HP Client Automation Enterprise

Policy Server

for the HP-UX, Solaris and Windows® operating systems

Software Version: 7.80

Installation and Configuration Guide

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER
Copyright © 1996-1999 Intel Corporation.

TFTP SERVER
Copyright © 1983, 1993
The Regents of the University of California.

OpenLDAP
Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.
Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License
Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License
Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

DHTML Calendar
Copyright Mihai Bazon, 2002, 2003

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 indicates changes made to this document.

Table 1   Document Changes

Chapter	Version	Changes
All	7.20	Most HP Configuration Manager products have been rebranded to HP Client Automation.
1	7.50	Page 16, IP Networking Support, new topic.
2, 3	7.20 Aug 2008 July 2009	Installation and Configuring Policy chapters, made general editorial improvements. Added cross-references back to the *Core and Satellite Servers Getting User Guide* topics regarding the Generate LDIF feature and Implementing an External Policy Store.
2	5.10	Page 24, Verify Installation, revised procedures. After installation, click **Config** and then **Reconnect** to verify you can successfully reconnect to the sample database.
2	5.00	Page 24, Verify Installation, revised procedures.

Chapter	Version	Changes
3	5.10 7.50	Page 27, Configuring Policy, chapter title and contents revised to remove topics related to 'Administering Policy'. Policy Administration tasks are now performed from the Enterprise Manager. Deleted topics include: • Distributed Administration • Configuring the Service Drop Down • Adding and Removing Policy • Setting Policy Defaults and Overrides • Controlling Policy Scope Locally
3	7.20	Page 28, Adding Client Automation Policy Attributes, minor correction to the object ID values for the optional attributes; edmPolicyDefault is 1.3.6.1.4.1.2133.2.1.**4**, and edmPolicyOverride is 1.3.6.1.4.1.2133.2.1.**5**. Note: Previous documentation switched these object ID values. However, there is no need to change any existing values because they have no affect on Policy Server performance.
3	All Apr 2008	Page 32, Table 3, Retry definition updated to include: "This is also the number of attempts to reconnect to the directory if the ping detects the directory to be offline."
3	All Nov 2008	Page 35, Configuring the LDAP Method, modified steps 8 though 11 to show the method name of **RADISH** entered in uppercase, which is required for Configuration Servers running UNIX.
3	5.00	Page 39, Connecting to the LDAP Method, modified Step 4 to indicate the _ALWAYS_ Utility Method requires a value of **SYSTEM.ZMETHOD.LDAP_RESOLVE**.
A	5.00	Page 49, Substitution, earlier references to these minimum inbound object attributes were deleted: • in.os is not available by default • in.uid is now in.smsystemuuid • in.host is now in.hostname

Chapter	Version	Changes
		Table 5 on page 50 lists the minimum inbound attributes that are available when using the Policy Server with LDAP.
A	5.xx Jan 2008	Page 53, Table 8, LDAP Extension URL Namespace, updated the pre-requisite and syntax information for `/admin/ldap/flush?dn=<dn>` and `/admin/ldap/reset`.
C	7.50	Page 57, Domain Filtering, Modified content to show the latest default domain name filtering in the HPCA product.
	7.20 Aug 2008	Previous Appendix for Name Changes was removed; it is no longer needed due to HP support self-solve search capabilities.

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:

- Know the benefits of the HP Client Automation Policy Server (Policy Server).
- Understand Policy Server processing.

About HPCA Policy Server

The HP Client Automation (HPCA) Policy Server is a web server used for administration purposes such as mapping services to users in the directory tree. It is one of the management extensions in the HPCA infrastructure providing integration and extended enterprise functionality with your directory services. Policy method connections in the HPCA Configuration Server Database (CSDB) are used to determine what services should be distributed and managed for the user that is currently logged on by querying the Policy Server.

The HPCA Integration Server service, installed with the Policy Server, is a run-time technology that integrates HPCA infrastructure services. The Policy Server leverages your investment in directory services while using HPCA for software management. This greatly reduces the total cost of ownership of your environment. In other words, directory services handle policy management and HPCA manages services. This saves you time because you do not have to define or maintain lists of users in the HPCA Configuration Server Database.

> The Policy Server was formerly known as the Policy Manager. As of this printing, the name still remains Policy Manager in some of the configuration windows.

The Policy Server integrates with existing Lightweight Directory Access Protocol (LDAP) directory servers and SQL databases in a customer's enterprise to enable single source points of control for user authentication, access policies, and subscriber entitlement. These LDAP directory servers include Microsoft Active Directory, Novell NDS, and other vendor's LDAP servers, as well as Microsoft NT Domain Manager, Computer Associates ACF2 and Top Secret, and Oracle, Sybase and Microsoft SQL-based databases.

Benefits

Our goal is to provide the best policy-based management based upon the latest technologies. The HP vision of the Policy Server can be summarized in the following points:

*   **Simplicity**
    The model should be no more complex than your policies.

- **Sophistication**
  The model should be capable of expressing even the most subtle or complex policies you need.

- **Clarity**
  Each organizational policy should exist only once in the model, and be associated directly with the logical object that is the subject of that policy.

- **Investment Protection**
  The model should build upon your existing Directory Services infrastructure.

- **Openness**
  The model should be flexible.

Policy Server Processing

The Policy Server acts as a bridge between the Configuration Server and a directory server. It is a separate component from the Configuration Server. Therefore, when a customer has multiple Configuration Servers, he may have a single Policy Server co-located with his directory server. Figure 1 on page 14 provides an overview of Policy Server Processing.

Figure 1   Policy Server processing
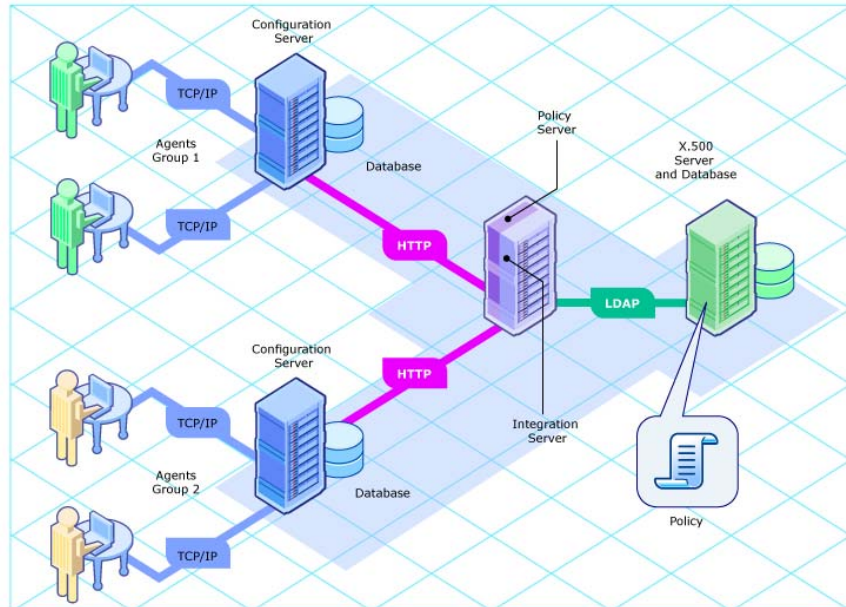
In Figure 1 the following things occur:

1   The HPCA agent connects to the Configuration Server to resolve its
    desired state. The desired state embodies the content that HPCA
    manages for a device. The desired state for each device is dynamically
    created by the Configuration Server based on information in the
    Configuration Server Database.

2   The Configuration Server contacts the Policy Server to perform policy
    resolution, and builds the agent's desired state using the policy
    information.

3   The policy method, LDAP_RESOLVE, handles the resolution requests,
    converting the requests into HTTP queries to the Policy Server, and
    treats the results as a set of objects and attributes to be incorporated into
    the desired state of the connected agent.

4   The Configuration Server completes resolution of the desired state and
    returns the information to the HPCA agent.

The Policy Server maintains a persistent connection to an LDAP directory server and responds to policy requests by performing a policy resolution against the policy database and returns the set of objects resolved as the result set of the HTTP query.

As of Policy Manager Version 5.10, the interface for administering policy information has moved from the Policy Server to the Enterprise Manager. Refer to the *HPCA Enterprise Manager User Guide* or online help for more information. For advanced policy administration tasks, also refer to the *HPCA Portal Installation and Configuration Guide*.

The Policy Server can also take input via HTTP POST from multiple Configuration Servers. The Policy Server can reformat data and insert or update associated database tables. It is also possible to provide HTML-based interfaces for generating operational reports on the current or historical activity of the system.

About the HPCA Integration Server

The HPCA Integration Server (Integration Server) integrates independent modules, such as the Policy Server and Proxy Server, giving them access to all the functions and resources under the control of the Integration Server. The Integration Server is *not* a separately installed product. Each module resides in a common Integration Server's modules directory. These HPCA components use the same Integration Server files, and run under the same process.

Benefits of the Integration Server are:

- All the products using a common HPCA Integration Server for Windows are loaded from a single service called "HPCA Integration Server".

- When the HPCA Integration Server starts, it will scan its configuration file and try to load all the products marked as loadable.

- Each product is separately licensed.

- The Integration Server provides web services that are shared by all loaded modules, resulting in a single entry point for all HTTP (web-based) requests. This integration provides performance, efficiency, and ease of maintenance in an adaptable and cohesive (server) framework.

Using this Guide with Core and Satellite Servers

If your environment uses Core and Satellite servers, the Policy Server is installed as part of those servers, and its configuration is performed from their online Consoles. First refer to the *HPCA Enterprise Core and Satellite Servers Enterprise, Standard or Starter User Guide* for Policy Server installation and basic configuration information.

Continue to refer to this guide for additional details on the Policy Server's setup and functioning with the HPCA environment.

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. This includes support for connecting to an external Policy store in an IPv6-enabled environment. IPv6. For details, refer to the appendix, *IPv6 Networking Support*, in the *HPCA Enterprise Core and Satellite Server User Guide*.

HPCA agent communications, however, are currently limited to IPv4. For details, refer to the appendix, *IPv6 Networking Support*, in the *HPCA Enterprise User Guide*.

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

About this Guide

In addition to this chapter, this book contains the following information.

- **Installation**

  This chapter describes how to install the Policy Server.

- **Configuring LDAP Policy**

This chapter describes how to configure your HPCA environment with LDAP services.

Summary

- The Policy Server integrates with Lightweight Directory Access Protocol (LDAP) directory servers and SQL databases to enable single source points of control for user authentication, access policies, and subscriber entitlement.

- The Policy Server acts as a bridge between the Configuration Server and a customer-provided directory server.

- The Policy Server is a module of the HPCA Integration Server service.

2 Installation

At the end of this chapter, you will:

- Know how to install the HP Client Automation (HPCA) Policy Server.
- Be able to verify installation of the Policy Server.

> ⚠️ If your environment uses Core and Satellite servers, first read the HPCA Core and Satellite Servers User Guide as the installation, configuration, and troubleshooting information in that guide overrides the information in this guide.

> ➤ This document covers installation information for Windows servers only. Full product documentation is available on the HP Technical Support web site.

Policy Server Installation

Before you install the HPCA Policy Server (Policy Server), identify the server where the Policy Server will reside. Administrators usually choose the same physical server that is running the Directory Services or the Configuration Server. Review the reference documentation on the HP Technical Support Web site to help you determine which machine is best suited in your environment for running the Policy Server. Install the Policy Server from the HPCA installation media.

License File and Support

Before starting the installation, download your license file from the HP ftp site. This license file must be accessible to install the products that your enterprise purchased.

If you need assistance, contact HP Technical Support.

Tips

- Have the license file easily accessible for your installation.

- Click **Cancel** in any of the windows to exit the installation. If you click **Cancel** accidentally, prompts enable you to return to the installation program.

- Click **Back** at any time to return to previous windows. All the information that you entered thus far will remain unchanged.

- Most windows have associated error messages. If your specifications are invalid, an error message will appear. Click **OK** and enter the correct information.

- This installation program will display default values. We strongly recommend accepting all defaults; however, they can be overridden by specifying the parameters necessary to suit your environment.

Platform Coverage

For information about the platforms that are supported in this release, see the accompanying release notes.

Installation Steps

1 From the HPCA installation media, navigate to the `\Infrastructure\management_extensions\policy_server` directory. Open the folder for your operating system.

2 Double-click **setup**. The HPCA Policy Server Install window opens.

3 Click **Next**. The License Agreement window opens.

4 Read the license agreement and click **Accept**. The Select the installation folder window opens.

5 Use this window to select the folder where you want to install the Policy Server.

— Click **Next** to accept the default installation folder.

or

— Click **Browse** to select a different folder.

6 Click **Next**. The Select License File window opens.

7 Click **Browse** to navigate to the location of your `license.nvd` file, and click **Open**. You will return to the License Information window, and the complete path to your license file will be displayed.

8 Click **Next**. A summary of the installation information opens.

9 Click **Install** to begin the installation. The installation progress window opens.

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

Verify Installation

Confirm that the Policy Server is running by performing the following verifications. You can directly access the Policy Server by following the procedure To access the Policy Server below.

To access the Policy Server

1 Open your Web browser.

2 In the Address bar, type **http://IP_Address:3466**. This will be referred to as the Policy Server page.

The *IP_Address* is the IP address of the computer where the Policy Server is installed.

The **HP Client Automation Integration Server** web page for the Policy Server opens.

3 Click **Directory Services** on the command bar.

The Policy Manager for LDAP page opens.

> The [Browse] and [Query] tabs are no longer used to perform Policy Administration tasks. After configuring your Policy Manager for LDAP, refer to the *HPCA Enterprise Manager User Guide* for policy administration tasks.

Policy> LDAP> [Browse] | [Config] | [Query] | [Refresh] | [Status] | [Setup] | [Test]   ◄ ▲ ⊕ ⊙ more information

Policy Manager for LDAP

The Policy Manager supports the ability to resolve policy via an LDAP connection to a X.500-style Directory of your choice. [See Documentation]

- Browser - provides both the means to browse your directory and also serves as a simple interface for administering directory-based policies (*subject to the privileges of the account used to connect to the directory*).
- Configuration - provides summary information on the current LDAP configuration, and also allows controlled flushing of the cache.
- Query Tool - provides the means to generate interactive querys and provides a fine degree of control on the behaviour of the LDAP policy engine to aid in understanding and diagnostics. *Human-readable* equivalent of **/policy/ldap** - which is the *Machine-readable* URL used by the Policy Method.
- Status - current operational status information.
- Test Tool - a simple form to test that your LDAP parameters are correct

4 Click **Config** to go to the current configuration page. This page points to the sample database by default.

5   Click **Reconnect** to verify that you can successfully reconnect to the sample database.

Policy> LDAP> [Browse] | [Config] | [Query] | [Refresh] | [Status] | [Setup] | [Test]   more information

Admin:

(i) The cache has been flushed and the connection to the directory server sucessfully re-established

Reconnect

Summary

- Have the appropriate files ready before installing the Policy Server.
- Back up your Configuration Server Database before installing the Policy Server.
- Verify installation using an Internet browser.

3 Configuring Policy

At the end of this chapter, you will:

- Know what attributes to add to your directory service for use with HP Client Automation (HPCA) Policy Server.

- Understand how to configure the method for resolving LDAP policies in the HPCA Configuration Server Database.

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

You must complete the following steps to connect your directory services, the Policy Server, and the Configuration Server.

1 Add the required attributes for Policy Server to your directory service.

2 Configure the Policy Server to connect to your directory server.

3 If your Configuration Server and Policy Server are on two separate computers, you will need to configure them to communicate.

4 Configure the LDAP resolve method on your Configuration Server to use your directory server.

5 Connect the LDAP resolve method to a policy instance in your Configuration Server Database.

After completing these steps, you can begin to administer policy using the HPCA Enterprise Manager (Enterprise Manager).

Adding Client Automation Policy Attributes

⚠ If your environment uses Core and Satellite servers, the Generate LDIF feature eliminates the need to manually add the LDAP policy attributes as discussed below. For more information, refer to the *Core and Satellite Servers User Guide* topics on Policy configuration, the Generate LDIF feature, and Implementing an External Policy Store.

The Policy Server requires that the LDAP schema of an existing directory implementation be modified before it can be used to manage policy. These attributes are used to manage policy scope, relationships, and assignments. Consult your directory service documentation and your enterprise's directory service administrator to make these changes. Be sure to back up your directory schema before any modifications.

▶ Changes to the LDAP schema can be risky because modifications to many directory services are not reversible. Be sure you type correctly. Check and double check the values you are entering before saving the changes to each value entered into the directory schema. Consult your directory services administrator and documentation.

Add the following required attributes:

- Add edmFlags as a single-valued, integer attribute with an object ID of 1.3.6.1.4.1.2133.2.1.1. It controls the scope of your policy. This is added as an optional attribute of the nvdObject class.

- Add edmLink as a multi-valued, case-sensitive string with an object ID of 1.3.6.1.4.1.2133.2.1.2. This attribute allows you to create a connection to a group that is not part of the user's LDAP group membership. This is added as an optional attribute of the nvdObject class.

- Add edmPolicy as a multi-valued, case-sensitive string with an object ID of 1.3.6.1.4.1.2133.2.1.3. Use edmPolicy to assign services to users and groups. This is added as an optional attribute of the nvdObject class.

The following attributes are not mandatory, but you may want to add them.

- Add edmPolicyDefault as a multi-valued, case-exact string with an object ID of 1.3.6.1.4.1.2133.2.1.4. Use edmPolicyDefault to assign policy defaults. This is added as an optional attribute of the nvdObject class.

- Add edmPolicyOverride as a multi-valued, case-exact string with an object ID of 1.3.6.1.4.1.2133.2.1.5. Use edmPolicyOverride to define policy overrides. This is added as an optional attribute of the nvdObject class.

> Previous versions of this documentation incorrectly switched the object ID values for edmPolicyDefault and edmPolicyOverride. However, there is no need to correct existing values because the object IDs have no affect on Policy Server performance.

Adding the nvdObject Class

Some directory services, such as Microsoft Active Directory, do not allow adding of attributes to the *top* class. This is the highest level in the schema. If you cannot add attributes to the top class, create a class that will hold the required edmLink, edmFlags, and edmPolicy attributes, and inherit the values included in the *top* class. EdmPolicyOverride and EdmPolicyDefault are not required, but may be added for additional functionality. By creating this class, including its inherited values, we can modify the areas needed to apply HPCA policies to specific areas of the directory tree. If you can add the attributes to the *top* class, policies can be placed anywhere in the tree.

If you need to create a class, name the class nvdObject. Create it as an auxiliary class with top as its parent class. Set the object ID to 1.3.6.1.4.1.2133.2.1. After creating the nvdObject class, you must add the edmFlags, edmLink, and edmPolicy. To proceed, you must reload your directory schema. Consult your directory service's documentation for instructions on how to do this.

Modifying classes with nvdObject

Once the schema has been re-loaded, the values entered above will show up as a selection, and you can add the nvdObject class to areas of your directory affected by the Policy Server.

To complete the modification for Microsoft Active Directory, nvdObject must be added as an Auxiliary class on the **Relationships** tab to all of the Active Directory classes listed below.

- Person

- Container

- DomainDNS

- Organizational Unit

- Group

You have now completed the necessary modifications to your directory schema. See To configure the Policy Server for LDAP on page 31 for instructions on how to connect the Policy Server to your directory services.

> If you are not able to change the schema, you can use an attribute that already exists in the directory schema.
>
> This feature should only be used when it is *not* possible to make the necessary changes to the schema. See Appendix B, Use Existing LDAP Attributes for instructions on how to do this.

Connection to LDAP

The LDAP extension supports a range of options that are stored in the LDAP start up script. This script is located in the Integration Server directory. HP recommends changing the LDAP configuration through the Policy Server's Setup page to perform validation of user input.

> If you make manual changes to pm.cfg, you will need to restart the HPCA Integration Server service that is hosting the Policy Server.

Below is a procedure for setting the LDAP configuration.

> For the ability to bind an Active Directory domain and edit Policy objects, the BIND_DN needs to have read access rights to the entire directory and write access rights to the top of the tree to which it will be editing.

To configure the Policy Server for LDAP

1 From the Policy Server page, click the **Setup** page.

Setup/Configuration

Any changes made here will effect the running service, and also be saved to disk.

Type	⦿ ldap ○ ldif
Ldif	
Host*	10.10.10.12
Port*	389
Version	○ 2 ⦿ 3
Base Dn	dc=asdfoods,dc=com
Bind Dn	cn=Administrator,cn=Users,dc=asdfoods,dc=cor
Bind Pw	********
Prefix*	edm

2 For Type, select the **ldap** option.

3 In the **Base Dn** line, type the base domain. This is the highest level of the directory structure. If you leave it blank, the highest level is assumed.

Table 2   BASE_DN and BIND_DN Examples

Item	Microsoft Active Directory	Novell Directory Services
Base Dn	Specifies the base domain. Example: dc=asdfoods, dc=com.	Specifies the base organization. Example: o=asdfoods

Item	Microsoft Active Directory	Novell Directory Services
Bind Dn	Specifies the fully qualified name of the account that has Active Directory Schema Permissions on the Directory. Example: cn=Administrator , cn=Users, dc=asdfoods, dc=com or administrator@asdfoods.com	Specifies the fully qualified name of the account that has NDS Permissions on the Directory. Example: cn=Admin, ou=Users, o=asdfoods

4 In the **Bind Dn** line, type the fully qualified name of the account that has update authority to the specific OUs and containers to which the edmPolicy attributes will be applied.

5 In the **Bind Pw** line, type in the password of the Account name referred to in the Bind Dn.

6 In the **Host** line, type the hostname or IP address of the Active Directory Server you wish to bind to for resolving policies.

7 Click **Submit** to submit the changes to the HPCA Integration Server service hosting the Policy Server.

Table 3   Configurable Values in the Web Interface

Field	Default	Description
Host	Localhost	Hostname or TCP/IP address of LDAP Server/Gateway.
Port	389	TCP/IP port of LDAP Server/Gateway.
Version	2	LDAP Protocol version to use (2 or 3)
Base Dn		DN of the logical root of the Directory—used to constrain the directory browser. Also used for pinging the directory server periodically to ensure it is up.
Bind Dn		DN of account to use when authenticating (BIND) with directory. If this parameter is not supplied, then an anonymous BIND is performed.
Bind Pw		Password for Bind Dn account. Note: This is stored in plain text in pm.cfg. It is highly recommended that customers secure access to the <root>/etc directory for administrators only.
Cache	1	Enable caching (0 or 1).
Delay	1	The delay in seconds between each retry attempt.

Field	Default	Description
Flush_freq	3600	The delay in seconds between each flush of the cache.
Retry	1	Number of attempts to issue the LDAP request before marking the directory as unavailable. If this occurs, a reconnection attempt will be made when the next ping is performed. This is also the number of attempts to reconnect to the directory if the ping detects the directory to be offline.
Ping_freq	300	The delay between each attempt to search Base Dn (in seconds). This enables the Policy Server to reconnect to a directory server than may have been restarted, and also serves as an active monitor of the availability of the directory.
Timeout	120	Timeout (in seconds) for LDAP request.

Support for Multiple LDAP Connections

The Policy Server supports multiple concurrent LDAP queries. Configure the number of concurrent LDAP queries in the Policy Server's configuration file, `pm.cfg`, The default location of this file is *System Drive*:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc. Use a text editor such as Notepad to edit the file. The table below describes which parameters apply. When you make changes to `pm.cfg`, you will need to restart the HPCA Integration Server service.

Table 4   Configurable Values for Multiple LDAP Queries

Value	Default	Description
N_workers	2	Specifies number of parallel LDAP directory connections to be created.
PolicyUrl	/policy/ldap	Registers the URL of the Policy Server's LDAP. This is required to use the N_WORKERS parameter. The parameter name is case sensitive. If you do not have this line in your `pm.cfg`, then you will need to add it.

Specifying the Configuration Server

If your HPCA Configuration Server is not on the same computer as your Policy Server, you will need to specify the location of the Configuration

Server. To do this, edit the Configuration Server profile file, edmprof.dat, and the Policy Server configuration file, pm.cfg.

To specify the location of the Policy Server on the Configuration Server

1 On the Configuration Server computer, open the Profile Editor. This opens the Configuration Server's profile file, edmprof.dat, in a text editor.

2 Go to the [MGR_POLICY] section as shown below.

```
* Manager Policy Section                                   *
*  HTTP_HOST      = Host name of Policy Server             *
*          Multiple hosts may be specified (space or comma *
*          separated) for fail over                        *
*  HTTP_PORT      = IP Port number of Policy Server        *
*          NO restart required                             *
*----------------------------------------------------------*
[MGR_POLICY]
HTTP_HOST = XXX.XXX.XXX.XXX
HTTP_PORT = 3466
```

3 Type the IP address of the Policy Server as the value for HTTP_HOST.

4 Type the port of the Policy Server as the HTTP_PORT.

5 Save and close the edmprof.dat.

After specifying to the Configuration Server where the Policy Server is located, you need to specify to the Policy Server where the Configuration Server is.

To specify the location of the Configuration Server to the Policy Server

1 Open the Policy Server's configuration file, pm.cfg, using a text editor. This file is located in the HPCA Integration Server's \etc directory.

2 Type the IP address of your Configuration Server as the value for the RCS_CACHE_HOST. If the port is different from the default of RCS_CACHE_PORT, change that value as well.

3 Save and close the modified pm.cfg.

4 Stop and restart the HPCA Integration Server service.

Configuring the LDAP Method

If you are using LDAP, you must create a connection to the LDAP method in the Configuration Server Database, and connect the users to the LDAP method. Perform the following two procedures to prepare your Configuration Server Database to use the Policy Server.
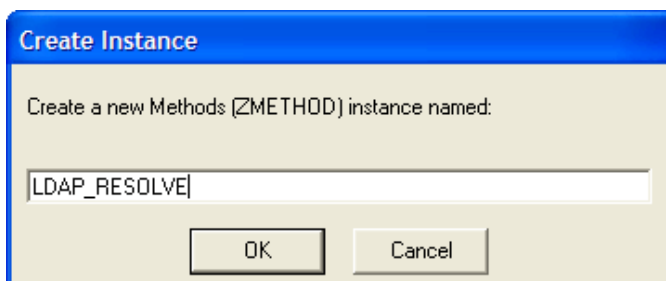
1 Open the HPCA Admin CSDB Editor, and go to PRIMARY.SYSTEM.ZMETHOD.

2 Right-click **Methods (ZMETHOD)**.

   A shortcut menu opens.

3 From the shortcut menu, select **New Instance**.

   The Create Instance dialog box opens.

Create Instance
Create a new Methods (ZMETHOD) instance named:
LDAP_RESOLVE
OK   Cancel

4 Type **LDAP_RESOLVE** in the text box, and click **OK**.
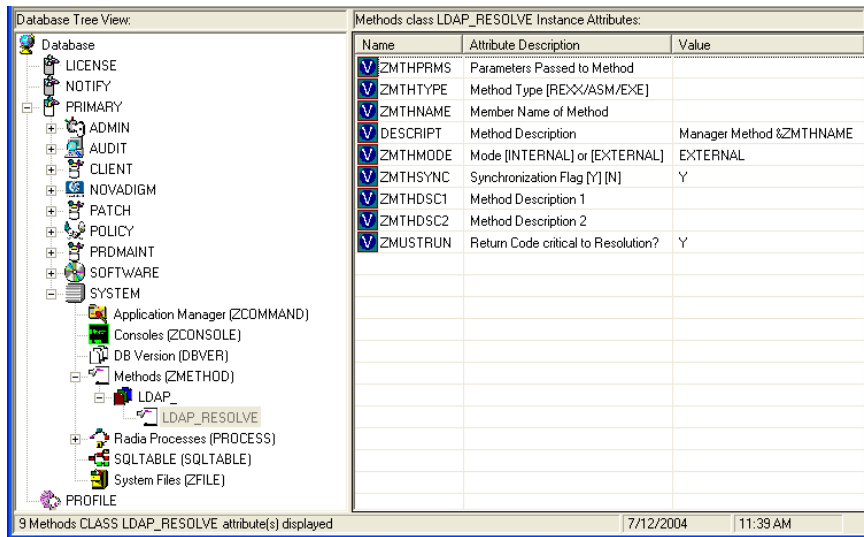
   The HPCA Admin CSDB Editor window opens.

5 Double-click **LDAP_**.

   The tree expands.

6 Double-click **LDAP_RESOLVE** in the tree view.

   The attributes of LDAP_RESOLVE appear in the list view.

Database Tree View:		Methods class LDAP_RESOLVE Instance Attributes:		

Database Tree View:
- Database
  - LICENSE
  - NOTIFY
  - PRIMARY
    - ADMIN
    - AUDIT
    - CLIENT
    - NOVADIGM
    - PATCH
    - POLICY
    - PRDMAINT
    - SOFTWARE
    - SYSTEM
      - Application Manager (ZCOMMAND)
      - Consoles (ZCONSOLE)
      - DB Version (DBVER)
      - Methods (ZMETHOD)
        - LDAP_
          - LDAP_RESOLVE
      - Radia Processes (PROCESS)
      - SQLTABLE (SQLTABLE)
      - System Files (ZFILE)
  - PROFILE

Methods class LDAP_RESOLVE Instance Attributes:

Name	Attribute Description	Value
ZMTHPRMS	Parameters Passed to Method	
ZMTHTYPE	Method Type [REXX/ASM/EXE]	
ZMTHNAME	Member Name of Method	
DESCRIPT	Method Description	Manager Method &ZMTHNAME
ZMTHMODE	Mode [INTERNAL] or [EXTERNAL]	EXTERNAL
ZMTHSYNC	Synchronization Flag [Y] [N]	Y
ZMTHDSC1	Method Description 1	
ZMTHDSC2	Method Description 2	
ZMUSTRUN	Return Code critical to Resolution?	Y

9 Methods CLASS LDAP_RESOLVE attribute(s) displayed   7/12/2004   11:39 AM

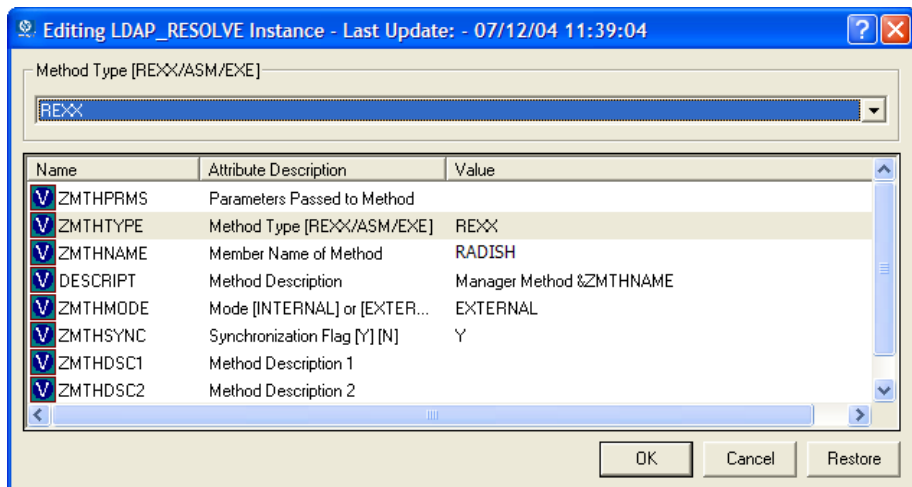7 Double-click the **ZMTHNAME** attribute in the list view.

The Editing Instance dialog box opens.

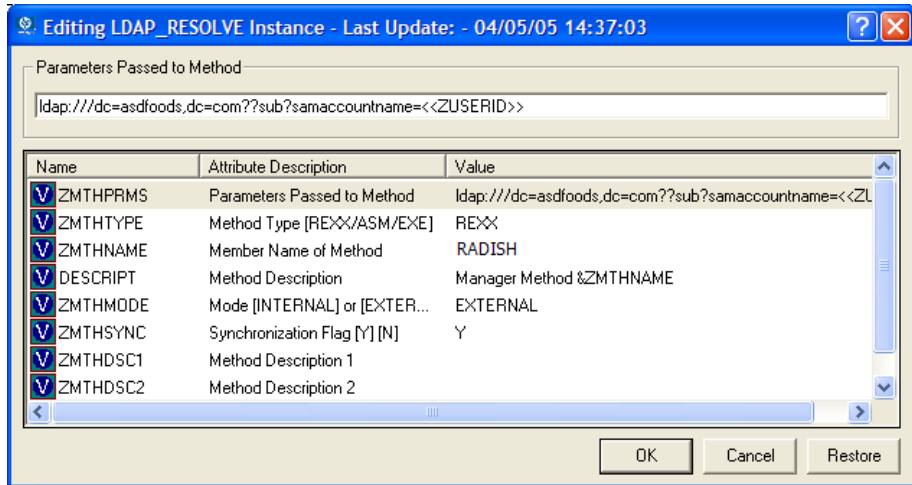8 In the **Member Name of Method** field, type **RADISH**.

> Configuration Servers running on UNIX platforms are case-sensitive and require **RADISH** entered in upper case.

9 Click **ZMTHTYPE**.

Editing LDAP_RESOLVE Instance - Last Update: - 07/12/04 11:39:04

Method Type [REXX/ASM/EXE]

REXX

Name	Attribute Description	Value
ZMTHPRMS	Parameters Passed to Method	
ZMTHTYPE	Method Type [REXX/ASM/EXE]	REXX
ZMTHNAME	Member Name of Method	RADISH
DESCRIPT	Method Description	Manager Method &ZMTHNAME
ZMTHMODE	Mode [INTERNAL] or [EXTER...	EXTERNAL
ZMTHSYNC	Synchronization Flag [Y] [N]	Y
ZMTHDSC1	Method Description 1	
ZMTHDSC2	Method Description 2	

OK   Cancel   Restore

10 In the **Method Type** drop-down list, select **REXX**.

11 Click **ZMTHPRMS**.

Editing LDAP_RESOLVE Instance - Last Update: - 04/05/05 14:37:03

Parameters Passed to Method

ldap:///dc=asdfoods,dc=com??sub?samaccountname=<<ZUSERID>>

Name	Attribute Description	Value
V ZMTHPRMS	Parameters Passed to Method	ldap:///dc=asdfoods,dc=com??sub?samaccountname=<<ZL
V ZMTHTYPE	Method Type [REXX/ASM/EXE]	REXX
V ZMTHNAME	Member Name of Method	RADISH
V DESCRIPT	Method Description	Manager Method &ZMTHNAME
V ZMTHMODE	Mode [INTERNAL] or [EXTER...	EXTERNAL
V ZMTHSYNC	Synchronization Flag [Y] [N]	Y
V ZMTHDSC1	Method Description 1	
V ZMTHDSC2	Method Description 2	

OK   Cancel   Restore

12 In the **Parameters Passed to Method** text box, use the following values.

For HTTP:

http:///policy/ldap?dn=<<ZDN>>&&os=<<ZOS>>

For Microsoft Active Directory:

— To manage policies by machine (preferred method):

ldap:///dc=*domainname*,dc=*forestname*,dc=com??sub?samac countname=<<ZUSERID>>$ (If the client uses $MACHINE as the ZUSERID)

http:///policy/ldap?dn=<<COMPDN>>

For example,

ldap:///dc=asdfoods,dc=com??sub?samaccountname=<<ZUSE RID>>$

— To manage policies by user:

ldap:///dc=*domainname*,dc=*forestname*,dc=com??sub?samac countname=<<LOCALUID>>

For example,

ldap:///dc=asdfoods,dc=com??sub?samaccountname=<<LOCA LUID>>

For Novell Directory Services (NDS):

— To search the entire NDS tree for policy, type:

ldap:///o=organization??sub?cn=<<ZNTUSER>>

For example,

`ldap:///o=cert??sub?cn=<<ZNTUSER>>`

— To search NDS with a specified Distinguished Name, type:

`http:///policy/ldap?dn=<<ZMASTER.DN>>`

For Netscape iPlanet:

— To manage policies by user type:

`ldap:///dc=com??sub?uid=<<ZUSERID>>`

13 Click **OK**.

The Instance Edit Confirmation dialog box opens.

14 Click **Yes** to confirm the changes. The HPCA Admin CSDB Editor window opens.

Now, whenever a managed device connects to the Configuration Server, the null instance calls the policy method, and will point to the appropriate services for that user.

Specifying the Distinguished Name

If there is no way to search the LDAP directory for a unique attribute, such as **samaccountname** in Active Directory, you will need to specify the distinguished name for each subscriber on each client computer (in the ZMASTER object). This must be done because there is no lookup from the HPCA Application Self-service Manager logon screen to the distinguished name in LDAP due to a limitation in LDAP.

To specify the distinguished name (dn)

1 Go to **Start → Programs → HP Client Automation Administrator** and click **Client Automation Admin Agent Explorer**.

2 Go to *SystemDrive*:\Program Files\Hewlett-Packard\CM\Agent\Lib.

3 Double-click **ZMASTER**.

4 From the **Variable** menu, click **Add**.

The Add Variable to Object dialog box opens.
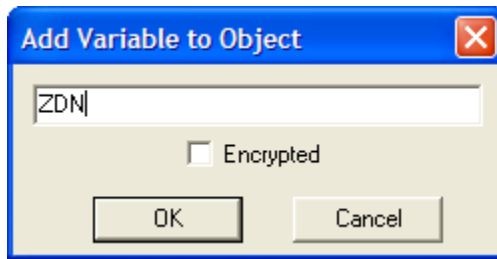
5   In the text box, type a name for the variable, such as **ZDN**.

6   Click **OK**.

The Change Variable dialog box opens.
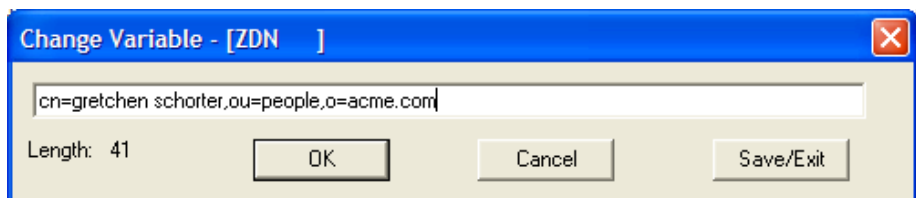
7   Type the distinguished name information, such as **cn=gretchen schorter, ou=people, o=acme.com.**

8   Click **OK**.

9   Click **Save/Exit**.

Connecting to the LDAP Method

You must connect the LDAP method to an instance in the POLICY domain for policy resolution.

To connect the user to the LDAP method

1   Open the HPCA Admin CSDB Editor.

2   Navigate to PRIMARY.POLICY.USER.

3   Double-click the null instance.

> If the null instance is connected to the Default workgroup, change the name of the instance from Default to _NONE_.

4 In the list view, double-click on the **_ALWAYS_ Utility Method** line.

The Editing Instance dialog box opens.
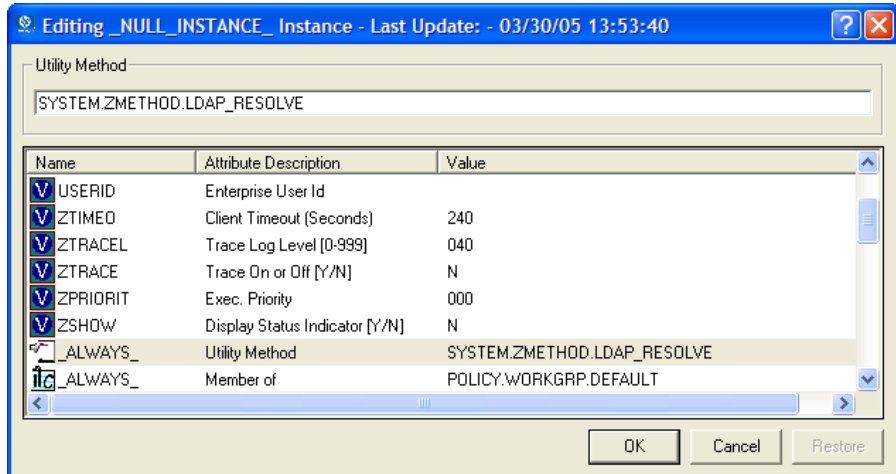
5 In the **Utility Method** text box, type **SYSTEM.ZMETHOD.LDAP_RESOLVE.**

6 Click **OK**.

The Instance Edit Confirmation opens.
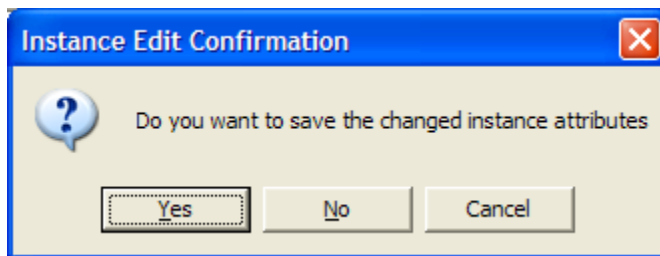
7 Click **Yes**.

The LDAP_RESOLVE method is connected to the Null User instance.

Policy Scope

By default, a subscriber inherits the policy from the parent of any groups it is linked to. This link can be through either the subscriber's directory service membership or through the use of the edmLink attribute. Figure 2 on page 41 shows a part of the Acme organization. It has three organizational units,

Computers, Development, and People. **Computers** holds the Laptop
container. **Development** includes the Product, QA, Research, and Support
organizational units. **People** includes the actual users of the enterprise.

67

Figure 2   Acme organization directory structure
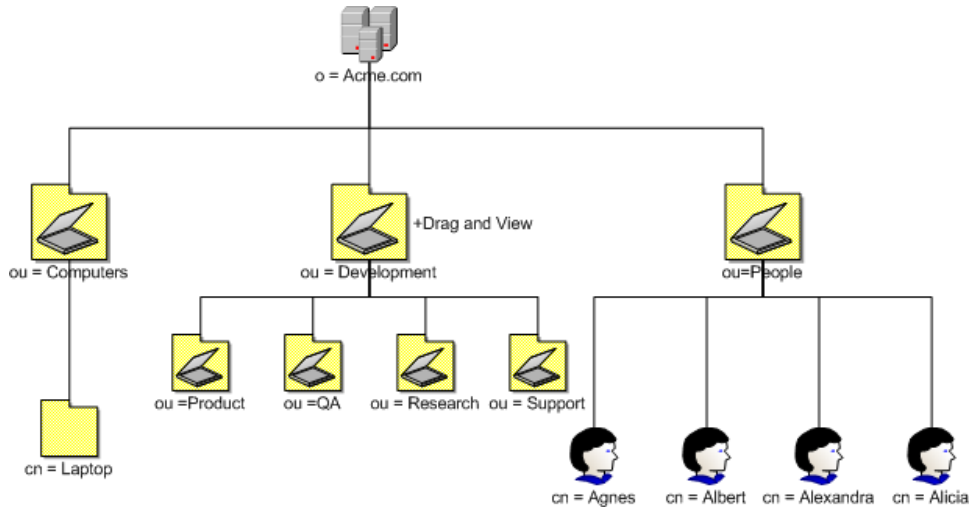
In this figure, Agnes will inherit the policy of the People organizational unit
and the Acme organization.

Figure 3   Agnes is a member of Product organizational unit
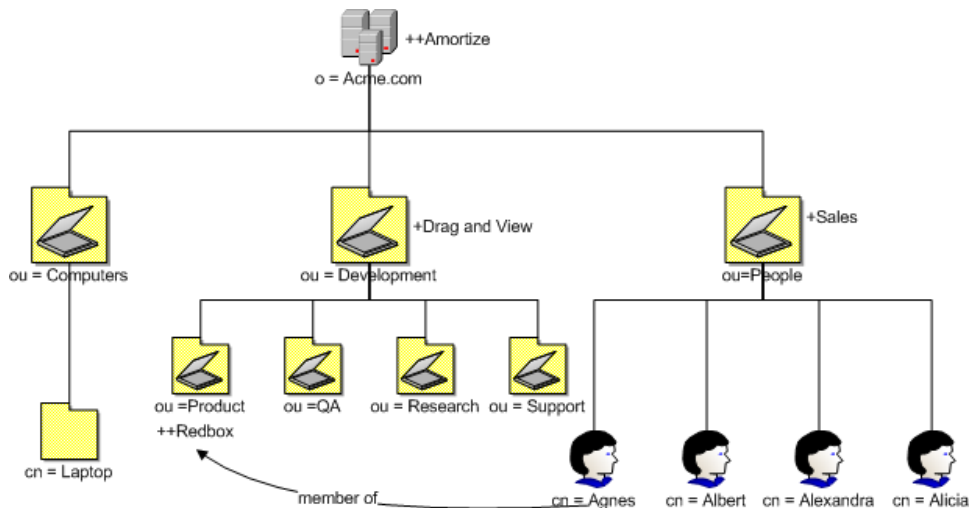
If Agnes is a member of the Product organizational unit, she will also inherit the policy from that unit and the Development organizational unit. In Figure 3 above, Agnes would get Sales and Amortize because she is a part of the People organizational unit. Because Agnes is a member of the Product organizational unit, she would *also* inherit Redbox *and* Drag and View.

Suppose that you need Agnes to receive the services associated with the laptop container, but she is not linked to that container through directory services. Use edmLink to connect her to that container.

Figure 4   Agnes is linked to the laptop container
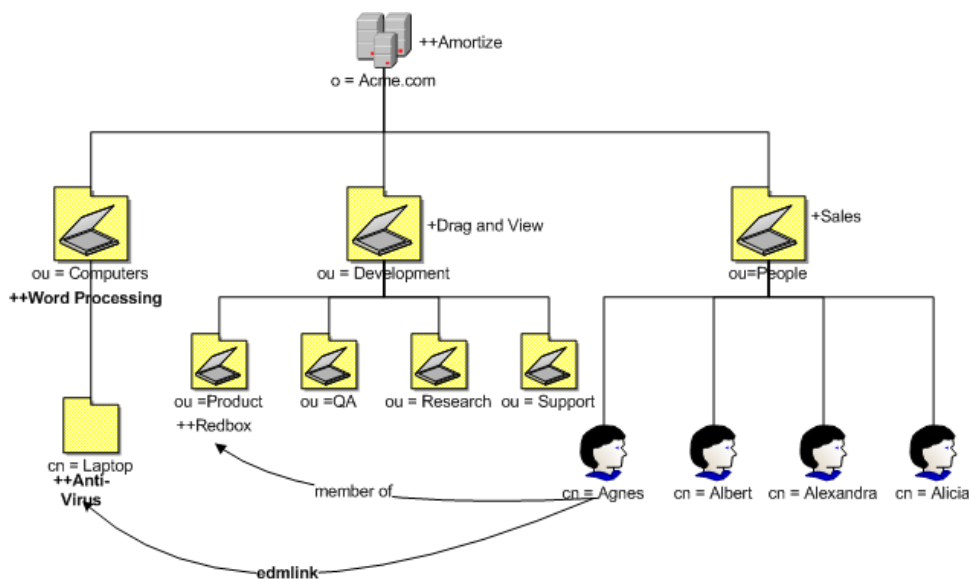
In Figure 4, above, Agnes will receive Anti-Virus because she has been linked to the laptop container. Since laptop is part of the Computers organizational unit, she will also get Word Processing. Now, she has a total of six applications.

Managing Policy Scope

If you do *not* want to inherit the policy from the parent objects, you can limit the Policy Server's scope of resolution. You can do this either globally for the entire directory structure or for only specific objects. Manage the scope globally by modifying the Policy Server configuration file. Control policy scope for one object by using the edmFlags attribute.

⚠️ Be sure that you have a thorough understanding of your directory structure. When designing a change to the scope of policy resolution, anticipate the result of your modifications *before* making the modifications.

Controlling Policy Scope Globally

The VIEW option allows you to control whether or not to continue up the directory tree to assign policy. Modify the VIEW option in the Policy Server configuration file, `pm.cfg`, to control the scope.

The syntax for the VIEW option is:

```
VIEW {
    <attr> {view}
    }
```

Where *attr* is one of the attributes listed in the LINKS configuration option in `pm.cfg`, and *view* is a list of LINKS the Policy Server is allowed to see. An empty list means that there is no view when visiting an object from the specified attribute. This would result in following that link and not continuing. You can list as many or as few attributes as needed.

The default values for the LINKS configuration option are edmLink, memberof, groupmembership and aliasedobjectname. When you look at a particular object such as a group or user through the Policy Server interface, you will see only these attributes for that object. If you do not want Policy Server to inherit the policy for any parents of an edmLink attribute, modify the VIEW option in `pm.cfg` like this:

```
VIEW {
    edmLink {   }
    }
```

This configuration with the empty brackets tells Policy Server to follow edmLink, but not to inherit from any parents or any links contained within the object from that branch of the directory tree.

Looking back at the Acme organization example, suppose you want Agnes to receive policy for the laptop container, but not inherit any policy from the Computers organizational unit. In Figure 4 on page 42 Agnes will receive Anti-Virus because she has been linked to the laptop container, but she will not inherit Word Processing when edmLink is configured with empty brackets to not inherit from any parents.

Similarly, if we wanted to follow a memberof attribute, and then not inherit from the parent objects, we would replace edmLink with memberof. The VIEW option would look like this:

```
VIEW {
    memberof {   }
    }
```

This configuration with the empty brackets tells Policy Server to follow memberof, but not to inherit from any parents from that branch of the directory tree or any links contained within the object.

Finally, suppose that we only want to follow memberof relationships. The VIEW option would look like this:

```
VIEW {
    memberof {memberof}
    }
```

This configuration with the memberof in quotes tells Policy Server to follow memberof, but not to inherit from any parents from that branch of the directory tree. When we follow a memberof relationship, we will continue to follow memberof relationships until we reach an object that does not contain a memberof relationship. In Figure 5 below, Agnes will get Sales, Amortize. Then she will get Redbox because she is a member of Product. Since Product is a memberof laptop, she will get Anti-Virus. If Laptop had any memberof relationships, she would follow those relationships, too. Agnes will not follow any relationships other than memberof.

Figure 5   Product is a member of the laptop container
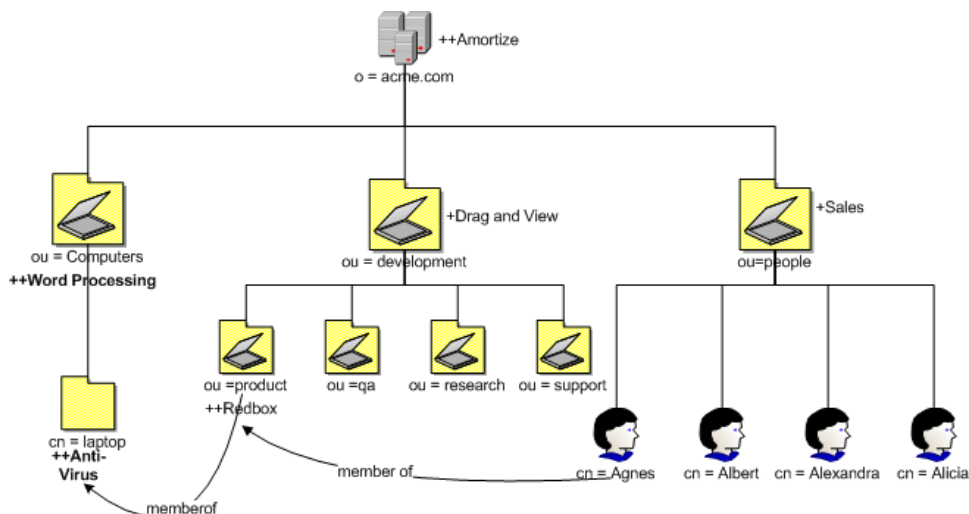
Log Files

To troubleshoot your Policy Server, you may need to examine the log file. Within the logs directory for your Integration Server, examine `httpd-3466.log`. This log is created when the Integration Server service starts up. It contains useful information if errors occur.

Summary

- Configure the Policy Server to connect to your directory services.

- Modify your directory schema to include the HPCA policy attributes that allow you to manage policy scope, relationships, and assignments.

- Configure your Configuration Server to use the LDAP method.

- You can control the scope of policy resolution globally using the VIEW option in the Policy Server configuration file.

- Following Policy Server configuration, use the Enterprise Manager to add, administer, and query policy entitlements in your LDAP policy store.

A   LDAP Discussion

This appendix provides more information on directory services for policy administrators needing additional information. It also includes descriptions of LDAP terminology, the use of substitution and expressions, and URLs used for HP Client Automation (HPCA) Policy Server.

LDAP Background

An LDAP directory is a hierarchically named tree of objects, where each object has a class (type) or classes, and contains potentially many named attributes, appropriate to its classes. Each attribute may contain multiple values.

It is outside the scope of this document to describe in any detail what an LDAP directory means. As a rapidly growing force in the systems management industry, many excellent sources exist for further background.

The Policy Server is not concerned with such differences in interpretation—our only requirement is that the directory supports either the LDAP v2 or LDAP v3 protocols.

HPCA Policy Server and LDAP

The LDAP Policy Extension, in conjunction with the HPCA Policy Server (Policy Server), is intended to provide a scalable policy infrastructure, leveraging your existing investment in directories. The LDAP Policy Extension was developed to provide "Low Cost of Entry" to policy-based management, allowing you to start with a very simple policy model and incrementally grow the model as your policies mature. The LDAP Policy Extension provides a clean integration with the standard repository for enterprise management information (LDAP), and allows an organization to leverage the information represented in its directories to deliver sophisticated policy-management to the many computing devices in its enterprise.

The Policy Server is aimed at customers who have a detailed understanding of LDAP/X.500 directories, and an established directory infrastructure. The Policy Server uses the LDAP protocol (version 2 or 3) (over TCP/IP) to speak to the customer's directory. This protocol encompasses all major directory products on the market, including the latest offerings from companies such as Novell, Microsoft, and Netscape.

The LDAP Policy Extension extends the Policy Server with a number of features that enable you to represent your software management policy within your existing directory infrastructure and have this policy drive your HPCA infrastructure to provide a comprehensive and sophisticated software management solution.

The extension makes policy resolution available via a URL utilizing the standard Policy Server policy framework. It maintains a persistent LDAP connection to your corporate directory, and provides online HTML documentation. From the Enterprise Manager, there are a number of interactive tools for discovering or diagnosing the policy outcome for target objects (typically users or machines) in your directory.

It is anticipated, but not required, that the Policy Server hosting this extension be co-located on or near the directory to keep network latency to a minimum and enhance performance and manageability.

The LDAP Policy Extension understands the standard relationships that exist in a directory between different objects (parent-child, memberOf). In addition to these standard relationships, three additional attributes may be used:

- <pfx>Flags
  controls various subtle aspects of the policy resolution.

- <pfx>Link
  allows you to specify additional, potentially dynamic or conditional relationships.

- <pfx>Policy
  allows you to define resultant strings that will be netted out during policy resolution.

By default the prefix used is `edm`, but alternatives may be used to allow your directory to support multiple concurrent policy frameworks for different purposes.

The LDAP Policy Extension starts at the specified DN, and walks the entire tree of relationships that the object has with other objects, accumulating policy attributes. Then it evaluates all conditional policies, and finally

resolves any conflicting policies, using a straightforward should/may, grant/deny model.

Terminology

Before using directory-based policy management with Policy Server, it is important to establish some terminology that is used throughout this discussion.

- **Should**

  This is used to describe a mandatory or **required** policy.

- **May**

  This is used to describe a desired or **advisory** policy.

- **Policy**

  This is a string that is used to **represent** a **desired** outcome. The Policy Server does not impose any particular interpretation upon this. When used in conjunction with the LDAP Adapter, the adapter will *interpret* this as the name of an application defined within HP Client Automation.

- **Relationship (link)**

  Two directory objects are said to be **related** if one can be reached from the other, directly or indirectly. Examples of relationship include parent-child, and group membership (a user is **related** to the group he is a member of). Relationships are unidirectional.

- **MemberOf**

  This is used to describe a **relationship** between two objects. Many common directories support an attribute called **memberOf** that embodies this relationship, typically between users and groups.

Substitution

Two forms of substitution are provided:

- Current Object Attributes: <<nameOfAttr>, or

- Inbound Object Attributes: <<in.nameOfAttr>>

The former allows you to construct expressions based upon the value of another attribute in the current object (same one that contains the edmLink or edmPolicy), for example,

```
edmLink: cn=<<homePC>>, cn=Computes, o=Acme.
edmLink: cn=wnt001, cn=Computers, o=Acme ; <<homePC>> ==
"wnt001".
```

The latter allows you to reference attributes that were supplied as input to
the policy resolution, for example:

```
edmPolicy: ++SOFTWARE/STRATUS_PAD; <<in.hostname>> ==
"XKEZ01$"
```

Currently the minimum attributes that will exist are listed in Table 5, below.

Table 5   Default Inbound Object Attributes <<in.nameOfAttr>>

Attribute Name	Sample Value
context	{}
dn	{cn=su61er, cn=computers, dc=acme, dc=com}
dname	software
domain	{ACMEWEST\XKEZ01$}
hostname	{XKEZ01$}
ipaddress	192.168.0.100
mtime	{2007-06-22 18:54:35}
nvdipnetworknumber	192.168.0.0
nvdsubnet	255.255.255.0
smenclosureserialnumber	CNU0123456
smsystemproductname	{HP Compaq nc6000 (DU655C)}
smsystemmanufacturer	Hewlett-Packard
smsystemserialnumber	CNU0123456
smsystemuuid	27494E2D171E11DB09906D9908020929

Expressions

The expressions are implemented as Tcl (**www.scriptics.com**) expressions,
where instead of using $myVar you would use <<myAttribute>>. A simplified
summary of valid expressions is provided below. Most of the standard C
language expression operators are valid.

Table 6   Expressions

Expression	Meaning
A && B	Logical AND
A || B	Logical OR
!A	Logical NOT
<<myAttr>> == "Hello"	Test for equality (case-sensitive)
<<myAttr>> != "Hello"	Test for inequality
<<myAttr>> < 55	Numerical comparison for less than
<<myAttr>> >= "Hello"	Dictionary comparison for greater than or equal to (C locale)

There are also a small number of specialized functions.

Table 7   Specialized Function Example

Example	Meaning
[memberOf "ou=Accounting, o=Acme"]	Yields TRUE if the DN specified is part of your policy model.
[parent <<dn>>] == <<aSpecialDN>>	Yields TRUE if the parent DN of the current object is the same as the "aSpecialDN".

The LDAP Extension URL Namespace

The LDAP extension provides the following special purpose URLs:

Table 8   LDAP Extension URL Namespace

URL	Description
/policy/ldap?<x-url encoded query>	Perform machine-readable policy resolution. The query arguments should be an attribute value list of inbound attributes, formatted in accordance with the X-URL encoding specification. The following attributes are currently supported and interpreted by the LDAP Policy Extension: • **dn -** the distinguished name or LDAP URL to perform policy resolution upon. (REQUIRED) • **phase -** the value may be specified as "1", "2", or "3", to view the intermediate stages of policy resolution. (default=3) • **prefix -** the value is the prefix to use when searching the directory for policy related attributes, i.e., <pfx>Policy or <pfx>Link. (default=edm) • **debug** - the value is the log level to use for this single query, a value of 9 or above will generate detailed logging in the Policy Server log file. (no default)
/status/ldap	Return an overview of the current status of the extension.
/status/ldap/all	Return all available status information on extension.
/status/ldap/cache	Return information on cache.
/status/ldap/stats	Return statistics on usage of extension.

URL	Description

/admin/ldap/flush?dn=<dn>	Force a flush of the cache. If no dn, or an empty dn, is supplied, then the entire cache is flushed. Otherwise, just the specified dn is flushed. Encode any special characters in the <dn> value using their ASCII equivalents, as shown in the Syntax Example below.
	
	Pre-requisite:
	Uncomment this line in the `httpd.rc` file:
	`#Admin_Url        /admin`
	and restart the service for the HPCA Integration Server.
	
	Syntax Example:
	To flush the cache of the dn:
	`dc=test,dc=com`
	encode the <dn> value by replacing the equal signs (=) with **%3d**, and the comma (,) with **%2c**:
	The resulting URL to flush the cache of this dn is:
	/admin/ldap/flush?dn=dc%3dtest%2cdc%3dcom

/admin/ldap/reset	Reset connection to directory (forces a flush and reconnect). **Pre-requisite:** Uncomment this line in the `httpd.rc` file: `#Admin_Url        /admin` and restart the service for the HPCA Integration Server.
/ldap/config.tsp	Summary configuration page, and interactive controls for resetting cache and connection.
/ldap/browse.tsp?dn=<dn>	Directory Browser and Policy Editor.
/ldap/query.tsp?dn=<dn>	Interactive Policy Resolver—simple diagnostic page allowing you to interactively submit policy requests and see the policy outcome, as well as the steps that led to that outcome, in a friendly formatted HTML page.
/ldap/test.tsp?dn=<dn>	This URL can be used to test connections to arbitrary directory servers, and is useful when diagnosing problems with authentication and directory access.

B Use Existing LDAP Attributes

The goal of this feature is to allow HP Client Automation (HPCA) customers to implement the Policy Server without requiring schema changes. This can be accomplished by using an existing directory service attribute to embed the required attributes and their values.

> ⚠️ Do not implement this feature with a directory that already has the necessary attributes. The feature will *not* function properly. See Adding Client Automation Policy Attributes on page 28 before using an existing LDAP attribute.
>
> This feature should *only* be used when it is not possible to make the necessary LDAP schema changes as shown in Adding Client Automation Policy Attributes *on page 28*.

To use this feature, you must have an unused multi-valued LDAP attribute that already exists in the directory schema that can exist in any object that will have policy assignments. Use the EMBED configuration option in the Policy Server configuration file, `pm.cfg`. The value of EMBED must be the name of an attribute that already exists in the schema of your LDAP directory. The attribute should be one that is allowed to exist in all objects for which policy will be assigned.

The attribute should be multi-valued and of type string. The embedded data will be stored in multiple values of the attribute – one embedded policy per value. The original contents will be maintained along with any policies assigned to the object.

Suppose you are going to use an already existing attribute called "displayname". Add the following line to `pm.cfg`:

```
EMBED              {displayname}
```

By default, the EMBED options assumes that the displayname attribute is multi-valued.

C Domain Filtering

If you are using the HP Client Automation (HPCA) Policy Server to create entitlements in your enterprise, you can filter out which domains the Policy Server will assign services from based on connect parameters.

If you are using the Policy Server with HPCA Patch Manager (Patch Manager), you will want to separate resolution of regular software services from those for Patch Manager. The Policy Server filters services based on the dname passed on the radskman command line. The Policy Server configuration file, pm.cfg, contains filter settings in the format:

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

Where the DOMAIN NAME is the value passed in dname by RADISH. In the case of a Patch Manager agent, this will be the dname parameter of radskman. Dname should be patch. If the filter name passed in dname is not found in pm.cfg, then the filter DNAME=* will be used.

The default configuration for these filters is shown below:

```
DNAME=*          { * !PATCHMGR !OS !SECURITY !AUDIT }
DNAME=PATCH      { PATCHMGR }
DNAME=OS         { OS }
DNAME=VM         { SECURITY }
DNAME=SECURITY   { SECURITY }
DNAME=AUDIT      { AUDIT }
```

In this configuration the default rule (*) will ignore PATCHMGR, OS, SECURITY and AUDIT domains and allow everything else as denoted by the use of an exclamation point (!). PATCH, OS, and AUDIT rules allow only policies for PATCH, OS, and AUDIT domains, respectively.

If the dname parameter passed by radskman is either VM or SECURITY, the rules allow only policies for SECURITY.

If, for instance, we wanted to allow any policies for AUDIT resolution we would change the last filter to: DNAME=USAGE { * }.

Index