

HP OpenView Configuration Management Policy Server

for the UNIX and Windows operating systems

Software Version: 5.00

Installation and Configuration Guide

Document Release Date: January 2008

Software Release Date: April 2007



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2001-2008 Hewlett-Packard Development Company, L.P.

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.

Acknowledgements

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

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

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

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

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

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 since the last released edition.

Table 1 Document Changes for this 5.00 Release

| Chapter | Version | Changes |
|---------|-------------------|--|
| 2 | 5.00 | Page 18, Verify Installation , revised procedures. |
| 3 | 5.00 | Page 33, Connecting to the LDAP Method , modified Step 4 to indicate the <code>_ALWAYS_</code> Utility Method requires a value of <code>SYSTEM.ZMETHOD.LDAP_RESOLVE</code> . |
| A | 5.00 | Page 57, Substitution , earlier references to these minimum inbound object attributes were deleted: <ul style="list-style-type: none">• <code>in.os</code> is not available by default• <code>in.uid</code> is now <code>in.smsystemuuid</code>• <code>in.host</code> is now <code>in.hostname</code> Table 7 on page 58 lists the minimum inbound attributes available when using CM Policy Server with LDAP. |
| A | All 5.xx Versions | Page 59, Table 10, The LDAP Extension URL Namespace , updated the pre-requisite and syntax information for <code>/admin/ldap/flush?dn=<dn></code> and <code>/admin/ldap/reset</code> . |

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 | 9 |
| | About CM Policy Server | 10 |
| | Benefits | 10 |
| | CM Policy Server Processing..... | 11 |
| | About the CM Integration Server | 12 |
| | About this Guide | 13 |
| | Summary | 14 |
| | | |
| 2 | Installation | 15 |
| | CM Policy Server Installation..... | 16 |
| | License File and Support..... | 16 |
| | Tips..... | 16 |
| | Platform Coverage | 16 |
| | Verify Installation | 18 |
| | Summary | 20 |
| | | |
| 3 | Configuring and Administering Policy | 21 |
| | Adding Configuration Management Policy Attributes..... | 22 |
| | Adding the nvdObject Class | 23 |
| | Modifying classes with nvdObject | 23 |
| | Connection to LDAP | 24 |
| | Support for Multiple LDAP Connections..... | 27 |
| | Specifying the CM Configuration Server..... | 27 |
| | Configuring the LDAP Method..... | 28 |
| | Specifying the Distinguished Name | 32 |
| | Connecting to the LDAP Method..... | 33 |
| | Distributed Administration | 34 |

| | |
|--|-----------|
| Configuring the Service Drop Down..... | 36 |
| Adding a Policy (EdmPolicy)..... | 36 |
| Removing a Policy | 39 |
| Setting Policy Defaults and Overrides (EdmPolicyDefault and EdmPolicyOverride) | 41 |
| Adding a Link (EdmLink) | 43 |
| Policy Scope..... | 45 |
| Managing Policy Scope | 47 |
| Controlling Policy Scope Globally..... | 48 |
| Controlling Policy Scope Locally (edmFlags)..... | 50 |
| Log Files | 52 |
| Summary | 53 |
| A LDAP Discussion | 55 |
| LDAP Background..... | 55 |
| CM Policy Server and LDAP..... | 55 |
| Terminology | 57 |
| Substitution | 57 |
| Expressions | 57 |
| The LDAP Extension URL Namespace | 59 |
| B Use Existing LDAP Attributes..... | 63 |
| C Domain Filtering..... | 65 |
| D Product Name Changes | 67 |
| Index | 69 |

1 Introduction

At the end of this chapter, you will:

- Know the benefits of the HP OpenView Configuration Management Policy Server (CM Policy Server).
- Understand CM Policy Server processing.

About CM Policy Server

The CM 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 Configuration Management (CM) infrastructure providing integration and extended enterprise functionality with your directory services. Policy method connections in the CM Configuration Server DB (CM-CSDB) are used to determine what services should be distributed and managed for the user that is currently logged on by querying the CM Policy Server.

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



The CM 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 CM 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. 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 CM Policy Server can be summarized in the following points:

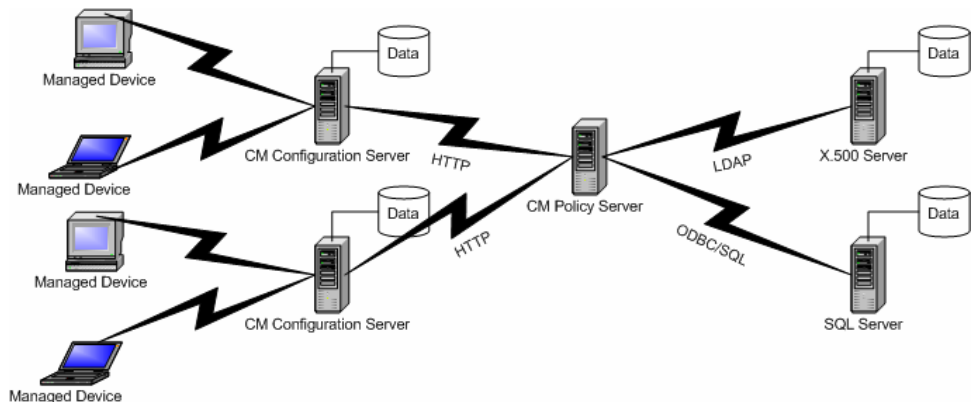
- **Simplicity**
The model should be no more complex than your policies.
- **Sophistication**
The model should be capable of expressing even the most subtle or complex policies you need.

- **Clarity**
Each organizational policy should exist only once in the model, 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.

CM Policy Server Processing

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

Figure 1 CM Policy Server processing



In Figure 1 the following things occur:

- 1 The CM agent connects to the CM Configuration Server to resolve its **desired state**. The desired state embodies the content that CM manages for a device. The desired state for each device is dynamically created by the CM Configuration Server based on information in the CM Configuration Server DB.
- 2 The CM Configuration Server contacts the CM Policy Server to perform policy resolution, and builds the client'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 CM Policy Server, and treats the results as a set of objects and attributes to be incorporated into the desired state of the connected client.
- 4 The CM Configuration Server completes resolution of the desired state and returns the information to the CM agent.

The CM Policy Server maintains a persistent connection to an LDAP directory server (or SQL database) 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. It also provides an HTML-based interface for administering policy information.

The CM Policy Server can also take input via HTTP POST from multiple CM Configuration Servers. The CM 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 CM Integration Server

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

Benefits of the CM Integration Server are:

- All the products using the CM Integration Server for Windows are loaded from a single Service called "HP OVCM Integration Server".
- When the CM 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 CM 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.

About this Guide

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

- **Installation** - This chapter describes how to install the CM Policy Server.
- **Configuring and Administering LDAP:** This chapter describes how to configure and administer your CM environment with LDAP services.

Summary

- The CM 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 CM Policy Server acts as a bridge between the CM Configuration Server and a directory server.
- The CM Policy Server is a module of the CM Integration Server.

2 Installation

At the end of this chapter, you will:

- Know how to install the HP OpenView Configuration Management Policy Server (CM Policy Server).
- Be able to verify installation of the CM Policy Server.



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

CM Policy Server Installation

Before you install the CM Policy Server, identify the server where the CM Policy Server will reside. Administrators usually choose the same physical server that is running the Directory Services (or SQL database), or the CM Configuration Server. Review to 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 CM Policy Server. Install the CM Policy Server from the CM 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.

To install the CM Policy Server for Windows

- 1 From the CM installation media, navigate to the `\Infrastructure\management_extensions\policy_server` directory. Open the folder for your operating system.
- 2 Double-click **setup**. The CM 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 CM 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 CM Policy Server is running by performing the following verifications. You can directly access the CM Policy Server by following the procedure [To access the CM Policy Server](#) below.

To access the CM Policy Server

- 1 Open your Web browser.
- 2 In the Address bar, type **http://IP_Address:3466**. This will be referred to as the CM Policy Server page.

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

The CM Integration Server CM Policy Server Web page opens.

- 3 Click **Directory Services** in the command bar.

The Policy Manager for LDAP page opens.

[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 queries 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 **Browse** to verify that you can move through the sample database.

| | |
|--|---|
| ldap://acme.ldif:389 o=acme.com | Resolve Policy: o=acme.com description: Not Available Show Children: Yes Verbose: No <input type="button" value="Filter"/> <input type="text"/> <input type="button" value="Goto"/> <input type="text"/> |
|--|---|

| Action | Attribute | Value |
|------------------------------------|--|---|
| <input type="button" value="Add"/> | <input type="text" value="edmPolicy"/> | <input type="text" value="-----Select-----"/> <input type="text" value="-----Select-----"/> <input type="text"/> |
| | edmpolicy: | +ms office |
| | ou=computers | ou=groups ou=sales |
| | ou=development | ou=people |
| | ou=fao | ou=roles |

Summary

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

3 Configuring and Administering Policy

At the end of this chapter, you will:

- Know what attributes to add to your directory service for use with HP Configuration Management Policy Server (CM Policy Server).
- Understand how to configure the method for resolving LDAP policies in the CM Configuration Server DB.
- Be able to administer policy.

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

- 1 Add the required attributes for CM Policy Server to your directory service.
- 2 Configure the CM Policy Server to connect to your directory server.
- 3 If your CM Configuration Server and CM Policy Server are on two separate computers, you will need to configure them to communicate.
- 4 Configure the LDAP resolve method on your CM Configuration Server to use your directory server.
- 5 Connect the LDAP resolve method to a policy instance in your CM Configuration Server DB.

After completing these steps, you can begin to administer policy using the CM Policy Server.

Adding Configuration Management Policy Attributes

The CM 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 scheme 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 `edmPolicyOverride` as a multi-valued, case-exact string with an object ID of 1.3.6.1.4.1.2133.2.1.4. Use `edmPolicyOverride` to define policy overrides. This is added as an optional attribute of the `nvdObject` class.
- Add `edmPolicyDefault` as a multi-valued, case-exact string with an object ID of 1.3.6.1.4.1.2133.2.1.5. Use `edmPolicyDefault` to assign policy defaults. This is added as an optional attribute of the `nvdObject` class.

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 CM 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 CM 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 CM Policy Server for LDAP](#) below for instructions on how to connect CM 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 CM Integration Server directory. HP recommends changing the LDAP configuration through the CM 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 CM Policy Server or CM Integration Server service.

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 CM Policy Server for LDAP

- 1 From the CM 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 | <input checked="" type="radio"/> ldap <input type="radio"/> ldif |
| Ldif | <input type="text"/> |
| Host* | <input type="text" value="10.10.10.12"/> |
| Port* | <input type="text" value="389"/> |
| Version | <input type="radio"/> 2 <input checked="" type="radio"/> 3 |
| Base Dn | <input type="text" value="dc=asdfoods,dc=com"/> |
| Bind Dn | <input type="text" value="cn=Administrator ,cn=Users,dc=asdfoods,dc=com"/> |
| Bind Pw | <input type="password" value="*****"/> |
| Prefix* | <input type="text" value="edm"/> |

- For Type, select the **ldap** option.
- 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 |
| 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 |

- 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 CM Integration Server or CM Policy Server service.

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. |
| 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. |
| Ping_freq | 300 | The delay between each attempt to search Base Dn (in seconds). This enables the CM 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

CM Policy Server supports multiple concurrent LDAP queries. Configure the number of concurrent LDAP queries in the CM 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 CM 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 CM 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 <code>pm.cfg</code> , then you will need to add it. |

Specifying the CM Configuration Server

If your CM Configuration Server is not on the same computer as your CM Policy Server, you will need to specify the location of the CM Configuration Server. To do this, edit the CM Configuration Server profile file, `edmprof.dat`, and the CM Policy Server configuration file, `pm.cfg`.

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

- 1 On the CM Configuration Server computer, open the Profile Editor. This opens the CM 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 CM Policy Server as the value for `HTTP_HOST`.
- 4 Type the port of the CM Policy Server as the `HTTP_PORT`.
- 5 Save and close the `edmprof.dat`.

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

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

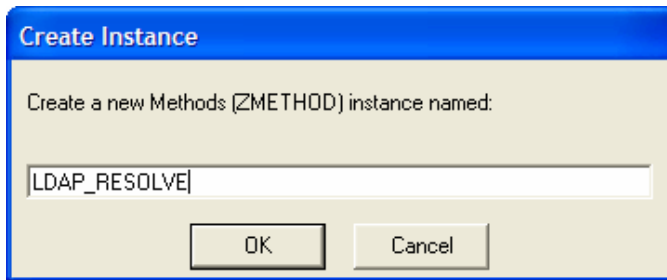
- 1 Open the CM Policy Server's configuration file, `pm.cfg`, using a text editor. This file is located in the CM Integration Server's `etc` directory.
- 2 Type the IP address of your CM Configuration Server as the value for the `RCS_CACHE_HOST`. If the port is different from the default of `RCS_CACHE_PORT`, change that value as well.
- 3 Save and close the modified `pm.cfg`.
- 4 Stop and restart the CM Integration Server service.

Configuring the LDAP Method

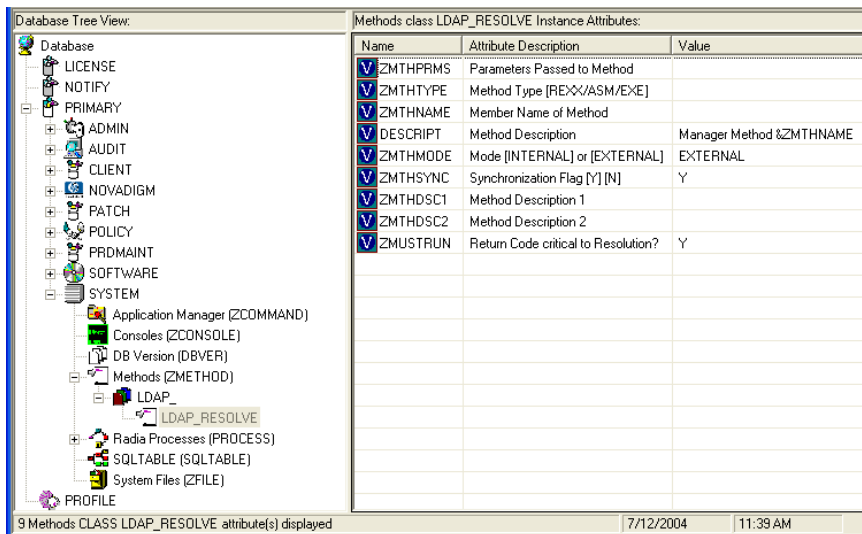
If you are using LDAP, you must create a connection to the LDAP method in the CM Configuration Server DB, and connect the users to the LDAP method. Perform the following two procedures to prepare your CM Configuration Server DB to use the CM Policy Server.

To create the LDAP method in the CM Configuration Server DB

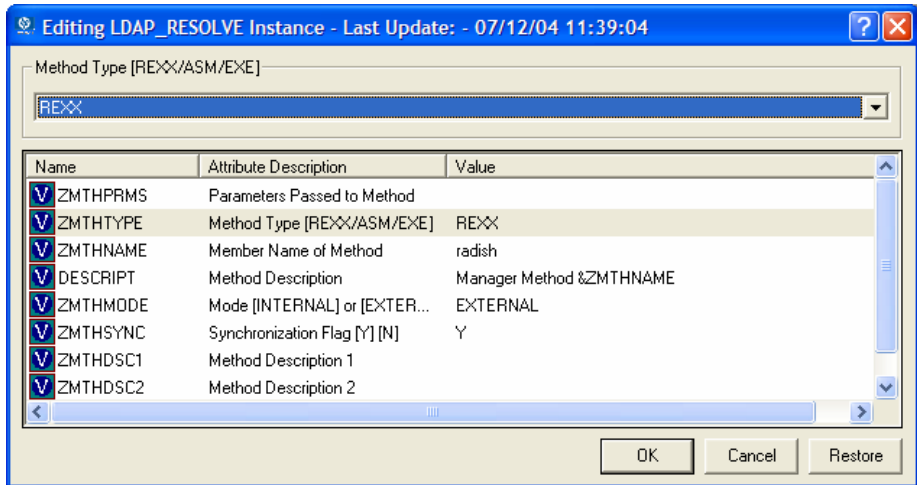
- 1 In the CM Admin CSDB Editor, go to `SYSTEM.ZMETHOD`.
- 2 Right-click **Methods (ZMETHOD)**.
A shortcut menu opens.
- 3 From the shortcut menu, select **New Instance**.
The Create Instance dialog box opens.



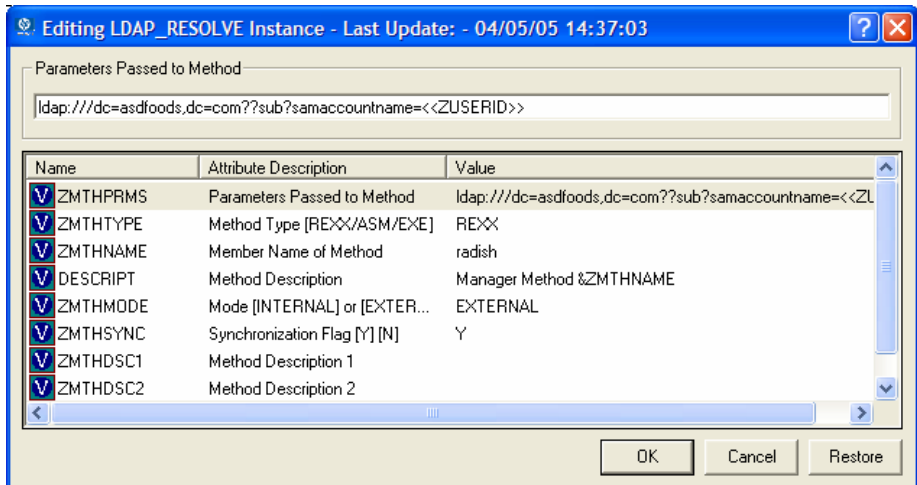
- 4 Type **LDAP_RESOLVE** in the text box, and click **OK**.
The CM Admin CSDB Editor window opens.
- 5 Double-click **LDAP_**.
The tree expands.
- 6 Double-click **LDAP_RESOLVE** in the tree view.
The attributes of **LDAP_RESOLVE** appear in the list view.



- 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**.
- 9 Click **ZMTHTYPE**.



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



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

For HTTP type:

`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?samaccountname=<<ZUSERID>>$ (If the client uses $MACHINE as the ZUSERID)
```

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

For example,

```
ldap:///dc=asdfs,dc=com??sub?samaccountname=<<ZUSERID>>$
```

- To manage policies by user:

```
ldap:///dc=domainname,dc=forestname,dc=com??sub?samaccountname=<<LOCALUID>>
```

For example,

```
ldap:///dc=asdfs,dc=com??sub?samaccountname=<<LOCALUID>>
```

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 CM Admin CSDB Editor window opens.

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

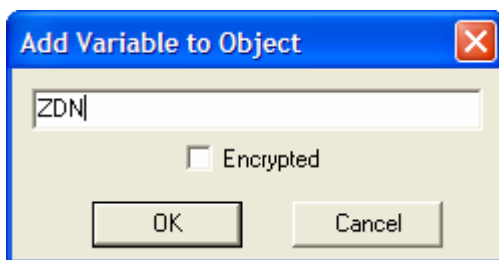
Specifying the Distinguished Name

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 Configuration Management Application Self-service Manager logon screen to the distinguished name in LDAP due to a limitation in LDAP.

To specify the distinguished name (dn)

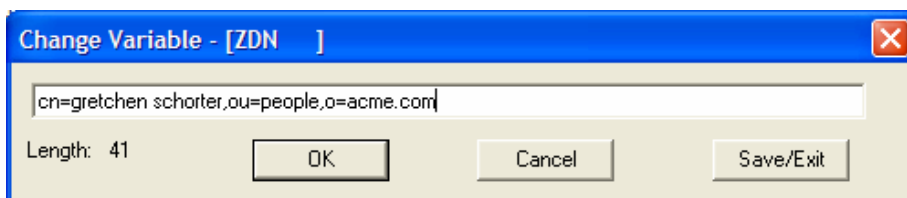
- 1 Go to **Start → Programs → HP OVCM Administrator** and click **CM Admin Agent Explorer**.
- 2 Go to *SystemDrive:\Program Files\Hewlett-Packard\CM\Agent\Lib*.
- 3 Double-click **ZMASTER**.
- 4 From the **Variable** menu, click **Add**.

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**.

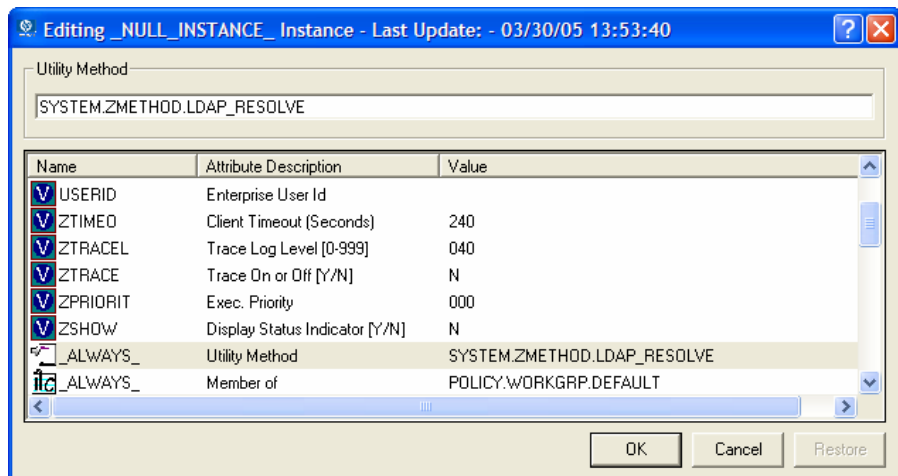
- 8 Click **OK**.
- 9 Click **Save/Exit**.

Connecting to the LDAP Method

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

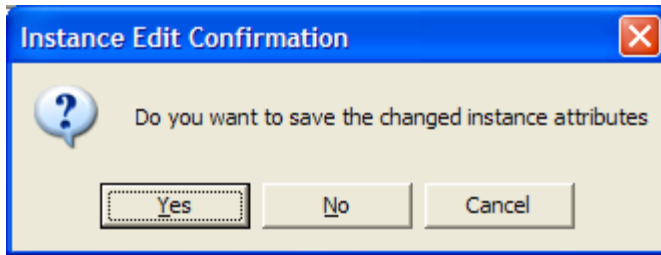
To connect the user to the LDAP method

- 1 Open the CM 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.

Distributed Administration

By default, the CM Policy Server connects to your directory service using the configured base DN. This user has administrative access to the entire directory starting from the configured base DN. In other words, all Configuration Management Policy administrators have full access to the entire LDAP directory.

You can limit access for a Configuration Management Policy administrator by defining his access in your LDAP directory. Then, when this administrator logs in, he will be prompted for a password, and will only have rights to the parts of the directory that you defined.

Figure 2 Set security



The administrator will be prompted to re-enter a user name and password if the connection has timed out. The logon times out when there is no activity on the Web page for a period of time. The default period is two minutes. To change the timeout, add the following to the `pm.cfg` file in the CM Integration Server `etc` directory:

```
ADMIN_TIMEOUT <timeout in seconds>
```

To enable distributed administration

- 1 Use a text editor to open the `pm.cfg` file from the CM Integration Server's `etc` directory.
- 2 Add or uncomment the following line from the `pm.cfg`:
`SetAccess /ldap "Policy Server" DIR <LDAP search URL>`
- 3 Replace `<LDAP search URL>` with the appropriate location for your enterprise. It should be typed all in one line.

Example:

```
SetAccess /ldap "Policy Server" DIR  
"ldap:///cn=users,dc=your_company_dc,dc=com??sub?(samaccountname=<<user>>)"
```

- 4 Save and close the file.

Distributed administration for your CM Policy Server has been enabled. Set security for your Configuration Management Policy administrator in your directory service.

Configuring the Service Drop Down

Now that you have configured your CM environment to use the policies created in CM Policy Server, you can begin administering it. To use the CM Policy Server's drop-down box for the service list, you will need to create and configure a user who is entitled to all of the services you want to manage using the CM Policy Server. If you are using Microsoft Internet Explorer version 6.0 or above, the services will be listed alphabetically under the domain where the service resides. Otherwise, the services will not be subdivided by domain.

To configure the Server Dropdown

- 1 Use the CM Admin CSDB Editor to create a user, such as POLUSER, in the CM Configuration Server DB POLICY domain.
- 2 Use the CM Admin CSDB Editor to assign POLUSER any services that you want to manage with the CM Policy Server.
 - ▶ Keep your list of services to a manageable size. However, if you need to be able to manage all of the services using the CM Policy Server, type **SOFTWARE.ZSERVICE.*** into one of the `_ALWAYS_` connections for POLUSER. This will connect POLUSER to all services.
- 3 Use a text editor to edit the `pm.cfg` file's `RCS_CACHE_USER` to be POLUSER. This connects the CM Policy Server to the services for the POLUSER. The default location of `pm.cfg` is `System Drive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc`.

Adding a Policy (EdmPolicy)

The procedure [To add a policy](#) below shows an example of how to add a software entitlement attribute using the CM Policy Server.



If CM Policy Server is used to store services, do not connect the same Application (ZSERVICE) instance using both the CM Configuration Server DB and the CM Policy Server. In addition, only ZSERVICE instances should be assigned using CM Policy Servers. The only notable exception to this rule is connecting an instance of the POLICY.STAGER class to a user or group of users in LDAP for the purposes of assigning an CM Proxy Server to a user or group of users. See technical note OV-ENKB01211: Assigning a Stager instance through the CM Policy Server on the HP Technical Support Web site for more information.

To add a policy

- 1 Open your Internet browser to the CM Policy Server page.
- 2 Click **Browse**.

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

| ldap://acme.ldif:389 o=acme.com | | Resolve Policy: o=acme.com description: Not Available Show Children: Yes Verbose: No <input type="button" value="Filter"/> <input type="text"/> <input type="button" value="Goto"/> <input type="text"/> |
|--|--------------------------------|---|
| Action | Attribute | Value |
| <input type="button" value="Add"/> | edmPolicy | <input type="text"/> |
| | edmpolicy : | +ms office |
| | ou=computers | ou=groups ou=sales |
| | ou=development | ou=people |
| | ou=fao | ou=roles |

- 3 Click on an organizational unit in the bottom section of the policy management screen to select it for policy management. In the figure on the next page, we selected the sales organizational unit.
- 4 Make sure that edmPolicy is selected in the **Attribute** drop-down box.
- 5 From the first drop-down box in the Value section, select the appropriate keyword. The options are **may**, **may not**, **should**, and **should not**. See [Table 5](#) on page 38 for additional information. After selecting the keyword, the value box will display the appropriate character for that value. In our example, we selected May.

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



| ldap://acme.ldif:389  o=acme.com  ou=sales | Resolve Policy: ou=sales, o=acme.com description: Not Available Show Children: Yes Verbose: No <input type="button" value="Filter"/> <input type="text"/> <input type="button" value="Goto"/> <input type="text"/> | |
|--|---|--|
| Action | Attribute | Value |
| <input type="button" value="Add"/> | <input type="text" value="edmPolicy"/> | <input type="text" value="May"/> <input type="text" value="-----Select-----"/> <input type="text" value="+"/> |
| ou=post-sales | | ou=pre-sales |

Table 5 Assigning Services with the Pick List

| If the value entry box, shows . . | You have specified . . . |
|-----------------------------------|---|
| + | that an application may be delivered. |
| - | that an application may not be delivered. This overrides +. |
| ++ | that an application should be delivered. This overrides -. |
| -- | that an application should not be delivered. This overrides ++. |

- From the second drop-down box in the **Value** section, select the appropriate CM Application (ZSERVICE) in its appropriate domain. In our example, we selected Amortize.

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

| ldap://acme.ldif:389 o=acme.com ou=sales | | Resolve Policy: ou=sales, o=acme.com description: Not Available Show Children: Yes Verbose: No <input type="button" value="Filter"/> <input type="text"/> <input type="button" value="Goto"/> <input type="text"/> |
|--|--|---|
| Action | Attribute | Value |
| <input type="button" value="Add"/> | edmPolicy <input type="button" value="v"/> | May <input type="button" value="v"/> Amortize <input type="button" value="v"/> +SOFTWARE/AMORTIZE |
| ou=post-sales | | ou=pre-sales |

7 Click **Add**. The Amortize service is added to the policy model.



If you do not want to use the drop down box, you may type in your policy entitlement instead of using the values shown in Table 5 on page 38.


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



| ldap://acme.ldif:389 o=acme.com ou=sales | | Resolve Policy: ou=sales, o=acme.com description: Not Available Show Children: Yes Verbose: No <input type="button" value="Filter"/> <input type="text"/> <input type="button" value="Goto"/> <input type="text"/> |
|--|--|---|
| Object has been modified | | |
| Action | Attribute | Value |
| <input type="button" value="Add"/> | edmPolicy <input type="button" value="v"/> | May <input type="button" value="v"/> Amortize <input type="button" value="v"/> <input type="text"/> |
| | edmpolicy : | +SOFTWARE/AMORTIZE |
| ou=post-sales | | ou=pre-sales |





Removing a Policy


As your software model continues to develop, you may want to remove a policy. Use the CM Policy Server interface to remove policy.


To remove a policy


- 1 Open your Internet browser to the CM Policy Server page. This default is port 3466 on your CM Policy Server.
- 2 Click **Browse**.
- 3 Navigate to the group or user whose policy you want to modify.
- 4 Click on the recycle-bin icon  in the edmPolicy field that is associated with the application.

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

|  ldap://acme.ldif:389  o=acme.com  ou=sales | | Resolve Policy: ou=sales, o=acme.com description: Not Available Show Children: Yes Verbose: No |
|--|-------------|---|
| <input type="button" value="Filter"/> | | <input type="text"/> |
| <input type="button" value="Goto"/> | | <input type="text"/> |
| Action | Attribute | Value |
| <input type="button" value="Add"/> | edmPolicy | -----Select----- <input type="text"/> |
| Delete the following attribute/value? <input checked="" type="checkbox"/> <input type="checkbox"/> | | |
|  | edmpolicy : | +SOFTWARE/AMORTIZE |
| ou=post-sales | | ou=pre-sales |

- 5 Click on the  icon to confirm the removal of this policy.

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

| <p>ldap://acme.ldif:389</p> <ul style="list-style-type: none"> o=acme.com ou=sales | <p>Resolve Policy: ou=sales, o=acme.com</p> <p>description: Not Available</p> <p>Show Children: Yes</p> <p>Verbose: No</p> <p>Filter <input type="text"/></p> <p>Goto <input type="text"/></p> | | | | | | | |
|---|--|--|-------|-----|-----------|--|--|--|
| <p> Object has been modified</p> | | | | | | | | |
| <table border="1"> <thead> <tr> <th>Action</th> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Add</td> <td style="text-align: center;">edmPolicy</td> <td style="text-align: center;"> <div style="display: flex; justify-content: space-between;"> -----Select----- -----Select----- </div> <input type="text"/> </td> </tr> </tbody> </table> | Action | Attribute | Value | Add | edmPolicy | <div style="display: flex; justify-content: space-between;"> -----Select----- -----Select----- </div> <input type="text"/> | | |
| Action | Attribute | Value | | | | | | |
| Add | edmPolicy | <div style="display: flex; justify-content: space-between;"> -----Select----- -----Select----- </div> <input type="text"/> | | | | | | |
| <p>ou=post-sales</p> | <p>ou=pre-sales</p> | | | | | | | |

The policy for the Amortize service is removed.

Setting Policy Defaults and Overrides (EdmPolicyDefault and EdmPolicyOverride)

In addition to the existing values of the edmpolicy attribute, which either grant or deny access to an application (or object), two other types of policy are available.

- **edmPolicyDefault** - this policy neither grants nor denies access - but *if* access has been granted, then these values are used as the **default template** for that policy. For example, this can be used to provide default attributes that typically appear in the <...> section of a policy - such that the result is identical to if they had actually been present in the policy.

➤ If attributes of the same name appear in an actual granting policy then those have priority.

- **edmPolicyOverride** - this policy neither grants nor denies access, but *if* access has been granted, then these values **override** any equivalent attributes that were provided in the actual granting policy.

For a given application, more than one default may be encountered when resolving policy. In this case the defaults are ranked lowest to highest priority based upon the pri attribute only with lower numeric value being a higher priority. The same applies to for overrides.

The actual resulting policy that is returned to the CM Configuration Server will be the logical set union performed as an ordered overlay. In other words, same named attributes are replaced. This will be performed as follows:

- 1 Lowest to Highest Priority DEFAULTS (0...n occurrences)
- 2 Actual Granting Policy (always singular)
- 3 Lowest to Highest Priority OVERRIDES (0...n occurrences)

Example 1: simple override

- policy: Firefly <version=7 mode=typical>
- override: Firefly <version=8>
- OUTCOME: Firefly <version=8 mode=typical>

Example 2: simple default

- policy: Firefly <mode=typical>
- default: Firefly <version=7>
- OUTCOME: Firefly <version=7 mode=typical>

Example 3: default and override

- default: Firefly <mode=typical>
- policy: Firefly <version=7 issue=4>
- override: Firefly <version=8 mode=complete>
- OUTCOME: Firefly <version=8 issue=4 mode=complete>

Example 4: multiple defaults and multiple overrides

- default: Firefly <version=7> - Note: pri defaults to 10
- default Firefly <version=6 pri=5>
- policy: Firefly <mode=typical>
- override: Firefly <mode=complete> - Note: pri defaults to 10
- override: Firefly <mode=typical pri=5>
- OUTCOME: Firefly <version=6 mode=typical>



Neither defaults nor overrides have any affect to policy resolutions that do *not* grant access to the subject (Firefly in the above example). Defaults and overrides only affect policy objects that are already granted access to an application - and the effect that they have is only to refine the definition of that access by possibly altering the set of attributes that contribute to the POLICY object that is present when the subject object is resolved on the CM Configuration Server.

Adding a Link (EdmLink)

You may need to add a subscriber to a group without using your network's directory service. To do this, use the edmLink attribute. EdmLink allows you to create a connection to a group that is not part of the user's LDAP group membership. Then, the subscriber will inherit both the group membership assignments from LDAP and the assignments created with the edmLink attribute.




EdmLink should be used sparingly in the directory model. Its primary goal is to represent policy relationships between two objects that are not otherwise present in the form of parent-child or memberOf relationships.


In the example below, we will add Albert Kirkman to the research organizational unit so that he will inherit any services assigned to that unit.

To add a link

- 1 Open your Internet browser to the CM Policy Server page.
- 2 Click **Browse**.
- 3 Click on an organizational unit in the bottom section of the policy management screen to select it, or continue to select until you reach a particular user. In the figure below, we selected **albert kirkman** from the People organizational unit in acme.com.

|  | | Resolve Policy: cn=albert kirkman, ou=people, o=acme.com description: Albert Kirkman Show Children: Yes Verbose: No |
|--|-------------|--|
| <input type="button" value="Filter"/> <input type="text"/> <input type="button" value="Goto"/> <input type="text"/> | | |
| Action | Attribute | Value |
| <input type="button" value="Add"/> | edmLink | <input type="text"/> |
| | cn : | Albert Kirkman |

- 4 Make sure that edmLink is selected in the **Attribute** drop-down box.
- 5 Type the complete distinguished name for the group or user that you want the selected user to connect to. In this example, we are connecting Albert Kirkman to ou=research,ou=development,o=acme.com.

|  | | Resolve Policy: cn=albert kirkman, ou=people, o=acme.com description: Albert Kirkman Show Children: Yes Verbose: No |
|--|-------------|--|
| <input type="button" value="Filter"/> <input type="text"/> <input type="button" value="Goto"/> <input type="text"/> | | |
| Action | Attribute | Value |
| <input type="button" value="Add"/> | edmLink | <input type="text" value="ou=research, ou=development, o=acme.com"/> |
| | cn : | Albert Kirkman |

- 6 Click **Add** to add the link. The object has been modified and edmlink is added to the list of attributes for Albert Kirkman.

| | |
|--|---|
| ldap://acme.ldif:389 o=acme.com ou=people cn=albert kirkman | <p>Resolve Policy: cn=albert kirkman, ou=people, o=acme.com</p> <p>description: Albert Kirkman</p> <p>Show Children: Yes</p> <p>Verbose: No</p> <p>Filter <input type="text"/></p> <p>Goto <input type="text"/></p> |
|--|---|

Object has been modified

| Action | Attribute | Value |
|------------------------------------|--------------------------------------|--|
| <input type="button" value="Add"/> | <input type="text" value="edmlink"/> | <input type="text" value="----Select-----"/> <input type="text" value="-----Select-----"/> |
| | cn : | Albert Kirkman |
| | edmlink : | ou=research, ou=development, o=acme.com ; |

- Verify that the object is inheriting the services from the object it is linked to by clicking **Resolve Policy**. In this example, Albert Kirkman should receive Stratus Pad from the research organizational unit.

Desired Policy State: [cn=albert kirkman, ou=people, o=acme.com](#)

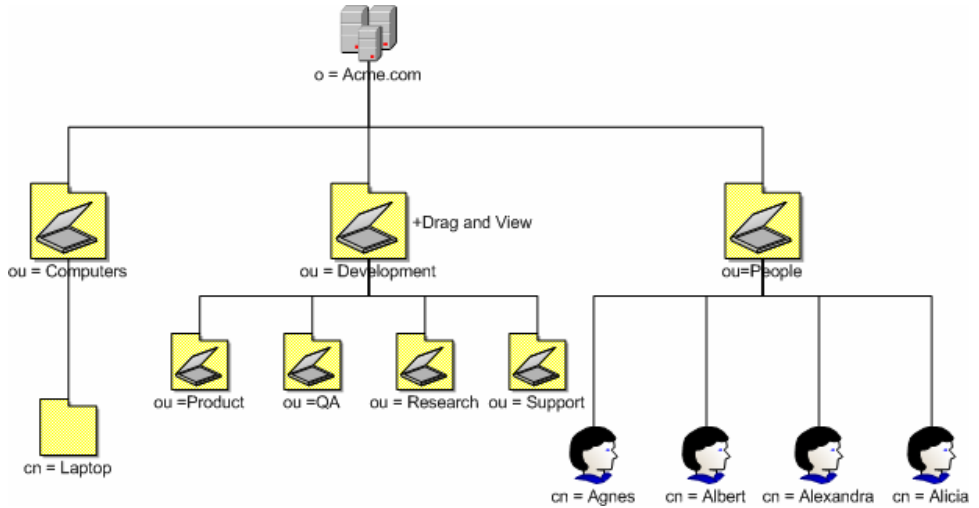
| Policy | Args | Object |
|----------------------|------|---|
| software/stratus_pad | | ou=research, ou=development, o=acme.com |
| ms office | | o=acme.com |

The user has been successfully linked to an additional organizational unit.

Policy Scope

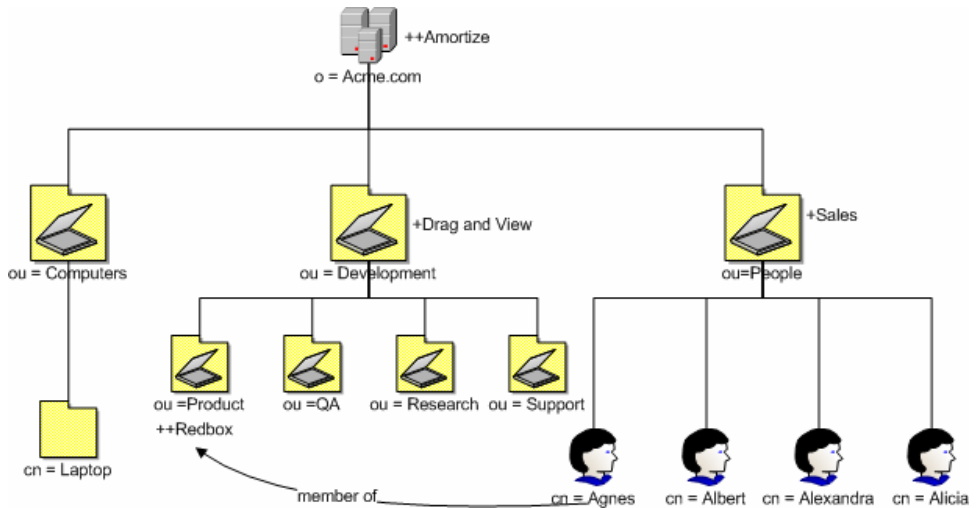
By default, a subscriber inherits the policy from the parent of any groups it is linked to. This link can be through either the subscriber's directory service membership or through the use of the edmlink attribute. Figure 3 on page 46 shows a part of the Acme organization. It has three organizational 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.

Figure 3 Acme organization directory structure



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

Figure 4 Agnes is a member of Product organizational unit

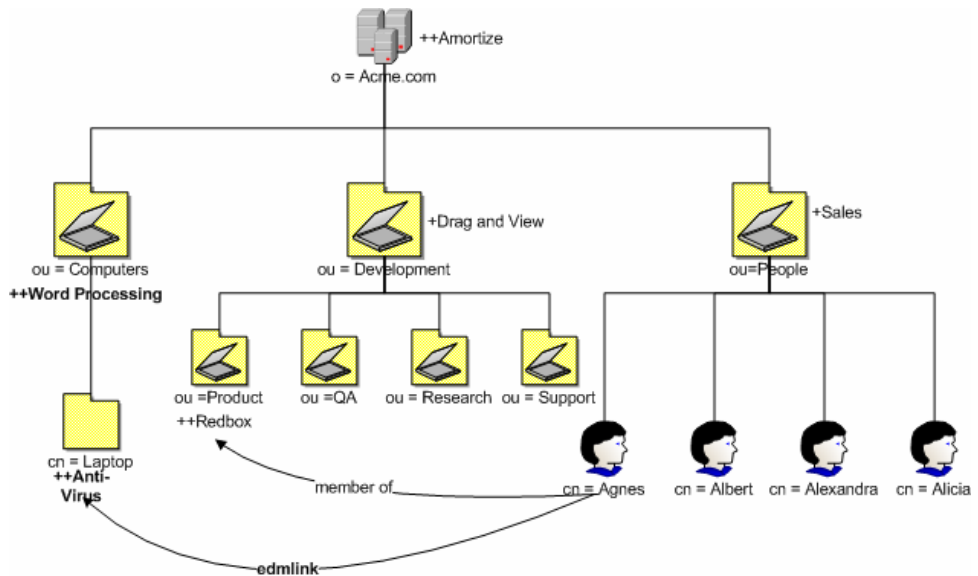


If Agnes is a member of the Product organizational unit, she will also inherit the policy from that unit and the Development organizational unit. In Figure 4 above, Agnes would get Sales and Amortize because she is a part of the

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. See the procedure [To add a link](#) on page 43 for more information.

Figure 5 Agnes is linked to the laptop container



In Figure 5, 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 CM 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 CM 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 CM 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 CM 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 CM Policy Server interface, you will see only these attributes for that object. If you do not want CM 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 CM 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 5 on page 47 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 { }
}
```

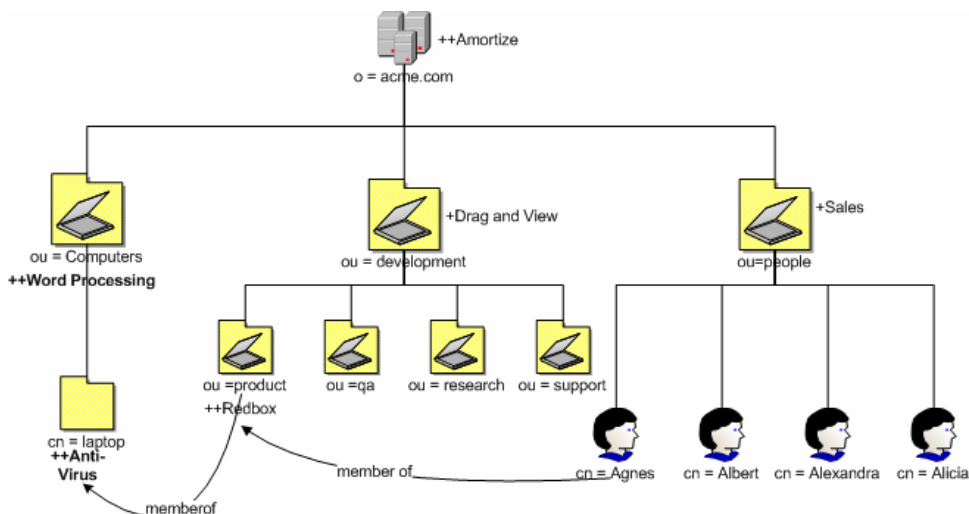
This configuration with the empty brackets tells CM Policy Server to follow memberof, but not to inherit from any parents from that branch of the directory tree or any links contained within the object.

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 CM 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 the figure 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 6 Product is a member of the laptop container



Controlling Policy Scope Locally (edmFlags)


You may want to limit the scope of policy resolution for only specific objects. To do this, use the `edmFlags` attribute. `Edmflags` is an optional, single-value integer attribute, and can contain any of the values shown in [Table 6](#) on page 51 with a logical OR. Use these flags very sparingly, as they can have a profound impact on the clarity and function of the policy model.

In the example below, we will prevent Albert Kirkman from traversing up the directory tree to resolve his policy.

To use `edmFlags`

- 1 Open your Internet browser to the CM Policy Server page.
- 2 Click **Browse**.
- 3 Click on an organizational unit in the bottom section of the policy management screen to select it or continue to select until you reach a particular user. In the next figure we selected **albert kirkman** from the people organizational unit in `acme.com`.

[Policy > LDAP >](#) [Browse](#) | [Config](#) | [Query](#) | [Refresh](#) | [Status](#) | [Setup](#) | [Test](#) [←](#) [↑](#) [i](#) [more information](#)

|  | Resolve Policy: <code>cn=albert kirkman, ou=people, o=acme.com</code> description: Albert Kirkman Show Children: Yes Verbose: No | |
|---|---|----------------------|
| <input type="button" value="Filter"/> | <input type="text"/> | |
| <input type="button" value="Goto"/> | <input type="text"/> | |
| Action | Attribute | Value |
| <input type="button" value="Add"/> | <input type="text" value="edmFlags"/> | <input type="text"/> |
| | cn : | Albert Kirkman |

- 4 Make sure that `edmFlags` is selected in the drop-down box for **Attribute**.
- 5 Using [Table 6](#) on page 51, type the number that corresponds to the control that you want to exert over Albert Kirkman's policy.

Table 6 edmFlags Values

| Value (Value Name) | Description |
|-------------------------------|--|
| 1 (NVD_SECEDE) | Use NVD_SECEDE to instruct the CM Policy Server not to include any parent objects traversing up the object's branch of the directory tree. Its primary use is to support semi-autonomous units within an organization. For example, if your organizational unit is a member of a larger organization, and you do not want to resolve your policy above your organizational unit, use NVD_SECEDE. Set edmFlags to 1 for your organization unit. |
| 2 (NVD_CONTINUE) | Use NVD_CONTINUE to ignore all of this object's attributes, and continue up the directory tree instead. The parent object is still processed, unless NVD_SECEDE is set. Set edmFlags to 2. |
| 4 (NVD_BREAK) | Use NVD_BREAK to abort the policy resolution and return the condition to the client. In this situation, the client device <i>should not</i> apply policy. It can be used to implement "change control freezes", to prevent policy changes being applied to certain parts of an organization. Set edmFlags to 4. |
| 8 (NVD_STRICT) | Use NVD_STRICT to ignore memberOf attributes, and only process edmFlags, edmPolicy, and edmLink. Set edmFlags to 8. |

- 6 In this example, we want to only resolve the policy for Albert Kirkman and none of his parent objects. Therefore, we will type 1 in the Value entry box.

| | | Resolve Policy: cn=albert kirkman,ou=people,o=acme.com description: Albert Kirkman Show Children: Yes Verbose: No | |
|------------------------------------|-----------|--|----------------------|
| | | <input type="button" value="Filter"/> | <input type="text"/> |
| | | <input type="button" value="Goto"/> | <input type="text"/> |
| Action | Attribute | Value | |
| <input type="button" value="Add"/> | edmFlags | <input type="text"/> | <input type="text"/> |
| | cn : | Albert Kirkman | |

- Click **Add** to add the flag. The object has been modified and edmFlags is added to the list of attributes for Albert Kirkman.

Verify that the object is only resolving the policy for itself and none of its parents' policies by clicking **Resolve Policy**.

Log Files

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

Summary

- Configure the CM Policy Server to connect to your directory services.
- Configure your CM Configuration Server to use the LDAP method.
- Connect any users that you want to use CM Policy Server for entitlements to the LDAP method.
- Add your policy to the CM Policy Server Web interface using your Internet browser.
- You can control the scope of policy resolution globally using the VIEW option in the CM Policy Server configuration file.

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 OpenView Configuration Management Policy Server (CM 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 CM 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.

CM Policy Server and LDAP

The LDAP Policy Extension, in conjunction with the CM 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.

CM Policy Server aimed at customers who have a detailed understanding of LDAP/X.500 directories, and an established directory infrastructure. The CM 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 CM 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 Configuration Management infrastructure to provide a comprehensive and sophisticated software management solution.

The extension makes policy resolution available via a URL utilizing the standard CM Policy Server policy framework. It maintains a persistent LDAP connection to your corporate directory, and provides online HTML documentation and 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 CM 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:

- `<prefix>Flags`
controls various subtle aspects of the policy resolution. See [Controlling Policy Scope Locally \(edmFlags\)](#) on page 50.
- `<prefix>Link`
allows you to specify additional, potentially dynamic or conditional relationships. See [Controlling Policy Scope Locally \(edmFlags\)](#) on page 50.
- `<prefix>Policy`
allows you to define resultant strings that will be netted out during policy resolution. See [Adding a Policy \(EdmPolicy\)](#) on page 36.

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 CM 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 CM 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 Configuration Management.
- **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 7, below.

Table 7 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 8 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 9 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 10 LDAP Extension URL Namespace

| URL | Description |
|------------------------------------|--|
| /policy/ldap?<x-url encoded query> | <p>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:</p> <ul style="list-style-type: none">• 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 CM 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> | <p>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.</p> <p>Pre-requisite: Uncomment this line in the <code>httpd.rc</code> file: <pre>#Admin_Url /admin</pre> and restart the service for the CM Integration Server.</p> <p>Syntax Example: To flush the cache of the dn: <pre>dc=test,dc=com</pre> encode the <dn> value by replacing the equal signs (=) with <code>%3d</code>, and the comma (,) with <code>%2c</code>: The resulting URL to flush the cache of this dn is: <code>/admin/ldap/flush?dn=dc%3dtest%2cdc%3dcom</code></p> |
| /admin/ldap/reset | <p>Reset connection to directory (forces a flush and reconnect).</p> <p>Pre-requisite: Uncomment this line in the <code>httpd.rc</code> file: <pre>#Admin_Url /admin</pre> and restart the service for the CM Integration Server.</p> |
| /ldap/config.tsp | <p>Summary configuration page, and interactive controls for resetting cache and connection.</p> |
| /ldap/browse.tsp?dn=<dn> | <p>Directory Browser and Policy Editor.</p> |
| /ldap/query.tsp?dn=<dn> | <p>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.</p> |
| /ldap/test.tsp?dn=<dn> | <p>This URL can be used to test connections to arbitrary directory servers, and is useful when diagnosing problems with authentication and directory access.</p> |

B Use Existing LDAP Attributes

The goal of this feature is to allow Configuration Management customers to implement the CM 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 Configuration Management Policy Attributes](#) on page 22 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 Configuration Management Policy Attributes on page 22](#)

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 CM 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 CM Policy Server to create entitlements in your enterprise, you can filter out which domains the CM Policy Server will assign services from based on connect parameters.

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

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

Where the `DOMAIN NAME` is the value passed in `dname` by `RADISH`. In the case of a CM 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 minimum version requirement for CM Policy Server is version 3.2.1.

The default configuration for these filters is shown in below:

```
DNAME=*                { * !PATCHMGR !OS }
DNAME=PATCH           { PATCHMGR }
DNAME=OS               { OS }
```

In this configuration the default rule (*) will ignore `PATCHMGR` and `OS` domains and allow everything else as denoted by the use of an exclamation point (!). `PATCH` and `OS` rules allow only policies for `PATCH` and `OS` domains respectively. If for instance, we wanted to allow any policies for `OS` manager resolution we would change the last filter to: `DNAME=OS { * }`.

D Product Name Changes

If you have used Radia in the past, and are not yet familiar with the newly rebranded HP terms and product names, Table 11 below will help you identify naming changes that have been applied to the Radia brand.

Table 11 Product Name and Term Changes

| New Name/Term | Old Name/Term |
|---|---|
| HP OpenView Configuration Administrator | Radia Administrator Workstation |
| HP OpenView Configuration Management | Radia |
| HP OpenView Configuration Management Admin CSDB Editor | Radia System Explorer |
| HP OpenView Configuration Management Application Manager | Radia Application Manager |
| HP OpenView Configuration Management Application Self-service Manager | Radia Software Manager |
| HP OpenView Configuration Management Configuration Server | Radia Configuration Server |
| HP OpenView Configuration Management Configuration Server Database | Configuration Server Database, Radia Database |
| HP OpenView Configuration Management Integration Server | Radia Integration Server |
| HP OpenView Configuration Management Patch Manager | Radia Patch Manager |
| HP OpenView Configuration Management Policy Server | Radia Policy Server |
| HP OpenView Configuration Management Proxy Server | Radia Proxy Server |

Index

\$

\$myVar, 58

<

<<in.nameOfAttr>>, 57

<<myAttribute>>, 58

<<nameOfAttr>, 57

<pfx>Flags, 56

<pfx>Link, 56

<pfx>Policy, 56

A

Add Variable to Object dialog box, 32

adding a link, 43

adding a policy, 36

authentication, 61

B

Bind Pw field, 26

C

Change Variable dialog box, 32

CM Policy Server

 configuring for LDAP, 24

 description, 10

 log file, 60

copyright notices, 2

current object attributes, 57

customer support, 5

D

debug attribute, 60

directory access, 61

Directory Browser, 61

distinguished name, 32, 60

distributed administration, 35

dn. *See* distinguished name

document changes, 4

documentation updates, 4

E

Editing Instance dialog box, 33

edmFlags, 50

 properties, 22

edmLink, 44, 50

 properties, 22

edmLink attribute, 43

edmPolicy, 37, 51

 properties, 23

edmPolicy field, 40

edmprof.dat, 27

EMBED configuration option, 63

enabling distributed administration, 35

H

httpd.rc file, 35

I

inbound object attributes, 57

installation, 17

L

LDAP directory, 55

LDAP extension, 24

- LDAP method
 - connecting the user, 33
 - creating in Configuration Server Database, 28

- LDAP policy attributes, 22

- LDAP Policy Extension, 55

- LDAP, multiple connections, 27

- legal notices

- copyright, 2
 - restricted rights, 2
 - warranty, 2

- link, adding, 43

- LINKS configuration option, 48

- log files, 52

M

- memberOf relationships, 57

- MGR_POLICY section of edmpref, 27

N

- nvdObject class, 23

O

- object attributes, 57

- object relationships, 57

P

- passport registration, 5

- phase attribute, 60

- pm.cfg, 24, 27

- pm.cfg file, 35

- policy

- adding, 36
 - removing, 39
 - scope, 45
 - controlling, 47

- Policy Adapter, description, 10

- Policy Editor, 61

- policy resolution, stages, 60

- Policy Resolver, 61

- prefix attribute, 60

- profile file, 27

R

- RCS_CACHE_HOST, 28

- RCS_CACHE_PORT, 28

- Relationships tab, 23

- removing a policy, 39

- Resolve Policy, 45

- restricted rights legend, 2

S

- support, 5

U

- updates to doc, 4

- URL namespace, 59

- Utility Method text box, 33

V

- VIEW option, 48

W

- warranty, 2

Z

- ZMASTER object, 32

- ZMTHNAME attribute, 29

- ZMTHPRMS attribute, 30

- ZMTHTYPE attribute, 29