provide to Technical Support when requesting help.
- Know what the Discover Boot Server Utility is and how to use it.

CM OS Manager Server Logs

The CM OS Manager Server writes several logs, which can be used to track progress and diagnose problems. The log files for the CM OS Manager Server are:

- `httpd-`*`port`*`.log`
  This is the main log, stored by default in *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\logs`. It contains information about the actions that you perform, as well as version and build numbers.

  Replace *`port`* with your port number, for example, `httpd-3466.log`.

  Each time you start the web server a new log is written. The old log is saved as `httpd-`*`port`*`.nn.log`.

- `httpd-`*`port`*`.YY.MM.DD.log`
  This log, stored by default in *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\logs`, contains the web server activity for each day. If the log is empty, it means that there was no activity that day.

- `httpd-`*`port`*`.error.txt`
  This log, stored by default in *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\logs`, contains messages written to any logs that contain the prefix ERROR. This allows you to view all errors in a single location.

- `machineID.log`
  This log, stored by default in *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\IntegrationServer\upload`, is a comprehensive log that is written after the CM OS Manager System Agent is executed. You will find one log for each device managed by the CM OS Manager. Open this log with WordPad, rather than Notepad.

  This log may be named `macAddress.log` if the machine instance has not been created.

  The following example from this log shows that the CM Configuration Server and CM Proxy Server address are in use, which confirms a successful image deployment.

```
20030703 10:10:01 Info: ::HOSTINFO(RADIA CONFIGURATION
SERVERHOST)
:10.10.10.2:3464
```

```
20030703 10:10:01 Info: ::HOSTINFO(RPSHOST)
:10.10.10.2:3466
```

CM Configuration Server and CM Configuration Server DB Logs

- `Nvdmr000.log`
  This log displays detailed information including version information and information about CM OS connects and is stored by default in *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\ConfigurationServer\log`.
- `import.log`
  This log displays the results of the database import and is stored by default in *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\ConfigurationServer\bin`.

CM Image Preparation Wizard Log

- `setup.log`
  This log is created if there is an error while the CM Image Preparation Wizard is running in Windows. It is located in the directory specified by the user's TEMP environment variable. It may be in a location similar to `c:\winnt\temp\setup.log`.

  `osclone.log`
  This log is created only if an error occurs when the CM Image Preparation Wizard reboots to Linux. This log to uploads to the `\upload directory` as *`imagename`*`.log`.

CM agent Logs and Objects

Use the CM agent logs (*`SystemDrive`*`:/Program Files/Hewlett-Packard/CM/Agent/Logs`) and CM agent object information (*`SystemDrive`*`:/Program Files/Hewlett-Packard/CM/Agent/LIB`) on the managed device to confirm that the following CM OS Manager Server services have installed successfully during the first CM agent connect:

- Operating System Service
- CM OS Manager Server agent files

If policy dictates that the Local Service Boot service is installed, you can also confirm that the LSB service has been installed.

You may want to review the following CM agent logs located in *SystemDrive*:\Program Files\Hewlett-Packard\CM\Agent\Logs:

- Connect.log
- Romsclimth.log
  This log stores information about operating system (OS) service resolution.
- LSB.log
  This log contains information about LSB installation.

You may want to review the following agent object information (located in *SystemDrive*:\Program Files\Hewlett-Packard\CM\Agent\LIB):

- OS/ZSERVICE/MASTER.edm
  Review the ZMASTER object for the OS Service.

Capturing, Migrating, or Recovering Data

If you use this capability, logs will be available in C:\Program Files\Hewlett-Packard\CM\Agent on the managed device.

Basic Infrastructure Tests

After you have installed your CM OS Manager Server infrastructure, the following tests may help you to determine whether your environment is properly configured.

Test 1: For use in an environment without bare metal machines

If you can answer yes to all of the following questions:

- Are you able to boot (via PXE) to a device that has not been discovered by CM OS Manager Server and does not have an OS that is managed by CM OS Manager Server?
- Does a ROM object get created in the CM Configuration Server when a device is discovered?
- When a device is discovered, is a log uploaded to the CM Integration Server's \upload directory?

Then the following are working correctly:

- DHCP, PXE, CM Configuration Server, and TFTP are working correctly.
- The CM Configuration Server is correctly forwarding methods, processes, and the MACHINE class' NULL instance to the CM Integration Server.
- The CM Configuration Server has the files needed to handle CM OS Manager Server objects.
- The Linux kernel supports the hardware in the machine.
- CM OS Manager Server appears to be configured correctly.

Test 2: For use in an environment with bare metal machines

If you can answer yes to all of the following questions:

- Are you able to boot a bare metal machine via PXE?
- Does a ROM object get created in the CM Configuration Server when a device is discovered?
- When a device is discovered, is a log uploaded to the CM Integration Server `\upload` directory?
- Is an OS installed on the machine?

Then:

- DHCP, PXE, CM Configuration Server, CM Proxy Server and TFTP are working correctly.
- The CM Configuration Server is correctly forwarding methods, processes, and the MACHINE class' NULL instance to the CM Integration Server.
- The CM Configuration Server has the necessary files to handle CM OS Manager Server (COP) objects.
- Linux kernel supports the hardware in the machine.
- CM OS Manager Server appears to be configured correctly.
- OS Policy correctly chose one OS.
- The OS State for the MACHINE instance is set to DESIRED.

Test Results

If any of the tests failed, you may have some problems with your infrastructure. Be sure to collect the following information:

- How are you trying to set up the infrastructure?

- In what order did you install the components?
- Gather the necessary logs related to your problem.

Collecting Information for Technical Support

If you need to contact Technical Support for assistance, be sure to review the latest release notes and confirm that you have installed any fixes. If you still need assistance, then collect the following information:

- Hardware information (including manufacturer, model, BIOS/firmware version for the NIC card, hard drive controller card, and hard drive).
- Gather the following files or folders:
  - *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntergrationServer\upload\machineID.log
  - *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer\logs directory

    or

    SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\RomVer.log
  - *SystemDrive*:\Program Files\Hewlett-Packard\CM\ConfigurationServer\log\nvdmr000.log
  - If specifically requested, gather the .MBR and .PAR files from *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer\UPLOAD on the RPS\RIS server
- What results you were expecting, what actually happened, and any other related details.
- Whether the problem can be reproduced. If so, specify the exact steps (providing detailed information) to reproduce the issue.
- Specify whether the issue occurs on more than one device.
- Indicate whether the image was ever successfully deployed. If so, what has changed since the successful deployment?
- If deployment of an image stops and goes to a bash prompt, be sure to collect the OSSELECT.log file. Use the following command to copy the OSSELECT.log to the CM Integration Server \upload folder:

```
curl -T osselect.log
http://$ISVR:$ISVRPORT/upload/osselect.log
```

Gathering Version Information

CM OS Manager Server Components

To determine the versions of the CM OS Manager components, go to *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer and run Romver.cmd. The log is created in the same directory.

CM OS Manager Admin Module

To determine the versions of the CM OS Manager Admin Module components, go to *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer and run Romadver.cmd. The log is created in the same directory.

To determine the versions of the CM Configuration Server, go to *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer and run Rcsver.cmd. The log is created in the same directory.

NVDKIT.EXE and .TKD Files

There are several ways to view version and module information for nvdkit.exe and the various .tkd files.

- In the banner area of the CM Portal, click  .
- Open a command prompt and navigate to the location of nvdkit.exe (by default, *SystemDrive*:\Program Files\Hewlett-Packard\CM\IntegrationServer. Then, type the following to get the corresponding module and version information:

  a nvdkit.exe
  Type **nvdkit version** and press **Enter**.

b `expandsmbios.tkd`
Type **`nvdkit version modules\expandsmbios.tkd`** and press **Enter**.

c `roms.tkd`
Type **`nvdkit version modules\roms.tkd`** and press **Enter**.

d `roms_udp.tkd`
Type **`nvdkit version modules\roms_udp.tkd`** and press **Enter**.

- See the `httpd-port.log` for version and build information.

CM Configuration Server

To check the version of your CM Configuration Server:

- Go to *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\ConfigurationServer\bin` and open `version.nvd`.

  or

- Go to *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\ConfigurationServer\log` and open `nvdmr000.log`.

  or

- Go to *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM\ConfigurationServer\bin` and run `Rcsver.cmd`.

CM Configuration Server DB

To check the version of your CM Configuration Server DB, use the CM Admin Configuration Server DB Editor to view the PRIMARY.SYSTEM.DBVER class. The DBVER attribute specifies the current version of your database. Refer to the *HP OpenView Configuration Management Configuration Server Database Reference Guide (CM CSDB Reference Guide)*.

CM OS Manager System Agent

To determine the version of the CM OS Management System Agent that you are running, you can use a text editor to open *`SystemDrive`*`:\ Program Files\Hewlett-Packard\CM \IntegrationServer\upload\machineID.log`. The line will read similar to the following:

```
20030905 19:02:35 Info: ROMA Version 1.3.1 Build 2 running
```

CM OS Manager Boot Loader

The version of CM OS Manager Boot Loader is displayed during the boot sequence. This information is not written to a log. Therefore, to find out the version number, you should do a PXE boot and one of the first lines will contain the version number.

Frequently Asked Questions

- Can I upgrade from my previous version?
  Yes, an upgrade process is available for upgrading from version 2.1 to 5.00. See the *HP OpenView Configuration Management OS Manager for the Windows operating system Migration Guide*.
- Are all OSs eligible for deployment?
  The eligible OSs are Windows 2000 Professional, Windows 2000 Server, Windows XP Professional, and Windows Server 2003.
- Can you use varying versions and builds of the OS Manager Server modules?
  Mixing and matching CM OS Manager Server modules is not supported unless you are directed by HP's Technical Support team to do so.
- Will my data partitions be captured with the system partition during the Image Preparation process?
  Multiple partitions on the source image will cause image deployment failures. Remove all partitions on the source other than the one that you want to capture. It is recommended that the partition contain only 100 MB of free space.
- Are dynamic disks supported with OS Manager Server?
  Not yet.
- What if I want to kick off a batch file to execute a backup program before sending a new image to a machine?
  Use the exit point (`Novapdc.cmd`). Rename your batch file (which contains the backup program) to `Novapdc.cmd` and store it on the target device in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent`. This will run before the new OS is deployed.
- What is the best way to size down a partition on a source machine?
  Use the option in the Image Preparation Wizard. If you do not use this you can use Partition Magic or another vendor's non-destructive partitioning. You can also Fdisk the partition to the correct size prior to installation of OS.
- Do I need to restart the CM Integration Server?
  If the CM OS Manager Server is being added to a CM-IS process that is already running another product then the `Roms.tkd` must either be explicitly loaded or the CM-IS restarted. However, for the current release it's recommended to avoid running the CM OS Manager Server in the same CM-IS process with other products. The other CM-IS products

include the CM Proxy Server, CM Portal, and the CM OS Manager Admin Module.

Changes made to the CM Integration Server `.cfg` files require a restart to implement the changes.

- What protocol is used to download the Linux service OS in a PXE-based implementation?
  The Linux service OS is served by the TFTP server using TFTP protocol.
- What protocol is used to download an OS image?
  HTTP.
- What must be enabled in a router to allow PXE to traverse subnets?
  The DHCP helper, which allows traversal of broadcast traffic on the DHCP ports, since broadcast is typically turned off on routers.
- What are the conditions in which the CM OS Manager System Agent will be booted on a machine?
  - If the CM OS Manager Boot Loader decides it must continue the boot process because there is no OS or it is invalid.
  - If NEXTBOOT = _SVC_LINUX_ in `Rombl.cfg`.
  - If the OSSTATE variable for the target device has been set to _INVALID_ in the CM Portal.
- Why is my TFTP server shutting down after starting?
  You may have another TFTP server running on the same computer.
- How can I check that the Boot Server is successfully installed?
  Press **Ctrl** + **Alt** + **Delete**, go to Task Manager, and review the list of Processes. `PXE.exe` and `Inetd.exe` should be running.

  or

  Go to the Event Viewer and check the application events. You will see when the process starts. Entries for problems will appear soon after the event starts.

  or

  In Windows 2003, go to a command prompt and type **`netstat /all`**. If you find `boot.ps` and `tftp`, the installation was successful.
- How do I know if the appropriate port is listening?
  From the command prompt `netstat -a`,
  you will receive a list of the ports and an indication of whether they are listening.

- What do I do if I receive a message that says "Checking Machine Status Times Out" or "Cannot find ROMS infrastructure?"
  You may receive this message if you're blocking ports or using a firewall. Be aware that you must be using both UDP and TCP. Verify that your ports are open, in particular ports 3466, 3471 and 2074. Go to the .cfg for each CM-IS product that you are running and find the value for the port. After you know which port isn't working, you can check your firewall to make sure it's not blocking the specified port.
- What do I do if I receive a message similar to the following during image deployment:

```
20061127 13:37:18 Info: *** Installing Standard Image

20061127 13:37:18 Error: InstallNvdm: An error occured
retrieving Current Partition information, err:

sfdisk: ERROR: sector 0 does not have an msdos signature

20061127 13:37:18 Info: Partitioning Hard Disk 20061127
13:37:18 Info: rpsadr: CCMSERVER:3467

20061127 13:37:18 Info: rpshost: CCMSERVER

20061127 13:37:18 Info: rpsport: 3467

20061127 13:37:18 Error: GetState Error: couldn't open socket:
host is unreachable

20061127 13:37:18 Error: Please check the Server configuration

20061127 13:37:18 Error: InstallNvdm: Error getting partition
information

20061127 13:37:18 Info:

20061127 13:37:18 Info: > sending AppEvent to
http://CCMSERVER:3461/proc/appeventxml

20061127 13:37:18 Info:

20061127 13:37:18 Error: Error sending AppEvent: couldn't open
socket: host is unreachable

20061127 13:37:18 Error: InstallOSerr: Error(s) occurred
during OS install, stopping

20061127 13:37:18 Error: This machine is in the process of
having an OS installed. However, a critical aspect of the
installation has failed. The machine will shut down until an
administrator fixes the problem and performs a Wake On LAN.
Please contact your adminstrator.

20061127 13:37:18 Info: *** Start of Update Machine
=======================*** Start of Update Machine
=======================
```

Check the configuration of your DNS server. Depending on the configuration, you may experience difficulties working with the short name and may need to use the IP address or fully qualified name.

Using the Discover Boot Server Utility

Use the following command to send out a DHCP discover request in order to identify the PXE servers that are in the environment. This is an essential command when trying to determine if a machine is able to access the PXE server.

```
./discoverbootserver.sh
```

Note that the results may be complicated to read. Contact Technical Support for more information.

A AppEvents

The following AppEvents are stored in the Events section in the ROM object.

Table 17 AppEvents

Message	Description
Previous install without ROM object	An OS was installed by the CM OS Manager Server, but the ROM object has been deleted.
UNMANAGED_OS_ resolved	An _UNMANAGED_OS_ was resolved for the device and administrative action is required.
No OS resolved	No OS was resolved for the device and administrative action is required.
No OS selected	No OS was selected for this device and administrative action is required. This can occur when multiple OSs resolve and the behaviors are configured for CENTRAL selection. The administrator must arbitrate the OS.
No OS resolved, unusable, shutdown	Device does not have a valid operating system. No OS was resolved so the device cannot be used.
Multiple OSs resolved and central control	Multiple OSs were resolved for this device and administrative action is required because the user was not given the option to select the OS.
No to install	A valid OS exists on the device and the user responded No to the prompt to perform an OS installation.
CD install, no CD drive	A CD-based installation was requested but no CD-ROM drive exists on the machine.
Partition error	The CM OS Manager System Agent was unable to retrieve partition information (file retrieval problem).

Message	Description
Boot partition problem	The CM OS Manager System Agent was unable to determine the boot partition after the disk was partitioned.
Error installing image	The CM OS Manager System Agent received an error while installing the OS image.
Error Installing MBR	The CM OS Manager System Agent encountered an error while installing the Master Boot Record (MBR).
unattend.txt error	The `unattend.txt` file could not be retrieved from the server.
Sysprep.inf error	The `sysprep.inf` file could not be retrieved from the server.
Successful	OS was successfully installed.
No OS has been resolved - RSLVDOS set to _NONE_	No policy has been assigned to this device and nothing will happen until policy is assigned.
Admin activity required - No OS has been selected	During policy resolution, no eligible OS was found for the device. The device may have no local OS or the device may be managed but the OS is in need of repair (_INCONSISTENT_OS). The device is unusable and the CM OS Manager does not know how to proceed. Therefore, the device has been turned off until the administrator changes policy and sends a WOL to the machine.
OS: *`NameOfOperatingSystem`* has been installed	The selected OS has been installed successfully.

Message	Description
Admin activity recommended - OSSTATE set to _INCONSISTENT_	On a managed device that was in its desired state, `Rombl.cfg` was lost. This may indicate serious corruption and therefore, the CM OS Manager changed the value of OS State to _INCONSISTENT_ and will allow the device to be used "as is". If possible, during the next CM OS Connect, `Rombl.cfg` will be recreated. If this does not happen, the administrator should force a reinstall of the OS.
Admin activity required - _UNMANAGED_OS_ is selected where an OS is to be installed	_UNMANAGED_OS was resolved for the device because it has no OS or because the device is managed but the OS must be repaired (_INCONSISTENT_OS). The device is unusable and the CM OS Manager does not know how to proceed. Therefore, the device has been turned off until the administrator changes policy and sends a WOL to the device.
OSSTATE has been set to _DESIRED_	The OS has been installed according to policy.
Admin activity required - no eligible OS, unusable device, device shutdown	During policy resolution, no eligible OS was found for the device. The device may have no local OS or the device may be managed but the OS must be repaired (_INCONSISTENT_OS). The device is unusable and the CM OS Manager does not know how to proceed. Therefore, the device has been turned off until the administrator changes policy and sends a WOL to the machine.
SLCTDOS has been set to _UNMANAGED_OS_	During policy resolution, no eligible OS was found for the device, which has an existing valid, but unmanaged, OS. The device has been set to _UNMANAGED_OS_ to allow the device to be used as is until admin changes policy.

Message	Description
Admin activity required - Multiple OSs resolved and central control	During policy resolution, several eligible OSs were found for the device. However, the behavior setting does not allow for user selection of the OS. Therefore, the administrator must intervene and determine what OS should be installed on the device. Until then, the device is usable as long as the OSSTATE is not set to INVALID.
OS: *NameOfSelectedOS* has been selected to be installed	Displays the OS that has been selected to be installed on the device.

B User Messages

The following messages may be displayed to the user. If the message does not require a response from the user, the message displays for the number of seconds specified in the USERTO attribute in the BEHAVIOR class and then the machine will shut down. If USERTO is set to –1, then the machine will wait for a user response indefinitely.

Table 18 Messages for Timeouts

Messages	User Action
This machine contains a factory pre-imaged OS that is managed by the CM OS Manager. The CM OS Manager System Agent is unable to connect to the CM OS Manager infrastructure to configure this machine. The machine cannot be used. The system will retry later.	N/A
The local machine does not contain a usable OS. Networking problems prevent the CM OS Manager System Agent from connecting to the CM OS Manager infrastructure in order to install an OS on this machine. The machine cannot be used. The system will retry later.	N/A
The local machine contains a usable OS. Networking problems prevent the CM OS Manager System Agent from connecting to the CM OS Manager infrastructure to determine policy for this machine. The machine will be booted to the local Operating System.	N/A
This machine has an operating system but is new to the CM OS Manager. It contains an active, bootable partition but no management marker (rombl.cfg). It cannot be determined whether an operating system should be reinstalled according to policy or whether the existing operating system should continue to be used. Please select "install" to reinstall or "use" to keep as is.	Select **install** to install the resolved OS, or select **use** to continue to use the existing OS.
This machine is new to the CM OS Manager. The attempt to register this machine in the device information repository failed and it is not allowed be used. The system will retry later.	N/A

Messages	User Action
Please select one of the following roles which will be used, along with other policy criteria, to determine the correct configuration for this machine.	Select a role.
This machine has no local OS or the OS is invalid. An OS must be reinstalled. Policy indicates that there are no eligible OSs assigned to this machine. The administrator should verify that at least one of the OSs selected for this machine have the following characteristics: ACPI: $::acpi APIC: $::apic Minimum CPU speed: $::cpuspeed Minimum RAM size: $::mem Boot Hard Drive Type: $::boottype Minimum Hard Drive Size: $::hdsize The machine cannot be used and will shut down until an administrator specifies policy and performs a Wake On LAN.	N/A
The current state of this machine is unusable. Policy returned multiple OSs for this machine. The machine will shut down until an administrator selects an eligible OS and performs a Wake On LAN.	N/A
The current state of this machine is unusable. Policy returned multiple Hardware Configurations for this machine. The machine will shut down until an administrator selects an eligible Hardware Configuration and performs a Wake On LAN.	N/A
Policy requires that the OS must be reinstalled on this machine. Select an OS from the following list:	Select an OS.
Policy requires that the Hardware Configuration must be reinstalled on this machine. Select a Hardware Configuration from the following list:	Select a Hardware Configuration.
This machine has no local OS or the OS is invalid. It must be reinstalled. However, no eligible OSs have been returned for this machine. The machine cannot be used and will shut down until an administrator changes policy and performs a Wake On LAN.	N/A

Messages	User Action
This machine has no local OS or the OS is invalid. It must be reinstalled. However, the intended OS for this machine cannot be determined due to an error during resolution. The machine cannot be used and will shut down until an administrator changes policy and performs a Wake On LAN.	N/A
Policy requires that the OS for this machine must be reinstalled. Is it ok to install the new OS now?	Indicate whether it is okay to continue the installation.
Policy requires that the OS for this machine should be reinstalled. The selected OS is the same as the currently installed OS. Do you want to use the current installation or do you want to refresh the OS?	Specify whether to use the existing installation or to refresh the current OS.
This machine is in the process of having its Hardware Configuration modified. However, a critical element of the configuration has failed. The machine will shut down until an administrator fixes the problem and performs a Wake On LAN. Please contact your administrator.	N/A
This machine is in the process of having an OS installed. However, a critical aspect of the installation has failed. The machine will shut down until an administrator fixes the problem and performs a Wake On LAN. Please contact your administrator.	N/A
This machine is in the process of having its Hardware Configuration modified. However, a critical Hardware Configuration Element has failed due to incorrect or corrupt instructions. The machine will shut down until an administrator fixes the problem and performs a Wake On LAN. Please contact your administrator.	N/A

C Storing Multiple Logs

Typically, logs stored on the CM OS Manager Server after an OS installation are rewritten with each installation. Now, you have the option to store multiple logs per machine on the CM OS Manager Server.

To store multiple logs on the CM OS Manager Server

1. Use a text editor to open `SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\put.cfg`.

```
# ------------------------------------------------------------------------
# - RIS Put Server - for file uploads
#
#   Put::cfg array is used by the PutEnter proc to allow a user-specified
#   number of previous files with the identical name to be saved.
#       -ROLLOVER is the max number of files to keep, each file has the
#           same root name with the suffix of .1, .2, etc.
#       -TYPELIST may include any number file extensions: e.g., ".log .txt .edm"
#   The default of -ROLLOVER is 0 (zero) and only the current version is stored.
# ------------------------------------------------------------------------

file mkdir [set dir $Config(ROOT)/upload]

Put_AddRoot /upload $dir

namespace eval Put {
    array set cfg [list \
        -ROLLOVER   0   \
        -TYPELIST   ".log"
    ]
}
```

2. Set -ROLLOVER to the number of logs that you want to be able to store. For example, if you set –ROLLOVER to 3, you will be able to store and review the previous three actions performed on the target device.

D Product Name Changes

If you have used Radia in the past, and are not yet familiar with the newly rebranded HP terms and product names, Table 19 below will help you identify naming changes that have been applied to the Radia brand.

Table 19 Product Name and Term Changes

New Name/Term	Old Name/Term
CM agents	Radia clients
HP OpenView Configuration Management	Radia
HP OpenView Configuration Management Admin CSDB Editor	Radia System Explorer
HP OpenView Configuration Management Admin Publisher	Radia Publisher
HP OpenView Configuration Management Application Manager	Radia Application Manager,
HP OpenView Configuration Management Configuration Server	Radia Configuration Server
HP OpenView Configuration Management Configuration Server Database	Configuration Server Database, Radia Database
HP OpenView Configuration Management OS Manager	Radia OS Manager
HP OpenView Configuration Management Solutions for Servers	Server Management
HP OpenView Configuration Management Portal	Radia Management Portal

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W