HP Client Automation Enterprise

Portal

for the Windows® operating system

Software Version: 7.50

Installation and Configuration Guide

Manufacturing Part Number: none

Document Release Date: June 2009

Software Release Date: May 2009

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

DHTML Calendar

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
  - The number before the period identifies the major release number.
  - The first number after the period identifies the minor release number.
  - The second number after the period represents the minor-minor release number.
- 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:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

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 Document Changes

Chapter	Version	Change
All	7.50	The Portal provides the underlying engine, web-services, and OpenLDAP Zone directory of managed devices to support HP Client Automation environment. The HPCA consoles or the CSDB Editor now provide the user interfaces for all tasks previously available from the Portal. All references to using the Portal as a front-end user interface have been removed from this guide. Refer to the *HPCA Enterprise Manager User Guide* and the *HPCA OS Manager System Administrator Guide* for new ways to perform the tasks previously performed from the Portal interface.
All	7.20	HP Configuration Management was renamed to HP Client Automation for this release. Note that not all components and products were re-branded.

Chapter	Version	Change
Chapter 1	7.20	Page 14, Using this Guide with Core and Satellite Servers, new topic.
Chapter 1	7.50	Page 15, IP Networking Support, new topic.
Chapter 1	5.10	Page 25, System Requirements have changed for this release. Page 26, Directory Size of a Single Zone, the maximum recommended size of a single Zone has increased to 50,000 devices.
Chapter 3	7.20	Page 36, About the Zone Containers, the *Cross-References Container* (cn=xref) has been renamed the *Device Categories* Container (cn=xref) as of Version 7.20.
Chapter 3	5.10	Page 49, Setting Additional Configuration Parameters, added the following rows to Table 3: RCS_AUTO_CONNECT – used to automatically connect to the Primary ds-rcs whenever the startup property is Auto or Manual; REFRESHMSC – used to adjust how often the Managed Services Catalog is refreshed with the available managed-services in the Primary Configuration Server database.
Chapter 3	5.10	Page 53, Directory Service Connection Status upon Portal Restart, added topic and Tables 11, 12, and 13 to summarize the conditions under which a Directory Service is reconnected to the Portal upon restart.
Chapter removed	7.50	The Operations chapter has been removed from this guide. Refer to the Enterprise Manager or Core and Satellite User Guides for new ways to perform the tasks previously performed from the Operations tasks of the Portal interface.
Chapter 5	7.50	Page 78, Managing the Portal Web Services Token, new topic allows you to adjust the session timeout period related to the Portal Web Services credentials.
Chapter 5	5.10	Page 75, Portal Directory Troubleshooting, added topic for troubleshooting the Slapd service, adjusting the OVCMLDAP_HEARTBEAT_INTERVAL, and starting and stopping logging for the Slapd and related services.

Chapter	Version	Change
Chapter 5	5.10	Page 77, Managing Portal Agent Signal Processing, new topic defines the rmp.cfg parameters that specify the the number of dedicated threads available to handle incoming RMA requests, RMA processing requests, and RMA registration requests.

Support

You can visit the HP Software support web site at:

www.hp.com/go/hpsoftwaresupport

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 an active support contract. To find more information about support access levels, go to the following URL:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to the following URL:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Introduction

At the end of this chapter, you will:

- Understand the benefits and core capabilities of the HP Client Automation Portal (Portal).
- Understand the architecture and directory structure of any Portal Zone.
- Be familiar with new terminology for this release.
- Understand the process of adding devices to your Portal Zone and grouping them for operational purposes. Creating and using device groups for administrative and operational tasks greatly improves Portal performance.

The Portal performs best when operations are run against groups of devices, as opposed to running the same operation against one device at a time.

Introduction

As of Version 7.50, the Portal is a backend component of any HP Client Automation environment that provides an engine, Web Services, and an OpenLDAP database for the devices being managed in your environment.

The Portal provides the following benefits:

- **Web-based administration**
  Use a browser from anywhere to administer your Client Automation infrastructure.
- **Role-based entitlement**
  Administrators can view and manage only those objects in the infrastructure for which they are responsible.
- **Security**
  Administrators are authenticated against the Portal Directory.
- **Extensibility**
  Access any Configuration Server, Configuration Server DB, Active Directory, or other LDAP Directory in your enterprise from within the Portal's interface. Administer policy, services, users, and machines directly from the Portal's user interface.
- **Enterprise-Wide Solutions**
  Create multiple Portal Zones, if desired, to administer the infrastructure at different sites in your enterprise. From any Portal, you can access any Zone in your enterprise and perform operations across multiple-zones.

Using this Guide with Core and Satellite Servers

⚠ If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started and Concepts Guide* as the installation, configuration, and troubleshooting information in that guide overrides the information in this guide.

IP Networking Support

With this release, HP Client Automation adds support for **IPv6**—the latest version of the internet protocol addressing structure—to its Windows-based Core and Satellite servers. The Core and Satellite servers can now use either IP version 4 (**IPv4**) or IP version 6 (**IPv6**) for server-to-server communications. HPCA agent communications, however, are currently limited to IPv4. For details, refer to the appendix, *IPv6 Networking Support*, in the *HPCA Enterprise Core and Satellie Servers User Guide*.

HP Client Automation environments that use the traditional, component-based, HPCA server installations will continue to be supported on IPv4 only.

About the Portal Capabilities

After installing the Portal, you can perform administrative and operational tasks from a Core Console or from an Enterprise Manager console on any piece of your Client Automation infrastructure. The capabilities of the Portal include:

- **Network Discovery**
  The Portal engine automatically discovers the objects in your networks.
- **Authentication**
  Entries in the Portal Directory to authenticate administrators. These are entered from the Core Console or Enterprise Manager Console.
- **Supports the Remote Installations of Client Automation**
  Other HPCA consoles rely on the Portal in order to install Client Automation products or components to remote devices.
- **Device Categories**
  The Portal captures detailed information about device hardware, operating system, Client Automation infrastructure and managed services and stores it in the Portal Directory in self-managed device categories. This simplifies notification of all devices for a given classification in a single step.
- **OpenLDAP Directory for Device and Group Tasks**
  From the Enterprise Manager or Core console, many activities, such as Notify, are performed on the target device groups that you select. The

Portal provides the OpenLDAP directory hosting the device and device groups.

About the Product Architecture

Although you will work with the Portal in your web browser, you may want to be familiar with its base architecture.

The Portal contains the following:

- The **Portal Run-time** contains the HPCA Portal service (httpd-managementportal) and the `RMP.TKD` module (located in the `\modules` directory).
- The **Portal Zone Directory**, is an OpenLDAP directory service in the Portal's `\etc\openldap` directory. When the Portal starts, it loads the database objects that represent a given instance of the Portal, or Zone. The database objects include all information needed to manage a given set of infrastructure at a given location:
  - Managed devices
  - Device group memberships
  - Chassis container for blade enclosures and racks
  - Device Categories
  - Job Status and Job History
  - Users
  - Configurations for Entitlements, Tasks, and Services
  - Networks

  Whether you have one or many Portal Zones in your enterprise, all zones load the same-named set of containers at startup.
- The **Portal Agent**, installed on the remote devices when the HPCA Agents are installed, performs tasks on behalf of the Portal.

Portal Zones Overview

Very large enterprises often find it necessary to use multiple Portals to effectively view and manage their existing infrastructure. With multiple portal sites, it becomes desirable to be able to perform operations across all sites from one central location. This release extends the scalability of the Portal by defining a zone and a specific zone directory structure for each Portal in your enterprise.

What is a Zone?

A **zone** is a logical set of devices, infrastructure, and software that is represented and managed in directory services and administered by the Portal.

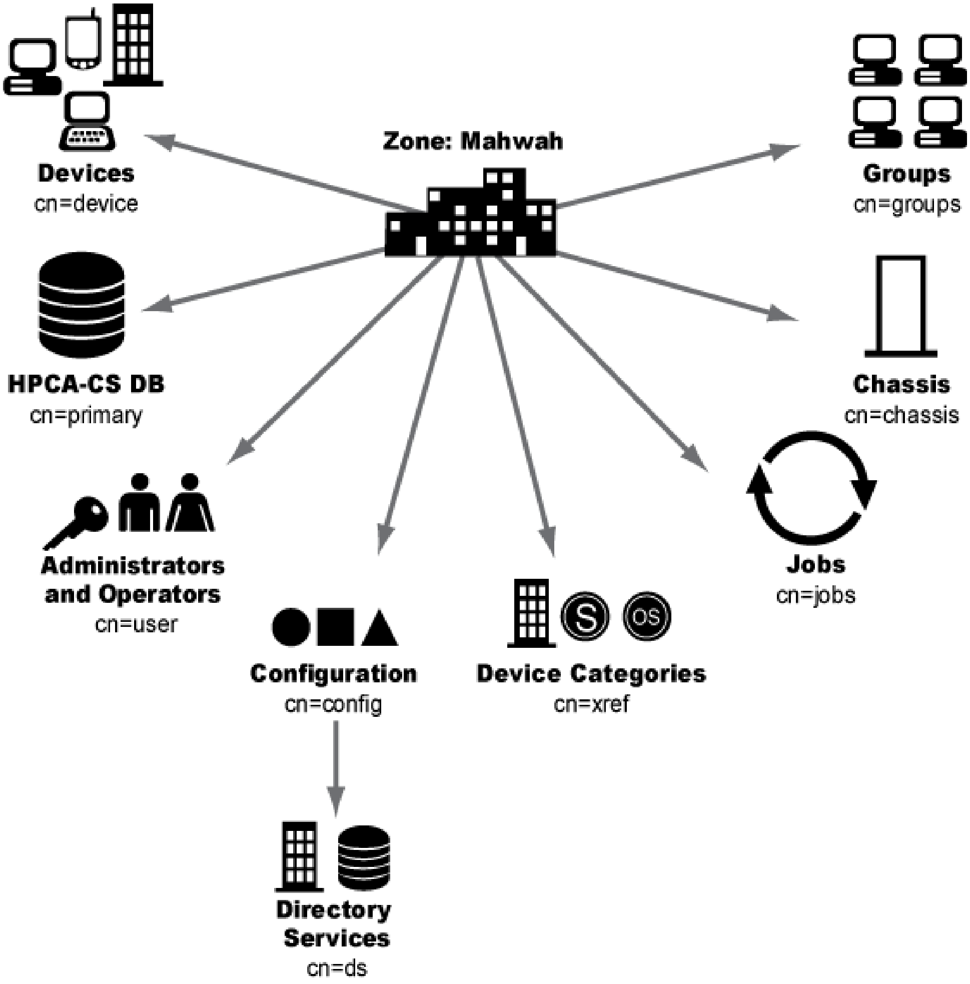
A zone is created whenever the Portal is installed, and all objects in the zone include the high-level qualifier of the zone name. The first installed zone is called the master zone and others are called subordinate zones. The properties for the zone object, itself, include the URL information needed to access the zone.

The Zone Directory Structure

Every Portal zone has the same directory structure and same-named containers at the highest levels.

The next figure illustrates the zone directory structure and containers. See About the Zone Containers on page 36 for a description of each container and how they are used.

Figure 1 Portal directory of a zone

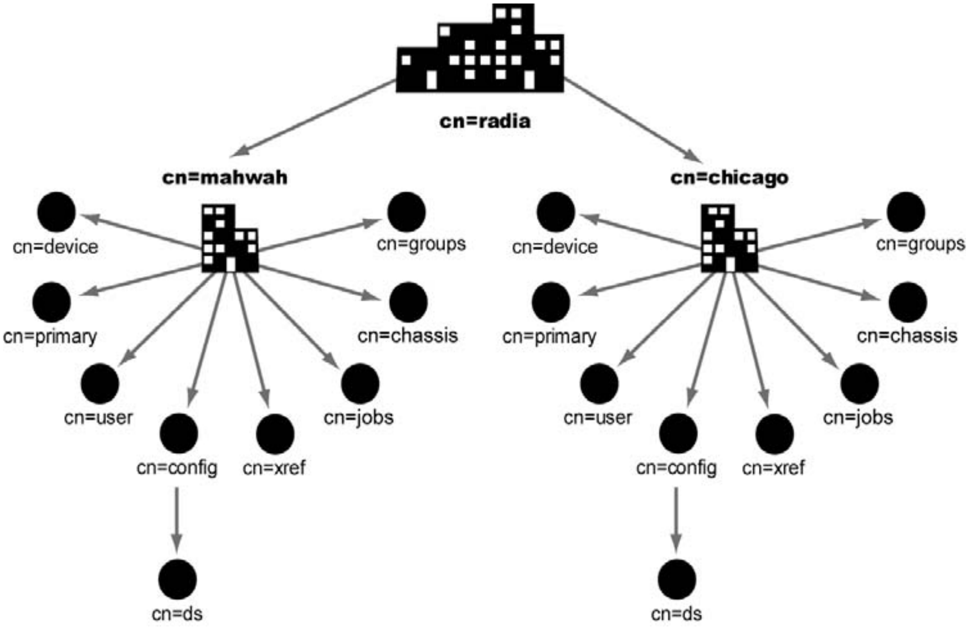


About Object Names in a Zone

The Portal, itself, is a directory service containing objects of various object classes. Each object is assigned a common name (cn=*name*). The common name given to an object must be unique among all objects in that class. For example, all zone names in your enterprise must be unique. Within a given zone, all common names of objects of the same class must be unique. The common names of the zone containers are pre-assigned and the same across all zones in your enterprise.

Each entry within a zone may be identified by its location. For example, the location of the **Devices** container entry in the figure above is `cn=device,cn=Mahwah` and the location of the PRIMARY File on the Configuration Server is `cn=Primary,cn=Mahwah`.

Figure 2 Multiple zones of the Portal



This naming convention serves to ensure that distinct names exist among devices and other objects across all zones in your enterprise. For example, in the figure above, the location of the devices container in the Mahwah zone is: `cn=device,cn=Mahwah,cn=radia` and the location of the devices container in the Chicago zone is `cn=device,cn=Chicago,cn=radia`.

The common name for any object displays in a small pop-up window as you hover your mouse pointer over the object's icon or label in the Portal.

The directory structure and naming context permit name distinction among all objects in all zones in your enterprise. This allows the HPCA administrators to schedule operations across devices in the entire enterprise from a single, central site.

Terminology

The following terms are used frequently throughout this guide. You should become familiar with them before using this guide. Also see the glossary at the end of this guide.

directory service

A directory service in this guide refers to any of the directory service types that can be accessed from the Portal. These include any Lightweight Directory Access Protocol (LDAP) directory and the Configuration Server Database.

An Enterprise Manager or HPCA Core console user can connect to the LDAP Directory Services for which they are configured (given proper authority). These configurations are stored in the directory services container of the Portal OpenLDAP directory.

blade enclosure

A physical container for a set of blades servers. It consists of a backplane that routes power and communication signals and additional hardware for cabling and thermal issues. It also hosts the CPU or server power supplies. See rack and server blade.

managed device

A computer or other hardware device in your network, such as a PDA or printer, that has been added to a Portal zone device container.

mount point

The location in a directory structure to which a connection is made. The mount point becomes the root node of the mounted directory, and thus you can only navigate to nodes at or below the mount point.

master zone

The initial Portal zone installed at an enterprise. Prior to 7.50, additional Portals were installed as subordinate zones to the Portal master zone, also called the master portal.

rack

A set of components cabled together to communicate between themselves. A rack is a container for an enclosure. See enclosure.

server blade

A single circuit board, containing microprocessors, memory, and network connections that is usually intended for a single, dedicated application (such as serving web pages) and that can be easily inserted into a space-saving rack or rack-mountable enclosure with many similar servers. Server blades are more cost-efficient, smaller and consume less power than traditional box-based servers. See enclosure and rack.

subordinate zone

Prior to 7.50, secondary Portal zones installed at an enterprise, usually from the initial Portal master zone. All zones across your enterprise must have unique names to allow for unique distinguished names for all objects across all zones in your enterprise.

zone

A zone is a logical set of devices, infrastructure, and software that is represented and managed in directory services and administered by the Portal.

A zone is created whenever the Portal is installed, and all objects in the zone include the high-level qualifier of the zone name. The first installed zone is called the master zone. If additional zones exist, they are called subordinate zones. The properties of the zone object specify the URL needed to access that zone.

zone access points container

The zones access points container defines all Portal zones in your enterprise. Go to the zone access points container to open another zone's Portal, as well as schedule zone operations on devices that exist in any zone in your enterprise.

Summary

- The Portal is an engine, a set of Web-services, and host to the OpenLDAP Zone directory for managed devices. The Portal components are required to support all HPCA Client Automation envrionments.
- The Portal consists of the Portal Run-time, the Portal Zone Directory, and the Portal Agent embedded in the HPCA Agents. The set of container objects in a zone directory are loaded at startup.
- A zone is a logical set of devices, infrastructure, and software that is represented and managed in directory services. Each zone directory contains the same set of containers.
- Multiple zones allow for management of unlimited numbers of devices at different device locations. Zone names must be unique. Object names in the same class must be unique in a zone.

2 Installing the Portal

At the end of this chapter, you will:

- Be able to install the Portal.
- Be able to stop or start the Portal Service.
- Be able to use the HPCA Consoles to access the Portal Zone.

Preparing for Installation

If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started and Concepts Guide* as the installation in that guide overrides the information in this guide.

1 Before you install the Portal, locate your HP license file.

  If you need assistance, contact HP Technical Support.

2 A complete Portal installation requires access to these folders of the HP Client Automation media:

  — **Infrastructure** media folder (In earlier releases, this was used to install additional Portal Zones or Proxy Servers from the Portal; not currently applicable.)

  — **Agents** media folder (required to install Client Automation agents from any HPCA Console)

3 Review the Release Notes delivered with the Client Automation product for the latest information.

Installing the Portal

Use the Portal to view and manage your existing Windows infrastructure, add new Client Automation infrastructure products and applications, as well as perform service and policy administration on your Configuration Server DB, using Active Directory, if needed.

This release supports environments with multiple Portal sites using the new zone architecture and features. Each Portal site being managed from the master portal site needs to have version 5.00 installed.

Prerequisites

The Portal has been optimized to work with the REXX method ZTASKEND and the Messaging Server.

HP recommends using the Portal with the latest ZTASKEND and the latest Messaging Server to improve the information process flow between the Configuration Server and the Portal.

- Using the latest version of ZTASKEND that is available with the latest Configuration Server enhances Portal performance.
- The minimum ZTASKEND required is Version 1.8. This is installed with the Configuration Server 4.5.4 SP3.

For details on migrating your Configuration Server, refer to the PDF located in the following folder on the Client Automation media: `Configuration Server\management_infrastructure\configuration_server\migrate_db`.

For details on installing the Messaging Server, refer to the *HP Client Automation Messaging Server Installation and Configuration Guide (Messaging Server Guide)*. For details on upgrading to the latest version of the Messaging Server, refer to the latest Migration Guide for that product.

System Requirements

- **Server**
  - Windows Servers* with the appropriate Service Packs as listed in the Infrastructure Platform Support Table in the accompanying *HPCA 7.50 Release Notes*.
  - Installation of the Portal requires administrator authority.
- **Web Client**
  - Any platform that supports a web browser
  - Microsoft Internet Explorer 4.0 or higher or Netscape 4.0 or higher *with cookies enabled*
  - Security for a Microsoft Internet Explorer browser must be set no higher than **medium**

Platform Support

For the latest information about the platforms that are supported in this release, see the accompanying *HPCA 7.50 Release Notes*.

Directory Size of a Single Zone

The **Portal Directory** includes all configuration and entitlement information for the Portal as well as devices, groups, managed infrastructure, job status, network and mounted services information.

For performance reasons, HP recommends limiting the number of devices managed by a single zone to the following:

- Recommended maximum: 50,000 devices

Multiple Portal zones can be installed to meet the needs of enterprises of any size.

Installation Procedures

You will not be permitted to install this version of the Portal to the same directory as an existing, pre-Version 5.00 Portal. It must be installed to a different directory.

For more information, refer to the Portal Migration Guide, located in the `\extended_infrastructure\management_portal\migrate` folder on the Client Automation media.

Use the following procedure to install a Portal zone in your enterprise.

Default Installation Path, Ports, and Service Name

The Portal no longer installs into a shared path, port or service of an Integration Server. The Portal installation defaults for v 5.x are summarized below:

- The default Portal install location is:

  `C:\Program Files\Hewlett-Packard\CM\ManagementPortal`

- Default Ports include:
  - Portal: **`3471`**
  - Listening Port for OpenLDAP: **`3474`**

  Earlier releases supported a Listening Port for OpenLDAP Backup: **`3475.`** The Portal Backup feature is not supported in this release and Enable Portal Backup should remain disabled. For alternative backup methods, see Managing the Portal Zone Directory on page 65.

- The Portal Service name is **`httpd-managementportal`**.
- The display service name is: **`HPCA Portal.`**

To install the Portal

Stop the service for the Integration Server (httpd) if it is installed and running on the machine on which you are installing the Portal.

1 From the `\Infrastructure` directory on the Client Automation Enterprise media, go to the folder for `\extended_infrastructure\management _portal\win32` and double-click **setup.exe**.

The Welcome window for the Portal setup program opens.

2 Click **Next**.

The End-User License Agreement window opens. You must accept the terms before you can install the Portal.

3 Click **Accept** to agree to the terms of the software license.

The Portal Location window opens.

4 Use this window to select the folder where you want to install the Portal.

> HP recommends accepting the new default path of:
> `C:\Program Files\Hewlett-Packard\CM \ManagementPortal`
> The Portal no longer installs into a shared Integration Server path, service, and port.

5 Click **Next** to accept the default installation folder specified in the window, or click **Browse** to navigate to and select a different folder, and then click **Next**.

The License File window opens.

6 Click **Browse** to navigate to the location of your license file. If necessary, the installation will rename the license file to `license.nvd`. Then, it will copy the license file into the Portal `\modules` directory.

The Enable Network Discovery window opens.

7 Click **Yes** to enable Network Discovery (*recommended*). This option enables the Portal to automatically discover all devices in your Windows environment that you can manage.

or

Click **No** to disable Network Discovery. This option is best used if you are testing the Portal and want to prevent the automatic discovery of all machines in your environment from occurring.

8 Click **Next**.

The Network Discovery Interval window opens.

9 In the Discovery Interval text box, type how often (in hours) you want the network discovery job to run. Valid entries are 1 to 24. The default is 24 hours.

To modify this Network Discovery Interval after installation, edit the NETSCAN_POLL parameter of the configuration file. For details, see Configuring Network Discovery on page 45.

10 Click **Next**.

The Discovery Start Delay window opens.

11 In the Discovery Start Delay text box, type how long you want to wait (in minutes) after the Portal starts before starting the network discovery. The delay applies each time the Portal is started. Valid entries are 0 to 1440 miniutes (or 24 hours). By default, Network Discovery starts 15 minutes after you start the Portal.

To modify the Discovery Start Delay after installation, use the NETSCAN_START_DELAY parameter in the configuration file. For details, see Configuring Network Discovery on page 45.

12 Click **Next**.

The first zone information window opens.

13 In the Portal Zone Name text box, type a zone name to represent this instance of the Portal. Each instance of the Portal in your enterprise must have a unique zone name.

Enter a name up to 64 characters long. Use only letters (a-z and A-Z), numbers (0-9) and the space character. Do not use special characters, such as an underscores, commas, or periods.

Typically, the initial zone name identifies the entire infrastructure being managed, such as ACMECorp. Later installations of subordinate zones are named for the division or location of infrastructure being managed under that zone, such as NorthAmerica or Chicago.

See What is a Zone? on page 17 for more information about Zones.

14 Click **Next**.

The second Zone information window opens.

15 In the Portal Zone Friendly Name text box, optionally type a friendly name for this Portal Zone. If omitted, the friendly name defaults to the zone name.

The friendly name is the display name for the zone object in the Portal user interface.

16 Click **Next**.

The Secure Listening Port window opens.

In the Secure Listening Port for Portal text box:

— Leave the default value of -1 to run the Portal on an unsecured port (the default is 3471).

— To specify an SSL-secured listening port for the Portal, enter the secured port number here.

Following installation, refer to the *HP Client Automation SSL Implementation Guide* for complete information on how to configure the Portal for secured communications.

17 Click **Next**.

In the Listening Port for OpenLDAP text box, select a port for the Portal Zone to communicate with its OpenLDAP Database. The default port is 3474.

18 Click **Next**.

The Enable Backup feature is disabled in this release. Just click Next when prompted for a Listening Port for OpenLDAP Backup.

In the Listening Port for OpenLDAP Backup text box, it is no longer necessary to select a port for the Portal Zone to communicate with a Backup OpenLDAP Database. The default port is 3475, but the feature is disabled in this release..

19 Click **Next**.

The Enable Backup window opens.

20 Leave the Enable Backup Directory task set to **No**.

The Backup Directory feature is not available in this release. Customers should refer to Admin Guide available from the *http://www.openldap.org* website for backup and restore procedures for the OpenLDAP directory.

21 Click Next.

A summary window of the installation information opens.

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

A message box prompts you to copy the modules used to perform remote installations of the infrastructure components.

> For 7.50, you can skip the installation of the Remotely Installable Components. The Infrastructure media is not required for Version 7.50 features.

23 Optionally, click **Yes.**

The Remotely Installable Components Location window opens.

If necessary, click **Browse** to navigate to the location of the **Infrastructure** folder on the Client Automation media.

24 Click **Next**. The modules are copied to the Portal `\media` directory.

A message box prompts you to copy the agent modules to be used for remote installations.

25 Click **Yes**.

The Remotely Installable Client Components Location window opens.

If necessary, navigate to the **\Agents** directory.

26 Click **Browse** to navigate to the location of the **\Agents** directory, which contains the media for all agents.

27 Click **Next**.

The HPCA Agent modules are copied to the Portal's `\media` directory.

28 Click **Finish** when the installation is complete.

Completing the installation automatically starts the HPCA Portal service and OpenLDAP directory service hosting the Zone for your managed devices.

> See Starting and Stopping the Portal on page 31 and Accessing the Portal Zone from the HPCA Consoles on page 32 for information on performing these tasks manually.

29 Continue with the installation of the HPCA Enterprise Manager. Refer to the *HPCA Enterprise Manager User Guide*.

Specifying the IP Address for a Remote Portal

➤ When running the Configuration Server with the Messaging Server, it is no longer necessary to specify the IP address and port for the Portal in the MGR_RMP section of the `edmprof` file.

Posting Agent Objects to the Portal Directory

All agent objects collected by the Configuration Server are routed to external servers and databases by the Messaging Server. When a Messaging Server is installed it may be configured to post objects to a Portal zone or discard them.

For details on how to configure the Messaging Server to post agent objects to a Portal Zone, refer to the *Messaging Server Guide*.

➤ Notifying agents using Wake-On-Lan (WOL) does not require you to route agent objects to the Portal. The embedded Portal Agent collects the MAC address and subnet information needed for WOL directly from any device which has a Client Automation agent installed.

To verify that the Messaging Server is posting objects to the specified Portal Zone, you can either monitor the posts to the Messaging Server through its `core.dda.log`, or use the HPCA Enterprise Manager or Core console to check the Device Categories container for Managed Services in the Zone (since each agent's device will show the services that you deployed to it under the Managed Services container).

Starting and Stopping the Portal

To start the Portal

1. Access Windows Services if it is necessary to start the Portal.
2. From Windows Services, right-click **HPCA Portal** and select **Start**.

To stop the Portal

1. Access Windows Services to stop the Portal.
2. Right-click **HPCA Portal** and select **Stop**.

Accessing the Portal Zone from the HPCA Consoles

If your environment uses Core and Satellite servers, use the information in the *Core and Satellite Servers Getting Started and Concepts Guide* to access the Portal.

To access the Portal Zone from the HPCA Enterprise Manager:

1. Open your web browser.

   See the Web-Client topic of System Requirements on page 25 to review the Web browser requirements for the Portal.

2. In the Address bar, type the following:

   `http://<`*`IP Address or host name`***`>:3471`**

   — *`IP Address`* is the IP address of the computer where the Portal zone directory is installed.

   — *`Host name`* is the host name of the computer where the Portal zone directory is installed.

3. Press **Enter**.

   The welcome page for the Portal prompts you to login.

Summary

- Install an initial Portal, giving it a zone name. This installation becomes your enterprise's Master Zone.
- To install additional Portal zones, use the Install Subordinate Portal task in the Operations task group. This task installs subordinate zones remotely. All zones in your enterprise must be unique.
- Run **Update Subordinate Portal** to update subordinate zones in your enterprise with a new build, such as a Portal Service Pack.
- Optionally, the Messaging Server can be configured to route agent-objects from the Configuration Server to the Portal.

3 Using the Portal

At the end of this chapter, you will:

- Be familiar with the zone containers that exist at the highest level of the directory.
- Know how to navigate to any location in the Portal Zone.
- Know how to navigate to locations that have been configured for access from the Portal, including networks, the Configuration Server Database and an Active Directory or other LDAP directory in your enterprise.

Portal OpenLDAP Directory and Zone Objects

Once you are familiar with the Portal user interface, you need to understand how to access the key areas of the infrastructure that you want to manage. However, first you must be familiar with the objects represented in a Portal Directory and zone in the Portal.

A tree view is used to organize these objects. The tree consists of the following icons, which represent the Zone Directory objects.

- **Zone**
  The Zone Directory contains all devices, infrastructure, and software that is managed and administered by the Portal at this location. Other Portal Zones are accessed from the connections available from the Zone Access Points container.

- **Active Directory**
  An external Active Directory configured for access by a Portal administrator appears at the directory level in the workspace.

- **PRIMARY File**
  The PRIMARY File is in the Configuration Server Database on a Configuration Server, whose common name has been assigned cn=primary.

- **Containers**
  A **container** is a grouping of objects used to select a particular object

type, or to limit the scope of influence that an administrator can have over the entire infrastructure. The containers at the highest level of a Portal Zone are discussed in About the Zone Containers on page 36. All zones include the same containers and container names. The procedures throughout the guide identify which containers to start from when performing any task.

- **Computer, Servers and Devices**
  A **server** is a physical device that is running a piece of the infrastructure (service) that you want to manage via the Portal. A server must be addressable by an IP address. An example of a server would be a Windows 2003 server that is running a Configuration Server.

  A computer is a physical device that exists in your infrastructure. If you want it managed by this Portal Zone, you must specify Manage Computer to add it to the Zone, Devices container.

  A device is a physical device that exists in the Devices container of the Zone, and is being managed from this zone. Devices also have memberships in groups in the Groups container and the Device Categories container.

- **Network**
  A network, such as Microsoft Windows Network, represents an external network directory that has been discovered by the Portal. Objects in a network can be selected for management by this Portal Zone.

- **Directory Service**
  External Services are defined to the Portal Zone to enable a connection to that service from within the Portal. An Active Directory, the Configuration Server DB on the Configuration Server, and other LDAP directories can be configured for access from the Directory Service container.

- **Services**
  A service is an application running on a server such as a Configuration Server or Proxy Server.

About the Zone Containers

This topic defines the Portal zone containers that are directly beneath the zone node. Containers designated as self-managed are directory areas where no administrative operations are performed.

The containers and objects allow Portal administrators to perform these tasks:

  - Perform operations against groups that are automatically created and managed by the Portal (based on known hardware, software, and managed service information for the devices)
  - Establish multiple zones in an enterprise, with the ability to access remote zones and perform operations against remote zone device groups.
  - Access the Configuration Server and administer services and policy at the instance-level. Apply policy using an LDAP directory, such as Active Directory.
  - Connect to and browse entries in an external LDAP directory, such as Active Directory.
  - Connect to and browse your existing network directories.
  - Perform modeling and policy-based management of server blade devices in a zone using the knowledge of their blade enclosures, racks, and enclosure configurations.

- **Administrators and Operators Container (cn=USER)**
  The Administrators and Operators Container is the default, built-in source for authenticating users of the Portal and specifying which tasks they are entitled to perform. There are separate user groups for Operators and Auditors, as well as administrators of the Portal, Accounts, Infrastructure, the Network, Packages, Policy, Services, and the Configuration Server.

- **Chassis Container (cn=chassis)**
  The Chassis container is used to manage and apply policy to the blade servers in a zone using the (physical) enclosures and racks in which they are mounted, as well as their (logical) enclosure configurations. It contains three groups:

  — Blade Enclosure Configurations

  — Blade Enclosures

  — Racks with Enclosures

- **Configuration Container (cn=config)**
  The Configuration container holds the start-up configuration of the Portal zone for both internal and external objects and mount points. All objects

in the previous containers are "mounted" as directories when the zone is started.

Directory objects that are defined and mounted from the Configuration container include:

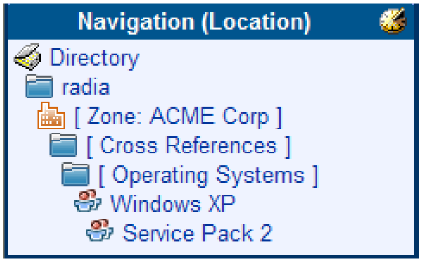
- Configuration Services – Contains an object for the default Configuration Server Database (HPCA-CS Database) and it's Primary file (cn=primary,cn=config) and schema.
- Delegated Administrators – Container for Entitlements.
- Device Discovery Types – Container for objects needed to discover LDAP Devices, NT Domains and HPCA Reporting Servers.
- Directory Services (cn=ds, cn=config) – Container of available directory services. See below for more information.
- Portal Task Groups and Tasks – Container defining the Portal Task Groups and Tasks available from the User Interface.
- Profiles – Container for Client Automation product profiles, such as Agent installation profiles.
- Session -- Containers with user-session objects and history
- Web Services – Container of HTTP Service configurations. These define the URLs invoked by the Portal web services for DSML, media downloads, and processes.

- **Directory Services Container**
  The Directory Services container is one of the Configuration containers. It defines the external directory services and mount points the zone is to connect with automatically at startup, or make available for connection during operation. Use this container to define access to other LDAP directory services in your enterprise, such as Active Directory, as well as access to the PRIMARY File on the Configuration Server Database (CSDB). Additional CSDBs can also be defined for access from this container.
- **Device Categories Container (cn=xref) Self Managed**
  The **Device Categories** container is a self-managed container of automatically-generated device groups. Most groups are created once the Portal Agent is installed on the computers in your Devices container. The Device Categories container creates and maintains the memberships for all devices according to the following classifications, using information passed from the Portal Agent to the Portal for all devices under a zone's management:
  - **Device Architecture**

- **Device Manufacturers** – For example, Hewlett-Packard, Dell, and Gateway device groups.
- **Enclosure Manufacturers** – For example, Hewlett-Packard and IBM are groups listed under the enclosure manufacturers for server blades.
- **Infrastructure Services** – For example, Proxy Server, Portal Agent, and Configuration Server device groups.
- **Load Balancer Types** Category to hold Load Balancer Type objects; for future use.
- **Managed Services** – For example, groups for each service being managed on devices through the CM Application Manager or CM Application Self-service Manager.

  The Managed Services groups are created and maintained using objects collected at the end of a client-connect session with a Configuration Server, and routed from a Messaging Server to the Portal Zone. For more information, see Posting Agent Objects to the Portal Directory on page 31.

- **Operating Systems** – For example, Windows XP. Within a specific operating system group are sub-groups for service pack levels, as shown in the following figure:



- **OS Management** - For example, Invalid OS, No Resolved OS, Pending Hardware Configuration, Pending OS Selection and Un-Managed OS.
- **Subnets** – For example, Subnet 16 groups all devices whose IP addresses are on that subnet.

  Subnet addresses for devices use the format `nnn.nnn.nnn.nnn`.

- **VM Services** – Virtual Management Services; for example, ESX Servers.

- **Devices Container (cn=device) Self Managed**
  The Devices container holds the object properties for all devices being managed by this Portal zone. Entries are automatically created in this container when other operations are performed, such as adding a device to a group in the Groups container or selecting **Manage Computer** from a computer object in your network.

  Devices in this container have **memberships** in other containers. For example, each device must have membership in at least one group in the Group container to facilitate operations. In addition, devices have **automatic membership** in various Device Categories container entries, based on what hardware, software, managed services, and Client Automation infrastructure they contain.

- **Groups Container (cn=group)**
  Most Portal Operations are performed against groups of devices, as opposed to individual devices. The Group container holds the provided All Devices Group, as well as any groups you create. Devices hold memberships in at least one group, but as many as you choose. Operations scheduled against a specified target group will include the members of that group at the time the job runs. Groups can be defined with a hierarchy, such that Group A includes a set of devices as well as all devices that are members of Group A1.

  To schedule jobs against groups in more than one zone, you can establish same-named groups in the Groups container of each zone, and then select the group for the operation.

- **History Container (cn=history)**
  Holds the daily records of completed jobs.

- **Jobs Container (cn=jobs)**
  Holds the objects for jobs and job groups scheduled or recently run by the Portal.

- **Network Container (cn=network)**
  Container used to access the enterprise networks that have been configured as mount points from the Directory Services container, including DNS and Microsoft Windows Network. Networks are often used to access computers that need to be brought under management in the Portal zone.

- **Services Container (cn=service)**
  Holds the Services Catalog of all managed-service instances (ZSERVICE class instances) that are in the CSDB identified to the Portal as Primary. Within the Service catalog are sub-containers for Inventory Management,

OS Management, Security Management to discover vulnerabilities, Patch Management and Sofware Management services.

- **Zone Access Points Container (cn=zone-sap)**
  Holds an entry for the current zone and any remote zones in your enterprise that have been configured for access. From this container, you can use the Operations task to open a subordinate zone's Portal, or schedule zone operations to launch jobs across multiple zones in your enterprise, at once.

Summary

- The Portal Zone is composed of containers. Navigate to the appropriate container and location to perform tasks related to the objects stored in each container.
- The Portal tasks are maintained in task groups that reflect their function. The task groups and tasks available at any time vary based on your assigned role as well as your current navigation location.

4 Administrative Functions

At the end of this chapter, you will:

- Be able to configure the Portal Zone for Network Discovery and Directory Services.
- Be able to connect to and disconnect from a Directory Service or Configuration Server Database, or other object defined in the Directory Services container.
- Be able to manage the Portal Zone Directory using Backup, Restore, Import, and Export tasks.

Configuring a Portal Zone

If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started and Concepts Guide* as the installation, configuration and troubleshooting information in that guide may override the information in this guide.

Following installation, you need to add the following objects to a zone's infrastructure in order to use various new features. Most of these are added by using the HPCA Enterprise Console or HPCA Core Console features.

- **Directory Services**
  Add a Directory Service object for each outside directory to which you want the Portal to be able to connect, such as the PRIMARY File on your Configuration Server or an existing LDAP Directory in your enterprise.
- **Network Discovery and Mount Points**
  The Portal is configured to connect to a set of network directories in your enterprise through mount points. The definitions are also found in the Directory Services container, where the startup can be changed from automatic to manual, if desired.
- **Groups (of Devices)**
  Almost all operations in this release are performed using device groups. The devices that are imported or added to a specific Portal Zone can be further clustered into different groups to expedite common operations.
- **Subordinate Zones**
  From the initial Portal, run the Install Zone task to remotely install subordinate zones in your enterprise, each with a unique name. All zones retain an entry in the Zone Access Points container, which can be used to schedule Zone Operations on devices in all zones in your enterprise.
- **Task Templates**
  Task templates need to be added before scheduling jobs for Zone Operations.
- **Device Categories Container**
  The groups in the Device Categories container are self-managed. They are automatically created after the Portal Agent is installed on devices in the Device container, and dynamically maintained.

Understanding Network Discovery

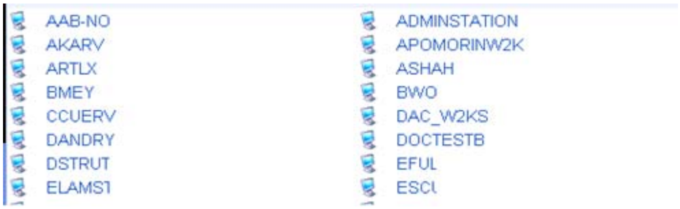
If enabled during the install, the Portal runs the network discovery job upon startup and at regular intervals to automatically discover the resources on your network. The discovered objects are placed in the appropriate network container in the **Zone → Network** location, where they can be selected for management by the Portal Zone.

To view the objects discovered in a specific network, navigate to the **Zone →Network** container and then click the specific network object in the workspace. For example:

- Click **Microsoft Windows Network (cn=lanmanredirector)** to view the Windows devices that you can manage.

Figure 3 below shows the objects discovered in a sample Microsoft Windows Network domain.

Figure 3 Sample Microsoft Windows Network domain devices



AAB-NO
AKARV
ARTLX
BMEY
CCUERV
DANDRY
DSTRUT
ELAMS1
ADMINSTATION
APOMORINW2K
ASHAH
BWO
DAC_W2KS
DOCTESTB
EFUL
ESCL

Configuring Network Discovery

In some environments, you may want to configure your network discovery so that you have more control over network discovery, especially in environments with large networks.

Each time the network discovery job runs, newly discovered objects are added to the Networks container. Additional Network Discovery jobs will only add objects to previously discovered Networks containers, not remove them.

To configure network discovery

1 Stop the HPCA Portal service (httpd-managementportal).

2 Use a text editor to open the Portal configuration file, `rmp.cfg`, located by default in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc`.

3 Look for these lines defining the the initial parameters. Your entries will vary from the code sample below.

```
rmp::init {
    ENABLE_BACKUP           0
    NETSCAN                 Yes
    NETSCAN_POLL            86400
    NETSCAN_START_DELAY     900
    URL                     /
    ZONE                    "cn=myzone, cn=radia"
    ZONE_PORT               3474
}
#
# END OF CONFIG
#
```

4 You can insert any of the parameters in Table 2 below into this file before the finishing curly bracket (}) as shown in the code sample above.

5 Use a space to separate the parameter and its value.

Table 2 Parameters to Configure Network Discovery

Parameters	Explanation
NETSCAN	Enables or disables network discovery. Default is disabled. During the install the user can set this value to enabled or disabled. • Type **NETSCAN 0** to disable network discovery. • Type **NETSCAN 1** to enable network discovery.

Parameters	**Explanation**

NETSCAN_START_DELAY	The time to wait (in seconds) before starting network discovery when the Portal starts up. Default is 15 minutes (900 seconds).
	You can specify this value as:
	`NETSCAN_START_DELAY 900`
	Another way to specify this value is by using a Tcl expression, which would read as follows:
	`NETSCAN_START_DELAY {15*60}`
	where 15 is the number of minutes. When multiplied by 60 seconds, the value becomes 900 seconds.

NETSCAN_POLL	Network Discovery Interval (in seconds). Default setting is 86400 seconds, or 24 hours. Optionally, specify this value using a Tcl expression in curly brackets. For example: to specify 12 hours, enter: **`NETSCAN_POLL {12*60*60}`** where 12 is the number of hours, multiplied by 60 minutes, multiplied by 60 seconds.
NETSCAN_INCLUDE	For each object class specified, limits network discovery to only those objects named in the include list. Default is to include all discovered objects in all classes within the network. Use the following syntax: `NETSCAN_INCLUDE { object_class {object_list} object_classn {object_list} }` where: *`object_class`* is a class whose discovered objects are to be restricted to the members specified in the following object list. Valid object classes include, but are not limited to: network, tree, domain, computer. Your network may include other classes. Tip: Any object's class is listed when you hover the mouse pointer over its icon. *`object_list`* is a space-separated list of common names within curly brackets. These are the only objects to be included in network discovery for the

Parameters	Explanation
	given object class. Unnamed objects in the specified class are excluded. All names are case-insensitive. Example: The following limits discovery to all objects found in the two listed domains in the Microsoft Windows Network. No other networks will be discovered. `NETSCAN_INCLUDE { network {lanmanredirector} domain {domain1 domain2} }` For additional examples, see Using NETSCAN_INCLUDE to Limit Network Discovery on page 48.

6 Save and close the file.

7 Restart the HPCA Portal service (httpd-managmentportal) and open the Portal.

Using NETSCAN_INCLUDE to Limit Network Discovery

1 The `NETSCAN_INCLUDE { }` parameter allows you to restrict network discovery of the objects and object classes in your network. It is very powerful, and can be extremely restrictive.

2 For general syntax, refer to the NETSCAN_INCLUDE entry in Table 2 on page 46. When using NETSCAN_INCLUDE, be aware of the following implications:

3 Classes are hierarchical, and the include lists are processed for higher-level classes before lower-level classes. For example, the network class include list is processed before the domain include list.

```
network
    domain
        computer
```

4 For a given class, if a class is not named in a NETSCAN_INCLUDE list, all objects are included. (This is subject to limits already processed for a higher-class object, discussed in Step 3 above)

5 Once you limit objects of a given class in a NETSCAN_INCLUDE list, you are also EXCLUDING the unnamed objects of the same class. In

addition, you are also EXCLUDING all lower-class objects contained in the excluded branches.

For example, including a domain list by definition EXCLUDES all domains in the network that are not listed. All computers contained in the excluded domains ARE ALSO EXCLUDED.

Examples:

Use the following examples as reference when coding your own NETSCAN_INCLUDE lists.

- `NETSCAN_INCLUDE {}`
  Discover all objects in the network. This is the default.
- `NETSCAN_INCLUDE { network {lanmanredirector}}`
  Limits discovery to the lanmanredirector network. (Lanmanredirector is the common name for Microsoft Windows Network.) No other network will be discovered. All the objects under lanmanredirector will be discovered.
- `NETSCAN_INCLUDE { computer {gta02 vhr01 kwo04 jra06} }`
  Limits discovery of computer objects to the four computers in the list: gta02, vhr01, kwo04, and jra06. Discovers all network objects that are not computers.
- `NETSCAN_INCLUDE { domain {Novad} computer {gta02 vhr01 kwo04 jra06} }`
  Discovers any of the computers listed *if* they exist in the domain Novad. No other computers will be discovered. Any network objects that are not domains or computers will be discovered.

Setting Additional Configuration Parameters

Separate topics discuss how to modify the `rmp.cfg` file for:

- Network discovery (see page 45)
- LDAP authentication (see page 55)
- Managing Portal Agent Signal Processing (see page 77)
- Customizing Domain Filters for Policy Resolution (see page 59).

Table 3 below, lists the parameters you can add to or modify in the `rmp.cfg` file for options that are not related to any of the topics listed above.

For detailed steps on how to modify parameters in the `rmp.cfg` file, refer to the procedure To configure network discovery on page 45.

Table 3 Additional Portal Configuration Parameters in RMP.CFG

Parameter	Definition
`ENABLE_BACKUP`	The portal directory backup feature is not supported in this release. Leave the default value of 0. To backup and restore the Portal's OpenLDAP directory, see Managing the Portal Zone Directory on page 65. Default and only valid value is 0.
`LINKS`	Specifies the policy configuration links to enable when policy has been applied to the objects in the Chassis container and related Device Categories containers for server blade devices. Refer to Enabling Policy Configurations for Blades, Enclosures and Racks on page 63 for the details on specifying the attributes for this parameter.

Parameter	Definition
LISTENING_ADDRESS	Specifies a valid network address (either an IP address, hostname, or DNS address) that is to be passed to Portal Agents, and then used by them to connect back to the Portal. Use a LISTENING_ADDRESS when the Management Agents are experiencing communication failures with the Portal and are unsuccessful in registering back to the Portal or performing remote tasks on behalf of the Portal. This can occur when the Portal resides on a machine with dual-NIC cards or is using a dynamic IP address. Specify a network address using the format that works best in your environment: LISTENING_ADDRESS *IPaddress* or LISTENING_ADDRESS *hostname* or LISTENING_ADDRESS *DNS* Ensure the network address you enter points to the current Portal Zone. If it does not, results are unpredictable.
RCS_AUTO_CONNECT	When a Primary Configuration Server directory service is defined for the Portal, controls an automatic connection to the Primary Configuration Server whenever the Portal is started and the ds-rcs Startup property is set to Auto or Manual. The RCS_AUTO_CONNECT is not enforced when Startup is set to Disabled. Default value is 1 (enabled). Enter RCS_AUTO_CONNECT 0 to disable the automatic connection to the Primary Configuration Server; and revert to the connections as defined by the Startup property when the Directory Service was configured.

Parameter	**Definition**
REFRESHMSC	When a Primary Configuration Server directory service is defined for the Portal, controls how often the Portal updates its *Managed Services Catalog* with those available in the source Configuration Server database. The Managed Services Catalog serves as the HPCA Definitive Software Library, and is accessible from the Services object (cn=services) located in the root of the Portal directory. Default value is 600 seconds, or 10 minutes. Specify a different interval for the refresh of the Managed Services Catalog in seconds.
USE_FQDNSHOST_NAME	Specifies that Portal should contact remote hosts using either fully qualified domain names or short names (that is, the left-most portion of a fully qualified domain name). Customers whose DNS tables contain imperfect entries may want to switch to the use of short names. Sample operations that involve contacting a remote host include a Notify, a Proxy preload or purge, stopping or starting services via the Portal Agent, and contacting the Portal Agent. • Type **USE_FQDNSHOST_NAME 0** to use short names (that is, the left-most portion of a fully qualified name). Customers whose DNS tables contain imperfect entries may want to switch to the use of short names. • Type **USE_FQDNSHOST_NAME 1** to return to the use of fully qualified domain names (the default).

Parameter	**Definition**
WOL_MCAST_ADDR	Permits Wake-on-LAN (WOL) support in multicast-enabled environments. Default is no support for multicast WOL. • Type **WOL_MCAST_ADDR <*IP_address*>** where the <*IP address*> specifies the multicast address to use to revolve a WOL request. • Type **WOL_MCAST_ADDR 0** to return to standard WOL support (no multicast WOL support). This is the default.
ZONE_PORT_BACKUP	In earlier releases, port used to communicate with a backup (replicated) database. Default port is 3475. Not used when ENABLE_BACKUP is disabled and set to 0.

Configuring Directory Services

The Zone Configuration container includes the Directory Services container. This is where the Directory Service objects configured through the HPCA Core Console or the HPCA Enterprise Manager console are stored.

For more information, refer to the Configuration topics in the appropriate User Guide related to the Console you are using.

Directory Service Connection Status upon Portal Restart

Startup Property Set to Auto or Disabled

Without exception, when a Directory Service's Startup property is set to Automatic, the Directory Service will be reconnected when the Portal is restarted.

Likewise, without exception, when a Directory Service's Startup property is set to Disabled, the Directory Service will not be connected when the Portal is restarted.

Startup Directory Service Property - Set to Manual

When a Directory Service's Startup property is set to Manual, there are several conditions and parameter-based overrides that affect whether or not the Directory Service will be connected after a Portal restart.

1. For an LDAP or LDAPS Directory Service, if the **Use for Policy** property is set to True, it will override a Manual startup setting and the Portal will always reconnect to the Directory Service upon restart.
2. For the Directory Service connecting to the HPCA Configuration Server Database, a Manual setting is overridden by the default **RCS_AUTO_CONNECT** 1 setting in the rmp.cfg file, which means the Portal will always reconnect to the Primary Configuration Server Directory Service upon restart.

   To disable the RCS_AUTO_CONNECT 1 entry, edit the rmp.cfg file and add the configuration parameter: RCS_AUTO_CONNECT 0. Save the rmp.cfg file and restart the HPCA Portal Service.
3. If the above overrides do not apply, the Portal will resume a previous Directory Service connection upon restart, but will not connect to the Directory Service if it was not connected when the Portal shut down.

The following tables summarize the Manual Startup behavior for an LDAP(S) and HPCA-CS Directory Service. If the Directory Service is connected to the Portal, its **Job activity** property indicates **started**.

Table 4 LDAP Directory Service Connection - Startup Property is Manual

Properties upon Portal shut-down		Property upon Restart
Used for Policy?	**Job activity**	**Job activity**
Yes	Does not matter	Started
No	Started	Started
No	Stopped	Stopped

Table 5 Primary CS Directory Service Connection - Startup Property is Manual

Configuration upon Portal shut-down		Property upon Restart
RCS_AUTO_CONNECT	**Job activity**	**Job activity**
1 (default)	Does not matter	Started
0 (set in rmp.cfg)	Started	Started
0 (set in rmp.cfg)	Stopped	Stopped

Table 6 Non-primary CS Directory Service Connection - Startup is Manual

Property upon Portal shut-down	Property upon Restart
Job activity	**Job activity**
Started	Started
Stopped	Stopped

Configuring for External LDAP Authentication

Use the procedures and the `rmp.cfg` configuration parameters listed in this topic to implement external LDAP authentication for users of the Portal. The LDAP_AUTH parameters specify:

- the default external authentication setting for all users of the Portal (on or off)
- the domain a user will bind to
- the hostname and port of the LDAP server

➤ By default, the Admin userID only binds to the local Portal directory.

If you set the default external authentication mode to on, you will also need to specify the external user ID and passwords for each user on the Person properties page.

If you set the default external authentication mode to off, use the Add Person or Modify Person pages to turn on External authentication as well as specify an External User ID and external password for anyone to be externally authenticated.

To configure external LDAP authentication for the Portal

1 Stop the HPCA Portal service (httpd-managementportal).

2 Use a text editor to open the Portal configuration file, `rmp.cfg`, located by default in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc`.

3 Insert the LDAP_AUTH, LDAP_AUTH_DN, and LDAP_AUTH_HOST parameters using uppercase into this file before the finishing curly bracket (}), as shown in the bold face portion of the sample code below.

```
#
rmp::init {
    URL          /

     LDAP_AUTH      1
          LDAP_AUTH_DN    <<user>>@mydomain.com
          LDAP_AUTH_HOST myldaphostname:389


    }
#
# END OF CONFIG
#
```

> The LDAP_AUTH value determines whether all users are enabled or disabled for LDAP authentication, by default.

4 Use one or more spaces to separate the parameter and its value. See Table 7 on page 57 for details.

Table 7 rmp.cfg parameters for external LDAP authentication

Parameter and Value	Definition and Examples

`LDAP_AUTH 1`
or
`LDAP_AUTH 0`
	Sets the default value of external authentication for all users logging onto the Portal. Use the External Authentication? field on the Person properties page to override the default value for any user.
	• Set to **1** to enable external LDAP authentication, by default, for all users.
	• Set to **0** to disable external authentication, by default, for all users.
	• If unspecified, LDAP_AUTH is set to **0**.

`LDAP_AUTH_DN <<`*`user`*`>>@<`*`mydomain`*`.com>`	Defines the domain that a user will bind to. Replace *`mydomain.com`* with the domain that users will bind to. The `<<user>>` portion will be substituted with the value entered on the login page.
	`LDAP_AUTH_DN <<user>>@`*`mydomain.com`*
	`LDAP_AUTH_DN <<user>>@domainA.com`

`LDAP_AUTH_HOST hostname:389`	The hostname and port of the LDAP server. Where "myldaphostname" is the hostname of the LDAP server.

5 Save and close the file.

6 Restart the HPCA Portal service (httpd-managementportal) and open the Portal.

Configuring for a Custom LDAP Policy Extension Prefix

Many Policy Server implementations use the default LDAP Policy Extension prefix of edm—as in edmPolicy. If you have defined an LDAP Directory Service for policy tasks, but it uses a policy extension prefix other than edm, use the following procedure to define its LDAP Policy Extension prefix value to the Portal. This procedure adds a PREFIX parameter to the `rmp.cfg` file where you specify a policy prefix value other than edm.

See the *Policy Server Guide* for more information on configuring the Policy Server and the LDAP Policy Extension.

To configure the Portal for a Custom LDAP Policy Prefix (other than edm)

1 Stop the HPCA Portal service (httpd-managementportal).

2 Use a text editor to open the Portal configuration file, `rmp.cfg`, located by default in `*SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc`.

3 Insert the PREFIX parameter (must be uppercase) into this file before the finishing curly bracket (}) as shown in the code sample here.

```
#
rmp::init {
    URL            /

     PREFIX     rad

    }
#
# END OF CONFIG
#
```

4 Use one or more spaces to separate the PREFIX parameter and its value. Specify the value using the same case as is entered for the LDAP Policy Extension prefix defined in the Policy Server.

Table 8 Parameter to Configure a Custom Policy Prefix

Parameter	Explanation
PREFIX	Defines an LDAP Policy Extension prefix other than the default value of edm. Enter one or more spaces to separate the PREFIX parameter and its value. The value must match the LDAP Policy Extension prefix defined in the Policy Server. For example: `PREFIX rad` defines a policy prefix of rad instead of edm.

5 Save and close the file.

6 Restart the lHPCA Portal service (httpd-managementportal) and open the Portal.

Customizing Domain Filters (DNAMEs) for Policy Resolution

If you have modified the domain filter settings defined in your Policy Server `pm.cfg` file, you can port your modified filter settings to the Portal. The modified filter settings will be available from the Dname drop-down list box on the Resolve Policy task page.

Domain filtering is defined in your Policy Server. Any custom filter settings must be properly defined in the Policy Server configuration file, `pm.cfg` using the format:

```
DNAME=<DOMAIN NAME>   { rule }
```

Refer to Appendix C, Domain Filtering in the *Policy Server Guide* for details on domain filtering and syntax.

To port your custom domain filter settings to the Portal Resolve Policy task you must modify the `httpd.rc` file, which is located in the etc directory of where the Portal is installed. Add the following custom code to the end of the `httpd.rc` file using the format:

```
namespace eval policy {

default cfg(DNAME=<DOMAIN NAME>)   { rule }

}
```

where `DNAME=<DOMAIN NAME>` and `{ rule }` correspond to a custom filter setting in your `pm.cfg` file. The code sample below displays the end of the `httpd.rc` file configured for custom policy filters. This example shows a modified definition for the default (*) filter as well as a new AUDIT filter.

```
namespace eval policy {

    default cfg(DNAME=*)          { * !PATCHMGR !OS !AUDIT}

    default cfg(DNAME=PATCH)      { PATCHMGR }

    default cfg(DNAME=OS)         { OS }

    default cfg(DNAME=AUDIT)      { AUDIT }

}
```

Save the changes to the `httpd.rc` file and restart the Portal service. The modified filter settings will be available from the Dname drop-down list on the Resolve Policy task.

Configuring Blades, Enclosures, and Racks

The Chassis container extends the device-based Client Automation infrastructure zone architecture to include the server blades, blade enclosures (both stand-alone and rack-mounted), and racks in a zone. The Chassis container also includes enclosure configurations, whose set of predefined entries can be extended, as necessary, to permit logical groupings of the blade enclosures in any enterprise.

Table 9 below lists the Chassis container contents and Table 10 on page 61 lists the related Device Categories containers for these objects.

Table 9 Chassis Container Objects

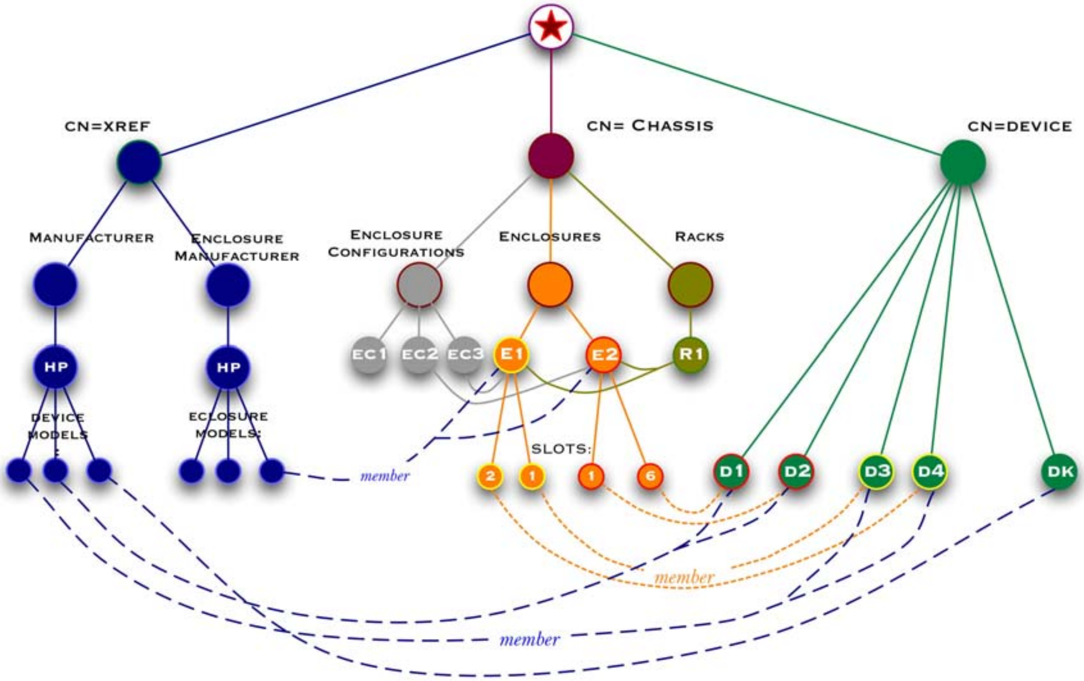
Chassis Container Group	Contents and Notes
Racks Containing Enclosures	Rack instances containing enclosures. • Physical racks IDs must be unique within all racks in a Zone. • Multiple enclosure instances may be linked to a single rack.
Blade Enclosures	Planned or actual enclosure instances. Each instance contains a set of slots. Slots are either *occupied* by a server blade or *empty*. • Enclosure instance names must be unique within a zone. HP recommends using names that are independent of their rack location, to allow for relocation. • Enclosures can be linked to an Enclosure Manufacturer and Model Number (in the Device Categories groups). • Enclosures can be linked to a single enclosure configuration and a single rack instance. • Occupied slots are linked to a managed blade device.
Blade Enclosure Configurations	• Predefined enclosure configurations (an enclosure model number and a predefined set of slots and server blades).

Table 10 Device Categories Groups for Blade Enclosures

Device Categories Group	Group Objects	Description
Enclosure Manufacturer	Manufacturers of blade enclosures, such as HP, IBM	Members include enclosure instances made by that manufacturer.
Enclosure Models	Models of blade enclosures, such as: HP Signal Blade	Members include enclosure instances with that model number.

Figure 4 on page 62 presents an architectural model for the server blade devices, containers, and racks in a zone. Notice the model emphasizes the relationships between these entities, allowing for a variety of policy assignment types. For example, policy assignments can be based on physical groupings (rack policies), logical configurations (policies for pre-defined enclosure configurations), as well as the manufacturers and model numbers of the enclosure instances. The openness of the underlying architecture allows solution architects to assign policies practically anywhere, and enables implementations that fit the particular requirements of any modern enterprise.

Figure 4 Architectural model for server blades, enclosures and racks



1 Server blades in your Zone are devices with membership links to their respective enclosure slots within the **Chassis → Enclosures** container. For example, Device D1 is linked to Slot 6 of the enclosure E2.

2 Server blade devices also hold membership links to the appropriate Manufacturer group in the Device Categories containers. Device D1 is a member of the HP Device Models listed in the **Device Categories → Manufacturers** container.

3 The enclosures defined in the Chassis container can hold memberships in a single enclosure configuration, enclosure model, or rack. For example, enclosure E2 is linked to the configuration EC2, an HP Enclosure Model (within the **Device Categories → Enclosure Manufacturers** container) and rack R1.

About the Predefined Blade Enclosure Configurations

The Blade Enclosure Configurations container includes several predefined configurations for the HP Signal Backplane enclosures described in Table 11 on page 63.

To view these configurations, navigate to the **Zone → Chassis → Blade Enclosure Configurations** location in the Portal.

Table 11 Provided Blade Enclosure Configurations

Displayname	Description
HP Sgnl Backplane/BL20	8 HP/BL20 Blade Slots
HP Sgnl Backplane/BL30	16 HP/BL20 Blade Slots
HP Sgnl Backplane/BL40	2 HP/BL40 Blade Slots

Applying Policy to Blades, Enclosures and Racks

Policy may be applied to many entities related to the blades, enclosures and racks in your zone. There are several approaches that are discussed on the topics that follow.

- Before applying policy, however, you must first add a LINKS entry to the Portal configuration file, `rmp.cfg`, as discussed in Enabling Policy Configurations for Blades, Enclosures and Racks below.
- After you enable the LINKS in the `rmp.cfg` file, use the tasks in the Policy and Advanced Policy tasks groups to assign policy that will apply to the server blade devices in your zone.

Enabling Policy Configurations for Blades, Enclosures and Racks

Resolution of policy applied to the objects related to blades, enclosures and racks in a Zone requires a LINKS entry in the `rmp.cfg` file, as shown below:

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

The specific set of links to include in the LINKS entry will vary for each enterprise, depending on which entities and containers have been used for policy. Table 12 on page 64 describes the policy link that is enabled when the value is added to the LINKS list. For example, if you have not assigned policy to the rack instances in your Zone, `rackdn` may be omitted from the set of LINKS shown above.

Table 12 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.
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).

Assigning Policy Based on Enclosure Model Types

To assign policies based on enclosure manufacturer model types, do the following:

1. Modify the `rmp.cfg` file to include the necessary policy links. See Enabling Policy Configurations for Blades, Enclosures and Racks on page 63.
2. If available, enable the server blade devices in your zone to report the model of the enclosure in which the blade occupies. When this attribute is reported, it is used for cross-referencing of the enclosures in the Enclosure Manufacturer Device Categories container.
3. Optionally, add slots to the models in the Enclosure Manufacturer containers. This allows you to define policy for some or all slots for a given Enclosure Manufacturer model number.
4. Establish a set of enclosure configurations for your zone.

Assigning Policy Based on Enclosure Configurations

To assign policies based on predefined enclosure configurations, do the following:

1. Modify the `rmp.cfg` file to include the necessary policy links. See Enabling Policy Configurations for Blades, Enclosures and Racks on page 63.

2 Establish a set of enclosure configurations that reflect the various configurations of server-blades in the enclosures in your enterprise. Use the predefined configurations or add your own.

3 For each enclosure instance in your enterprise, define it as member of an enclosure configuration.

> Once an enclosure is defined as a member of the enclosure configuration instance, all the slots of the enclosures have member of/member connections to the corresponding slots of the respective configuration.

4 Apply policy to the Enclosure Configuration itself, or to a Slot of the Configuration.

The enclosure instances and slot instances will inherit the policies of the enclosure configuration to which it is linked. A server that occupies a slot number in the enclosure will also inherit policy that is applied to the same-numbered slot in the enclosure configuration.

Managing the Portal Zone Directory

The Portal Zone Directory is an OpenLDAP directory.

- To backup and restore this directory, refer to the Admin Guide available from **http://www.openldap.org/**.
- For information on Portal Directory Troubleshooting and logging the Slapd service, refer to page 75 of the Troubleshooting chapter.

Terms for Database Recovery

slapd - The stand-alone LDAP daemon. A master slapd is an LDAP directory server for the Portal database; a slave slapd is an LDAP directory server for a replicated Portal database.

slurpd – The stand-alone LDAP update replication daemon. Responsible for all activities related to distributing changes made to the master Portal database out to the various Portal database replicas.

For more information on the use of these services with an OpenLDAP directory, refer to **http://www.openldap.org/**. Slapd and slurp are discussed on this page: **http://www.openldap.org/doc/admin23/intro.html**.

Restore Procedures

To restore the master database from a Portal Backup slave database:

1. Stop the HPCA Portal service, `httpd-managementportal`.
2. Copy the slave slapd's database(s) from the `\openldap\Database\rmp-backup` location of the Portal to the master database location at `\openldap\Database\rmp`.

   You should paste all files in the slave database location to the master database location.
3. Restart the Portal service.

To manually restore the database from an external backup directory

1. Stop the HPCA Portal service, `httpd-managementportal`.
2. Stop the Master Slapd.
3. Stop Slurpd.
4. Stop the Slave Slapd.
5. Copy the backup database from the desired << backup_directory>> to both `\Database\rmp` and `\Database\rmp-backup`.
6. Restart all services.

Summary

- Network Discovery can be configured using parameters that are set in the Portal configuration file: `rmp.cfg`.
- Use the standard tools available from *http://www.openldap.org* to backup and restore the Portal Zone OpenLDAP Directory.

5 Troubleshooting

At the end of this chapter, you will:

- Be familiar with the Portal log files.
- Be familiar with the common message types.
- Be familiar with the information that you need to collect for HP Technical Support.
- Be familiar with the Portal Zone Directory backup utilities.
- Be familiar with the options available for troubleshooting and logging the Portal Directory services (slapd, slurpd).
- Be familiar with Portal Agent signal processing parameters that can be tuned to enhance performance.

About the Log Files

⚠ If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started and Concepts Guide* as the configuration, installation and troubleshooting information in that guide may override the information in this guide.

The Portal writes several logs, which can be used to track progress and diagnose problems. The log files are stored by default in *SystemDrive*`:\Program Files\Hewlett-Packard\CM\Management Portal\logs` for the Portal for Windows.

The log files are:

- `httpd-managementportal-`*port*`.log`
  This is the main log for the Portal. It contains information about the actions that you perform in the Portal, operational statistics, as well as the version and build number of the Portal.

  Replace *port* with your port number, for example, `httpd-managementportal-3471.log`.

  Each time you start the web server a new log is written. The old log is saved as `httpd-managementportal-`*port*`.`*nn*`.log`.

- `httpd-port.YY.MM.DD.log`
  This log 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 contains messages written to any logs that contain the prefix ERRor. This allows you to view all errors in a single location.

Setting Trace Levels

By default the trace level is set to 3, which is the informational tracing level. This displays INFO, WARNING, and ERRor messages. See Common Message Types on page 72 for more information.

To change the trace level for the logs

1 Open the file *SystemDrive*`:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc\httpd-managementportal.rc` for Windows, which is located on the computer that is running the Portal. The following is an excerpt from this file.

```
# Config Array
# Element Default
# ======= =======
# HOST           [info hostname]
# PORT           3471
# HTTPS_HOST     [info hostname]
# HTTPS_PorT     443
# DEBUG          0
# DOCROOT        [file join $home htdocs]
# IPADDR         {}
# HTTPS_IPADDR   {}
# WEBMASTER      support@hp.com
# UID            50
# GID            100
# NAME           $tcl_service
# LOG_LEVEL      3
# LOG_LIMIT      7
#
Overrides Config {
    PORT         3471
    HTTPS_PORT   443
    LOG_LEVEL    4
}
#
# (Re)Initialize Logging
#
Log_Init
```

2 Type **LOG_LEVEL** and the appropriate trace level, space delimited, within the Overrides Config starting and ending brackets { }. Select the appropriate trace level, as follows.

Table 13 Trace Levels

Trace Level	Description
0	No logging.
1	Logs errors only.
2	Logs warnings and errors.
3	Logs informational messages, warnings, and errors. *Recommended trace level setting for customers.*
4	Logs all debug information. *Recommended for experienced customers only.*

Trace Level	Description
5 - 9	Full trace *Not recommended for customer use.*

3 Save the file changes and restart the Portal service.

Common Message Types

Table 14 below contains common message types found in the main Portal log (`httpd-port.log`).

Table 14 Common Message Types

Message Type	Description/Example

Info	Provides general information. For example:
	`20010913 12:37:55 Info: LdifImport/4: BEGIN`
	Indicates that a job to import an LDIF has begun.
	`20010913 12:37:55 Info: RMP: Starting Scheduler...`
	Indicates that the Portal's Scheduler service is started.
	`20010913 12:37:55 Info: RMP: Management Portal ready`
	Indicates that the Portal is up and running.

Audit/success	Indicates a successful change to an object in your Portal directory. For example: `20010913 12:46:43 Audit/success: RMP: (who/admin) add: uid=jbanks, cn=opsys,ou=who` Indicates that a new user was added.

Message Type	Description/Example
Audit/failure	Indicates an unsuccessful change to an object in your Portal directory. For example: `20010913 16:26:31 Audit/failure: RMP: (who/admin) add: uid=Guest, ou=who, object "uid=guest,ou=who" already exists` Indicates that you were not able to add a user with the ID Guest to the organizational unit "who" because it already exists.
Error	Indicates a critical problem.
Warning	Indicates a non-critical problem. `20010913 16:20:42 Warning: to: output to 1 job-create-reply 2 resume: no gate`

Collecting Information for HP Technical Support

If you need to contact HP Technical Support for assistance, be sure to collect the following information:

1 The log directory, stored by default in the following locations:

For Windows, *SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementPortal\logs

2 Version information for nvdkit.exe. See Viewing and Logging Version Information, below.

3 The etc directory files, stored by default in the following location:

```
SystemDrive:\Program Files\Hewlett-Packard\
CM\ManagementPortal\etc
```

Viewing and Logging Version Information

After logging into the Portal, click the Information button ? on the banner area to open the Version Information Window. This window displays the installed Module, Version, and Build levels for the Portal, including component modules NVDKIT.EXE, HTTPD.TKD, NVDCRT.TKD and RMP.TKD. Whenever this window is displayed, the version and build levels for each module are also written to the Portal log (httpd-mangementportal-*port*.log).

Gathering Version Information for RADISH.EXE

Radish.exe runs on the Configuration Server. Its build (version) information can be found using this procedure.

To gather the version information for RADISH.EXE

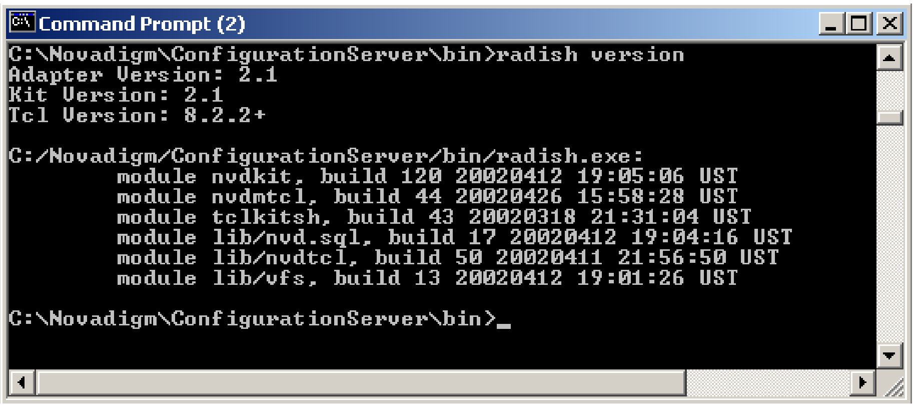
1 Locate the directory of your radish.exe on the machine running the Configuration Server. The default for Windows is:

SystemDrive:\Program Files\Hewlett-Packard\CM\ConfigurationServer\bin

2 Open a command prompt and change to the directory for radish.

3 Type **radish version**, and press **Enter**.

Below is an example of the version information.



```
C:\Novadigm\ConfigurationServer\bin>radish version
Adapter Version: 2.1
Kit Version: 2.1
Tcl Version: 8.2.2+

C:/Novadigm/ConfigurationServer/bin/radish.exe:
        module nvdkit, build 120 20020412 19:05:06 UST
        module nvdmtcl, build 44 20020426 15:58:28 UST
        module tclkitsh, build 43 20020318 21:31:04 UST
        module lib/nvd.sql, build 17 20020412 19:04:16 UST
        module lib/nvdtcl, build 50 20020411 21:56:50 UST
        module lib/vfs, build 13 20020412 19:01:26 UST

C:\Novadigm\ConfigurationServer\bin>_
```

4 The build number for radish.exe is actually given in the build number for module nvdmtcl (its predecessor's name) in the line:

```
module nvdmtcl, build xx <date> <time>
```

For example, the figure above illustrates a Configuration Server running Build 44 of radish (which is shown as module nvdmtcl, build 44 in the output).

`Radish.exe` replaced an earlier program named `nvdmtcl`.

Managing the Portal Zone Directory

The Portal Directory loads all configuration and entitlement information for the Portal as well as devices, groups, managed infrastructure, job status, network and mounted services information.

For performance reasons, HP recommends limiting the number of devices managed by a single zone to the following:

- Recommended maximum: 50,000 devices

Portal Directory Troubleshooting

The following two options can be configured if you are having difficulties with the Portal Directory's Slapd service.

To adjust the OVCMLDAP Heartbeat Detection Interval

By default, the "heartbeat" of the Master Slapd service for the Portal Directory is checked every 20 seconds. If the service is stopped, it is automatically restarted at this point to ensure continued support. You can change this heartbeat detection interval, if desired, by adding the following line to the `rmp.cfg` file:

```
OVCMLDAP_HEARTBEAT_INTERVAL    xx
```

Where: *xx* represents the interval value in seconds. For example, to set a heartbeat detection interval of 10 seconds, enter:

```
OVCMLDAP_HEARTBEAT_INTERVAL    10
```

Restart the Portal service to activate the new heartbeat interval.

To enable logging of the Slapd, Backupslapd, and Slurpd Services

If the Portal Directory's Slapd service requires troubleshooting, HP Software customer support may ask you to turn on logging for the slapd, backup slapd, and slurpd services.

To create a `slapd.log`, `backupslapd.log`, and `slurpd.log` in the Portal `\openldap` directory, add these parameters to `rmp.cfg`:

```
SLAPD_DEBUG_LEVEL         256
BACKUP_SLAPD_DEBUG_LEVEL  256
SLURPD_DEBUG_LEVEL        256
```

Where: *256* represents a sample debug level. Replace 256 with the desired debug level from Table 15, below. If no value is entered, the default is 0, which turns logging off.

Table 15 Debug levels for slapd, backupslapd, and slurpd logs

Debug level	Description
-1	Enable all debugging **Warning:** Logs ferocious amounts of data. Not recommended.
0 (default)	Turn off logging
1	Trace function calls
2	Debug packet handling
4	Heavy trace debugging
8	Connection management
16	Print out packets sent and received
32	Search filter processing
64	Configuration file processing
128	Access control list processing
256	Stats log connections/operations/results
512	Stats log entries sent
1024	Print communication with shell backends
2048	Print entry parsing debugging

Restart the Portal Service to begin logging the slapd, backupslapd, and slurpd services.

To turn off logging for the Slapd, Backupslapd, and Slurpd services

1. Reset the value of all *_DEBUG_VALUE parameters in rmp.cfg to 0, or delete the values.
2. Restart the Portal Service.

Managing Portal Agent Signal Processing

RMA Signal Processing Parameters

The Portal uses three types of dedicated thread pools to handle the incoming requests from Portal Agents (RMAs). You can adjust the number of threads assigned to each pool by adding or updating these parameters in rmp.cfg.

You can also adjust the maximum number of RMA signals the Portal will process at a time.

The parameter changes you make in the rmp.cfg file will take affect when the Portal is restarted.

- The Portal limits the number of RMA signals it will accept for concurrent processing. This is defined in the OPEN_RMA_SIGNAL_SOCKETS_MAX parameter.
- All incoming RMA requests are handled initially by the RMA_SIGNAL_RECEIVER_THREADS pool. These lightweight threads handle only the simplest tasks, such as RMA status checks when the device DN is known.
- RMA requests requiring a database update for a known DN are passed to the RMA_SIGNAL_PROCESSOR_THREADS pool.
- RMA requests requiring any RMA registration look-up or creation work (that is, the device DN is not known) are passed to the RMP_REGISTRATION_THREADS pool. These threads perform the heaviest work.

Table 16 on page 78 summarizes the default and valid values for each parameter related to RMA signal processing.

Table 16 RMA Signal Processing Parameters (rmp.cfg)

Parameter, Default, Valid Values	Definition
`OPEN_RMA_SIGNAL_SOCKETS_MAX` Default: 1024 Valid Values: 256 or greater	Maximum number of RMA signals concurrently being processed by the Portal. After reaching this maximum, the Portal will reject additional incoming signals.
`RMA_SIGNAL_RECEIVER_THREADS` Default: 20 Valid values: positive number	Number of lightweight threads to use to accept incoming RMA requests. These threads handle RMA status checks when the DN is known, or pass requests to appropriate RMA Signal Processor or RMA Registration pool.
`RMA_SIGNAL_PROCESSOR_THREADS` Default: 3 Valid Values: positive number	Number of threads to process database updates when the RMA device DN is known.
`RMP_REGISTRATION_THREADS` Default: 1 Valid Values: positive number	Number of threads to process RMA registration look-up or creation work when the DN is not known. If these threads have no work, they will automatically assist with any RMA signal processor work.

Signal Processing Logs

All messages related to RMA signal processing will be handled by a separate thread and written to a separate log file, `RMP-Signals.log`, located in the `\logs` folder. Older logs are renamed `RMP-Signals.log.1.log`, for example, just like the Portal logs.

Managing the Portal Web Services Token

The Portal Web Services (WS) require a valid token holding user credentials in order to perform HP Client Automation activities.

The `WS_TOKEN_TTL` parameter in the `rmp.cfg` determines how long, in seconds, a given Portal Web Services (WS) user credential token is valid before it expires. During normal usage of the Enterprise Manager Console or

Core Console the token is routinely refreshed. If no user activity is detected within the `WS_TOKEN_TTL` period, the user's session will expire and they will be asked to log in again.

The default `WS_TOKEN_TTL` period is 1200 seconds (20 minutes).

Valid Values: positive number

Default: 1200 seconds

Summary

- The `httpd-managementportal-`*`port`*`.log` is the main log for the Portal.
- The default trace level is set to 3, which tracks informational messages, warnings, and errors.
- Collect your logs and version information if requesting support from HP Technical Support.
- Version and build information can be found by clicking ? on the Portal banner area after logging on. Alternatively, from a command prompt you can run "nvdkit version" on the agent side, and "radish version" on the Configuration Server side.
- Adjust the values for the RMA thread pool parameters to meet the needs of your current Portal requirements.

Index