HP WBEM Services for HP-UX System Administrator Guide

HP Part Number: 5900-2999
Published: March 2013

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304
U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Copyright Notices. © copyright 2002, 2003 Hewlett-Packard Company, all rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

© copyright 1979, 1980, 1983, 1985-93 Regents of the University of California.

This software is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

©copyright 1980, 1984, 1986 Novell, Inc.
©copyright 1986-1992 Sun Microsystems, Inc.
©copyright 1985-86, 1988 Massachusetts Institute of Technology.
©copyright 1989-93 The Open Software Foundation, Inc.
©copyright 1986 Digital Equipment Corporation.
©copyright 1990 Motorola, Inc.
©copyright 1990, 1991, 1992 Cornell University
©copyright 1989-1991 The University of Maryland
©copyright 1988 Carnegie Mellon University

Intel and Itanium are trademarks of Intel Corporation in the U.S. and other countries.

This product includes software developed by The Open Group OpenPegasus Project (`http://www.opengroup.org/pegasus`). The Open Group Open Pegasus Project Copyright (c) 2000, 2001, 2002, 2003 BMC Software, Hewlett-Packard Development Company L.P., IBM, The Open Group, Tivoli Systems.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (`http://www.openssl.org`). OpenSSL Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). This package is an SSL implementation written by Eric Young (eay@cryptsoft.com), written so as to conform with Netscape's SSL. Original SSLeay License: Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

Contents

1 Introduction to HP WBEM Services

This chapter describes HP WBEM Services, the architecture, and how it functions with other products.

HP WBEM Services is an implementation of the DMTF-WBEM standard on HP-UX systems. HP WBEM Services enables management solutions to deliver increased control of enterprise resources at reduced cost. WBEM is a platform and resource-independent DMTF standard that defines a common information model and a communication protocol to monitor and control resources from various sources.

HP WBEM Services can operate on both the homogeneous and heterogeneous IT environments. It supports multi-platform and multi-operating system management tools. HP WBEM Services leverages the existing training and knowledge base of current IT staff, while preparing for different environments in the IT plan. In homogeneous environments, WBEM optimizes the management information and capabilities, using a standard method, regardless of the architecture or platform specifications, for example, PA-RISC and IPF systems.

HP WBEM Services includes a set of providers that enable management applications to access information about managed resources in the operating environment. These applications include HP Systems Insight Manager (HP SIM) or HP System Management Homepage (HP SMH). For developers, HP WBEM Services facilitates the creation of management applications for HP-UX systems. As a result, developers can optimally manage HP Servers and workstations.

HP WBEM Services functions as a mediator between providers and clients. Information is stored and exchanged, using the WBEM standards developed by Distributed Management Task Force, Inc.

HP WBEM Services is based on The Open Group's Pegasus Open Source Software (OSS) project. For more information about Pegasus Open Source Software, see https://collaboration.opengroup.org/pegasus/.

HP WBEM Services and common standards

HP WBEM Services is based on the following standards:

- "Common Information Model" (page 5)
- "CIM in Extensible Markup Language" (page 6)
- "CIM operations over HTTP" (page 6)

Common Information Model

The Common Information Model (CIM) specification is a language and a methodology for describing management data. CIM is a conceptual object-oriented information model that describes managed resources. CIM is not constrained to a particular implementation. The CIM specification includes the following:

- CIM Object — A representation of managed resource. 3
- CIM Class — CIM objects that have similar properties and purposes. The definitions of CIM classes are grouped into meaningful collections called schemas.
- CIM Instance — A representation of managed object that belongs to a particular class. These objects can be shared by any WBEM-enabled system or application.

Managed Object Format (MOF) is the language used to define CIM classes and instances. MOF files are ASCII files that use the MOF language to describe the CIM objects.

Using the CIM specification, HP WBEM Services accepts requests for information from any platform in a heterogeneous IT environment. HP WBEM Services collects and maintains information about managed resources in the HP WBEM Services repository, which also adheres to CIM.

For more information on CIM, see the *CIM Specification Version 2.2* available at:

http://www.dmtf.org/standards/cim.

For an overview of the data representation, see Appendix A (page 52).

CIM in Extensible Markup Language

The markup language for describing data on the web is Extensible Markup Language (XML). DMTF defines a standard for representing the CIM elements and messages in XML, referred to as CIM-XML. Since CIM-XML provides a standard way of describing data, any WBEM client can access CIM data on any WBEM-enabled system. Requests are received from clients by HP WBEM Services as CIM functions encoded in XML, which in turn, send responses to clients in CIM-XML.

For an overview of XML, see http://www.w3.org/XML.

For more information on CIM-XML, see DMTF Representation of CIM in XML available at:

http://www.dmtf.org/standards/published_documents.

CIM operations over HTTP

This section describes a mapping of CIM operations onto HTTP that enable implementations of CIM to inter-operate in an open and standardized manner.

For more information about the HTTP server in HP WBEM Services, ports reserved for HP WBEM Services, and other transport-related information, see Chapter 3 (page 33).

For more information on DMTF WBEM standards, see http://www.dmtf.org.

HP WBEM Services architecture

A typical IT environment consists of numerous servers and network resources and is rarely homogenous. To manage this diverse environment, a host of management applications must be available, such as HP Systems Insight Manager (HP SIM) or HP System Management Homepage (HP SMH).

These management applications informs you about the health of your network and potential issues. To gather information about any device in the network or information on any system, management applications depend on HP WBEM Services.

HP WBEM Services can be considered as an information gateway. In any system, a number of providers run. These providers are registered with HP WBEM Services.

When a management client sends a request, HP WBEM Services routes this request to the respective provider. For example, if the request is for information on an operating system, HP WBEM Services routes this request to the OS Provider (`PG_OperatingSystemProvider`). This provider gathers information on the managed resource, in this case the operating system, and routes it back to HP WBEM Services, which in turn, routes it back to the management client.

This is generally how HP WBEM Services functions in an IT environment. However, to process client requests in a network, HP WBEM Services depends on the following components:

- **CIM Server**

  The CIM Server receives requests from management clients. It then interacts with the respective providers to receive information that is requested by the management clients. The CIM Server receives information from the providers and sends it back to the management clients.

- **CIM repository**

  The CIM repository maintains the data definitions of all the managed objects and the providers. When a valid request for information is received, HP WBEM Services accesses the repository and then looks up the managed resource. The resource owners register the providers with HP WBEM Services. With this registration, managed resources inform HP WBEM Services of the nature of information that their providers can give and how HP WBEM Services can invoke the appropriate providers that are accessible as shared libraries.

The CIM repository can be modified, using CIM operations, which are provided through an XML file. Information can be entered in the repository either as MOF files using the `cimmof` command or as XML files using the `wbemexec` command. You can use the `wbemexec` command to execute CIM operations, such as create class or create instance, in the XML file.

For more information on maintaining the repository, see "Maintaining the repository" (page 31).

- **MOF compiler**

  The MOF compiler reads all the MOF files and loads the information in the CIM repository. An MOF file is a text representation of CIM classes.

  MOF standards are defined by the DMTF, and are explained in the tutorial section of CIM Managed Object Format at http://www.dmtf.org/education/mof.

- **HTTPS server**

  HP WBEM Services includes an embedded HTTPS server, which handles communication between the HP WBEM Services and the clients. This HTTPS server is not a web server. It receives only valid CIM messages and rejects any other HTTP request.

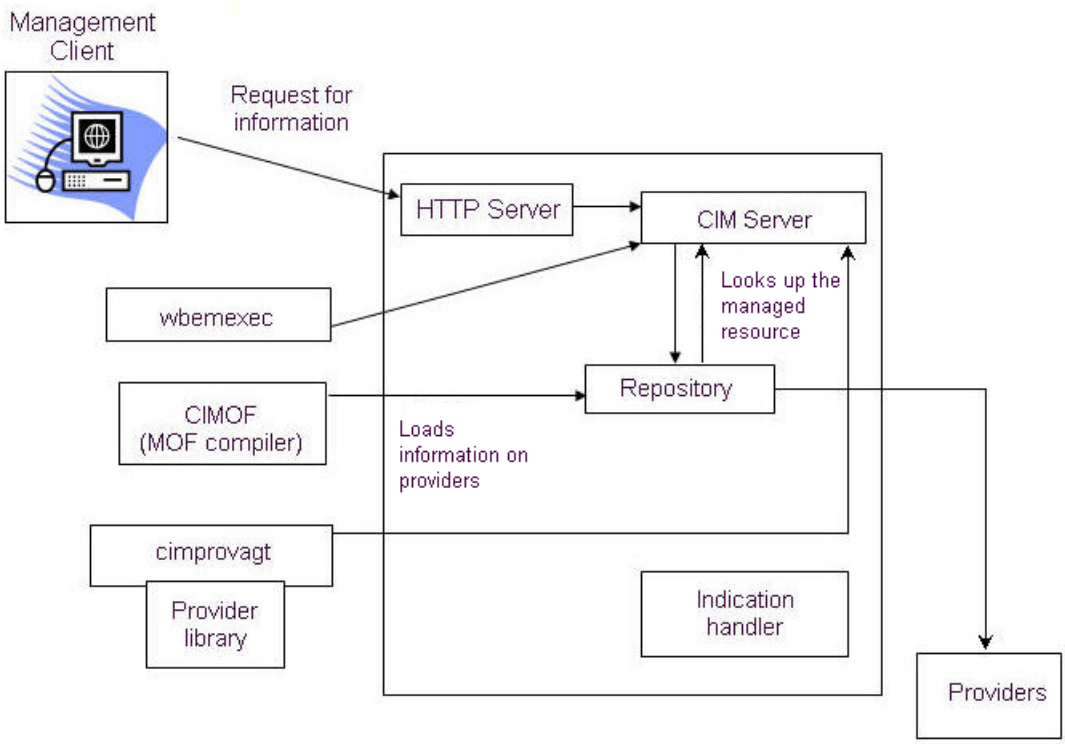
  For more information on the HTTPS server and how it operates, see "How HP WBEM Services works?" (page 8)

- **Provider agent**

  When CIM Server receives a request for information, it creates a process or a provider agent. This agent or process, loads the respective provider library. If an existing provider agent is running, in the same user context as the new request, the existing provider agent is used.

Figure 1 is a representation of the HP WBEM Services components and how they interact when a valid client request is received.

Figure 1 HP WBEM Services Components



How HP WBEM Services works?

This section describes how HP WBEM Services processes requests received from management clients, and collaborates with respective providers to send information back to these management clients.

In general, HP WBEM Services can receive requests from clients running on different kind of systems and platforms, as long as the requests conform to the DMTF CIM-XML standard. HP WBEM Services processes these client requests and passes them to the appropriate providers. When providers receive these requests, they gather the requested information and send it back to HP WBEM Services. The information is sent back to the client by HP WBEM Services.

NOTE: When HP WBEM Services receives information from several registered providers, only one response is sent to the management client.

Client requests

In a network, any client can send valid requests to HP WBEM Services. Any client request received by HP WBEM Services must include the following:

- A well-formatted HTTP header

  The remote request must be addressed to the HTTP server of HP WBEM Services either on the `wbem-http` port or the `wbem-https` port. All requests must be written in CIM-XML format.

  For information about CIM-XML, see *Representation of CIM in XML* at http://www.dmtf.org/standards/WBEM.

- Information required and respective parameters

  The request must clearly specify the required information along with the corresponding parameters.

  For example, for a `GetClass` operation, a class name is required. Similarly, a request for OS information uses the `EnumerateInstances` operation, and the only requirement is the class name.

- Namespace

  Every client request must include the respective namespace.

  For example, the request for OS information specifies the `PG_OperatingSystem` class in the `root/cimv2` namespace.

A management client can use CIM operations, such as the `EnumerateInstances` operation. If you are developing your own classes to gather resource information, you can use the standard CIM operations, such as the `GetClass` and `GetProperty`.

Providers

HP WBEM Services includes some default providers that are installed when HP WBEM Services is installed. Following providers are available with HP WBEM Services for HP-UX systems:

- "Computer System Provider"
- "Operating System Provider"
- "Process Provider"
- "Domain Name System Provider "
- "Network Time Protocol Provider"
- "Network Information Service Provider"
- "IP Provider "

- "Software Distributor Provider"
- "IOTree Provider"

For more information on these providers, see "Providers available with HP WBEM Services" (page 21).

When a provider is installed in the network, it automatically registers with HP WBEM Services, using the MOF compiler. Information on the provider is stored in the CIM repository. When a provider registers with HP WBEM Services, the following information is provided:

- Definition of the resource

  Resources are largely defined by the characteristics inherited from the most general classes and passed to the more specific subclasses.

  For example, consider a schema named `Creature`. This schema includes a class named `Human`, which includes all Homo sapiens. The class `Human` can include subclasses based on the gender — `Female` and `Male` subclasses. Each of these subclasses can have additional subclasses based on relationships. For example, the `Female` subclass can include additional subclasses such as `My Mother`, `My Sister`, or `My Daughter`.

  Resources can also be grouped as namespaces. HP WBEM Services includes four namespaces, which are enabled when HP WBEM Services is installed.

- Information on the resource that the provider can expose

  This information is categorized into Properties and Methods such as using the example of the `My Mother` class, one Property is the `Birth Date`, or the `Social Security Number`.

- A shared library to invoke actions that are offered to manage the resource

  For example, you can have a method `callMother` that reminds the user of the Phone Number when a `Birth Date` approaches.

- Information about the provider

  Provides information such as version, the type of provider, a description including how it can be invoked, and the name of its shared libraries.

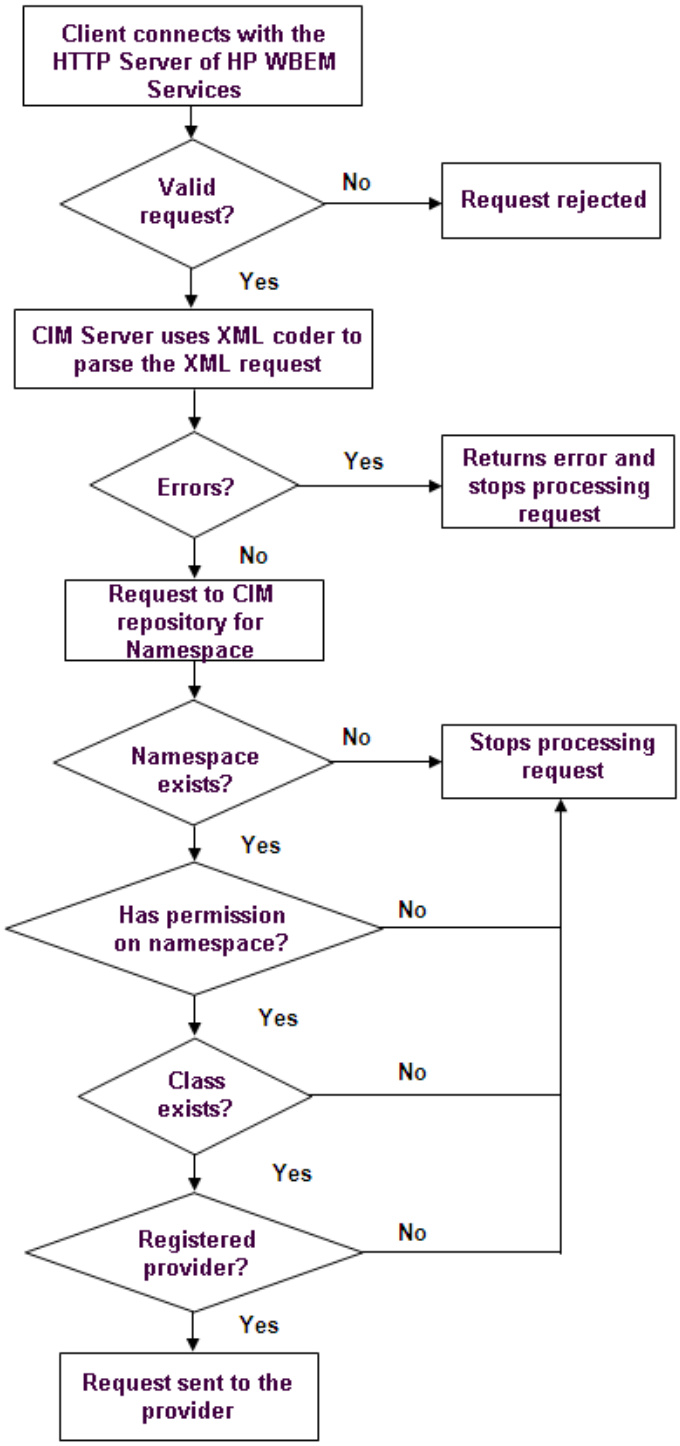
Providers are automatically enabled when they are registered with HP WBEM Services. If you want to disable a provider, use the `cimprovider` command. After a provider is disabled, you can enable it only by using the `cimprovider` command. You can also use this command to remove a provider registration from the CIM repository. However, removing a provider registration from the CIM repository does not remove the provider from the system.

IMPORTANT: In addition to these providers, you can develop your own set of providers. However, you must register these providers with HP WBEM Services. After the provider is registered with HP WBEM Services, you can replace it with a new version to add, remove, or modify information of a resource. This information includes new classes, properties, and methods.

Processing requests

When a management client sends a request to HP WBEM Services, it initiates a series of actions among the components of HP WBEM Services. Figure 2 is a representation of how the components in HP WBEM Services work together when a client request is received.

Figure 2 HP WBEM Services Processing Requests



Any client request that is sent as an HTTP request to HP WBEM Services is a CIM operation. The request is encoded in CIM-XML. The HTTP server of HP WBEM Services listens for the CIM messages on the `wbem-http` or `wbem-https` port. The following sequence of events occur when a client request is received by the HTTP server:

1. The client connects with the HTTP server.

   Any remote client, when sending a request, also sends a valid system login name and password information to a system with HP WBEM Services that has the appropriate provider installed. For information about login permissions, see Chapter 3 (page 33).

2. The CIM Server in HP WBEM Services uses its XML decoder to parse the XML data in the request.

   If an error occurs, the CIM Server returns an error message and stops processing the request. The CIM Server accepts only valid CIM operations.

3. If a request is valid, the CIM Server connects with the CIM repository to validate the following information:

   a. Does the namespace exist?

   If the request does not include a namespace, an error is reported and HP WBEM Services does not process the request. Every request must include a valid namespace that is registered in the CIM repository.

   For example, a request for OS information can include the following namespace:

   ```
   <LOCALNAMESPACEPATH>
   <NAMESPACE NAME ="root"/>
   <NAMESPACE NAME ="cimv2"/>
   </LOCALNAMESPACEPATH>
   ```

   b. Does the user have permission in this namespace?

   If the HP WBEM Services property `enableNamespaceAuthorization` is set to `true`, HP WBEM Services ensures the user is allowed to access this namespace.

   c. Does the class exist?

   HP WBEM Services looks up the class name given in the request.

   For example, for a request on OS information, HP WBEM Services checks for the following:

   ```
   <IPARAMVALUE NAME="ClassName">
   <CLASSNAME NAME="PG_OperatingSystem"/>
   </IPARAMVALUE>
   ```

   d. Does the resource have a registered provider?

   If no provider is registered for this resource, HP WBEM Services returns an error to the client.

   For example, the provider for the `osinfo` client request is the Operating System Provider.

4. HP WBEM Services determines, from the provider registration, how to access the appropriate shared library for the provider.

   HP WBEM Services uses this information to invoke the appropriate method, and informs the provider which user has sent the request. After receiving the request, the developers of the provider can provide any additional user authorization that is required for performing the action, and for returning a response to HP WBEM Services.

5. The CIM Server of HP WBEM Services receives the response from the provider and conveys the response to the client.

   Each client request receives only one response, even if CIM Server receives information from more than one provider.

   For example, a client might request HP WBEM Services for a list of all printers available with a particular system. Several providers in the network might respond — one for each type of printer. HP WBEM Services waits till all the providers respond and then combines all the information from all the providers into one response and sends it to the client.

   If no provider can be reached or no provider responds with the required information, HP WBEM Services sends the following error to the client:

`CIM_ERR_NOT_SUPPORTED`

For a list of standard CIM errors and other error messages, see Chapter 5 (page 42).

HP WBEM indications

In a network where several clients and resources are managed, certain events might occur. These events, irrespective of nature or criticality, must be reported so that appropriate action is taken.

In this network, you can receive a notification from HP WBEM Services when an **event** occurs. For example, if you want to know about errors in a disk write operation, it can be configured as an event. Other examples include authentication attempts that fail, or even mouse clicks.

When events occur in your environment, HP WBEM Services reports the event as an **indication**. Therefore, an indication is the representation of the occurrence of an event.

The abstract class `CIM_Indication` serves as the base class for all the `Indication` classes in HP WBEM Services. A CIM Indication Provider registers with the CIM Server to generate indications of one or more classes.

A CIM Indication Provider translates the detection of an event into a CIM Indication and sends the indication to the CIM Object Manager for further processing and delivery.

Any indication from HP WBEM Services includes the following components:

- "Indication Subscription" (page 12)
- "Indication Processing" (page 12)
- "Indication Delivery" (page 12)
- "Indication Consumption" (page 13)

Indication Subscription

An Indication Subscriber is a CIM client that issues the CIM operation requests to create instances of the `CIM_IndicationSubscription` class.

An Indication Subscription consists of an Instance, a Filter, and a Handler. The Instance is the Subscription; the Filter determines the Indications that must be sent; and the Handler specifies where these indications are to be sent and using which protocol.

The CIM Indication Service coordinates the handling of subscriptions among the Indication Providers. The CIM Server receives and processes CIM operation requests and issues the CIM operation responses. The CIM Indication Service is a component of the CIM Object Manager and is responsible for processing CIM operations on the classes in the CIM Subscription schema.

Indication Processing

The CIM Indication Service is a component of the CIM Object Manager. It processes each generated indication to determine which indication handlers, if any, the indication must be sent to.

Indication Delivery

A CIM Indication Handler receives indications, and then performs a mapping between the internal representation of a CIM Indication and the desired format and protocol. After the mapping is complete, the CIM Indication Handler sends the indication to the designated destination. The CIM Server supports multiple indication handler interfaces.

A CIM-XML Indication Handler, functioning as a CIM Client, uses the DMTF CIM-XML protocol to send an indication to each specified destination.

Indication Listener

When the CIM Server acts as a CIM listener, the CIM Server functions as an HTTP server to receive indications as CIM Export Messages.

A CIM message is a well-defined request or response data packet used to exchange information between the CIM applications. Following are the types of CIM messages:

- CIM Operation Messages

  A CIM Operation Message is used to invoke an operation on the target CIM namespace.

- CIM Export Messages

  A CIM Export Message is used to communicate information about a CIM namespace or element that is foreign to the target. A CIM Export Message is informational only and does not define an operation on the target CIM namespace or even imply the existence of a target namespace.

A CIM listener receives CIM Export requests, such as indications, and coordinates the distribution of requests among one or more consumers, and then sends the CIM export messages.

NOTE: For standalone CIM listeners, the listener waits at an application-specific port to receive the CIM export messages.

Indication Consumption

A CIM Indication Consumer "consumes" the CIM encapsulated in a CIM export message. For example, a Consumer might store an indication in an event database for further processing. An Indication Consumer registers with the CIM listener to receive indications.

For more information on troubleshooting WBEM Indications, see Chapter 5 (page 42).

HP WBEM Services executable scripts

This section elaborates the commands, executable scripts, and daemon processes that are available with HP WBEM Services.

Table 1 lists the commands, executable scripts, and daemon processes that are available with HP WBEM Services for HP-UX. The table also indicates the version that the executable scripts are available with, along with the permissions required to use them.

Table 1 Commands, Executable Scripts, and Daemon Processes in HP WBEM Services

Name	Type	Version	Required Permission	To Perform
`cimauth`	Command	A.02.07	`root`	Authorizes users for a specified namespace. Use this command to add, modify, or remove authorization per user, per namespace. You can also assign `Read` or `Write` permissions. Note that assigning `Write` permission does not automatically include `Read` permission. Use this command to list all authorizations that are configured on the CIM Server. This command can be used only if the property `enableNamespaceAuthorization` is set to `true`. To set this property to true, use the `cimconfig` command. To use this command, the CIM Server must be running. For more information, see *cimauth (1M)*.
`cimconfig`	Command	A.02.07	`root`	To set, clear, or view the properties of the CIM Server. With this command, an operation using the “current” option changes the value immediately. However, an operation using the “planned”

Table 1 Commands, Executable Scripts, and Daemon Processes in HP WBEM Services *(continued)*

Name	Type	Version	Required Permission	To Perform
				option takes effect the next time the CIM Server is started. When using the current values, the CIM Server must be running. When using planned values, the CIM Server can be running or not. For more information, see *cimconfig(1M)*.
`cimmof`	Command	A.02.07	`root`	Used by HP WBEM Services to compile `.mof` files and to load the information in the repository. MOF files can be used for resource and provider information. MOF files must follow the DMTF standard format. The `cimmof` manpage includes rules for specifying locations where the files are loaded. Schemas can only be loaded as local root, regardless of any authorizations specified through `cimauth`. If namespace authorization is enabled, user must also have Write authorization in the namespace. You can use the `cimmof` command only when the CIM Server is running. For more information on using this command, see *cimmof(1M)*.
`cimprovider`	Command	A.02.07	The list option can be executed by any user. You must have local `root` permission to use the other options.	To list (with status), disable, enable, or remove registered CIM providers or CIM provider modules. For more information, see *cimprovider(1M)*.
`cimprovagt`	Command	A.02.07	No user interface	A wrapper process that is used by the `cimserver` to load the shared libraries of individual providers as separate processes distinct from the CIM Server and other providers. This process provides protection for the `cimserver` in the event of a failure that occurs with a provider as only that specific provider is affected.
`cimserver`	Command	A.02.07	root	To start or gracefully stop HP WBEM Services. Use the `-v` option to view the version number of the CIM Server. Use the `-h` option for help with command syntax.
`cimservera`	Daemon	A.02.07	No user interface	This daemon is a standalone process that provides the CIM Server with PAM Authentication services. This daemon is controlled solely by the CIM Server and has no user interface.
`cimserverd`	Daemon	A.02.07	Cannot be used by users.	This daemon is used by HP WBEM Services to automatically restart in case of a failure. This daemon is not intended to be used by operators.

Table 1 Commands, Executable Scripts, and Daemon Processes in HP WBEM Services *(continued)*

Name	Type	Version	Required Permission	To Perform
				However, you can set the interval for this daemon. Normally, the CIM Server is started and halted using the `cimserver` command. If you halt the CIM Server using the `cimserver` command, the daemon does not automatically restart it in the event of a failure. For more information on using this command, see *cimserverd(1M)*.
`cimservermain`	Process	A.02.07	Yes	This process is the main executable for the WBEM server. This process can only be used with the `cimserver` command. The `cimserver` executable runs as the `root` user to perform privileged operations for the WBEM Server. The `cimservermain` runs as `cimsrvr` user to perform all WBEM Server functions that do not require privileged access.
`cimtrust`	Command	A.02.07	Yes	The `cimtrust` command is used to add, remove or list X509 certificates in the PEM format in the WBEM Server trust store. If the HTTPS connection and client verification is enabled on the WBEM Server, clients must use this command to add their certificates to the WBEM Server trust store.
`cimsub`	Command	A.02.09.06	any user	The `cimsub` command provides a command line interface to manage the CIM indication subscriptions on the local CIM Server.
`gen_wbem_certs`	Script	A.02.07.02	Yes	This script is used to generate WBEM certificates. This script must be used to generate certificates only when the existing certificates get corrupted. From version A.02.09 onwards, this script can also be used to verify existing WBEM certificates.
`init_repository`	Script	A.02.07	`root`	Initializes the repository. If the repository is moved or corrupted, you must first attempt to restore it from backup. If you cannot restore the repository from the backup, use the `init_repository` script to restore the repository to the state it was in, when HP WBEM Services was installed. You will lose all provider data that was loaded in the repository after the initial installation. You must re-install any providers that you had added. Use this command only when the CIM Server is running.
`osinfo`	Command	A.02.07	any user	Runs as a HP WBEM Services client that gathers information about the operating system where the command is issued. The command uses the Operating System Provider, which is bundled with HP WBEM Services for HP-UX. The response lists some properties of the class, including the hostname, operating system type, version, user license, OS capability (32- or 64-bit), last boot time, local date time, and system uptime.

Table 1 Commands, Executable Scripts, and Daemon Processes in HP WBEM Services *(continued)*

Name	Type	Version	Required Permission	To Perform
				By default, the information is formatted for display in English with uptime displayed in days, hours, minutes, and seconds. You can choose to receive the information in the CIM format. You can use this command only when the CIM Server is running. For more information on using this command, see *osinfo(1M)*.
`ssltrustmgr`	Command	A.02.07	`Root` permission is required to run this command.	To manage x509 certificates in a PEM format trust store file. Use this command to add, remove, or list x509 certificates in a PEM format trust store file.
`wbemexec`	Command	A.02.07	any user	To submit a CIM Operation Request to the CIM Server. The request must be encoded in XML. The CIM response is also encoded in XML. You will receive a message if the request does not pass the syntax checks of the HTTP server or the XML decoder. For more information, see *wbemexec(1M)*.
`WbemInfo.sh`	Script	A.02.07.04	Yes	This script is used to collect all system data that is needed for debugging when errors occurs in HP WBEM Services. This script collects information on system logs, system status, provider information and if required, repository information.
`wbemassist`	Command	A.02.09.02	Yes	A command that can be used to troubleshoot problems with HP WBEM Services.

2 Installing and setting up HP WBEM Services

This chapter describes the procedures for installing and setting up HP WBEM Services.

Compatibility information

HP WBEM Services is available on HP-UX 11i v1, v2, and v3. The provider versions that are compatible with HP WBEM Services will vary based on the version of HP WBEM Services that you want to install and the operating system version on which you install it.

Before installing HP WBEM Services, HP recommends that you read the HP WBEM Services release notes. The release notes lists the compatible provider versions with HP WBEM Services on HP-UX 11i v1, v2, and v3.

To view the HP WBEM Services Release Notes, see the *Networking and System Management* page at www.hp.com/go/hpux-networking-docs and select HP-UX 11i WBEM Software collection.

IMPORTANT: HP WBEM Services A.02.09.06 and later versions are not available on HP-UX 11i v2. HP WBEM Services A.02.09 and later versions are not available on HP-UX 11i v1. New features and enhancements for HP WBEM Services will not be addressed on HP-UX 11i v1 and 11i v2. Only defects that are critical in nature will be addressed.

The last available version of HP WBEM Services on HP-UX 11i v2 is A.02.09.04 (September 2010) and the last available version of HP WBEM Services on HP-UX 11i v1 is A.02.07.06 (March 2009).

HP WBEM Services compatibility tools

HP WBEM Services supports `wbemassist`, a command line utility to diagnose and report any installation and configuration related problems of HP WBEM Services on HP-UX.

It also provides information on the compatibility of providers supported by the specified HP WBEM Services for HP-UX versions.

The `wbemassist` utility tool checks for the following:

- If HP WBEM Services is successfully installed
- If required daemons are running on the system
- If cimsrvr group and user exist on the system
- If communication ports 5988 and 5989 are enabled
- If CIM Server is running and responding on the system
- If SSL certificate and its permissions are valid

To start the `wbemassist` utility, run the following command:

```
# wbemassist
```

The following output is displayed:

```
WBEMServices installation verification.....[PASS]
WBEM server running.....[PASS]
The WBEM ports are open.....[PASS]
Checking osinfo command response.....[PASS]
Checking WBEM Server response on local connection...[PASS]
Checking cimsrvr user.....[PASS]
Checking cimsrvr group.....[PASS]
Verifying WBEM SSL certificates.....[PASS]
```

```
Verifying WBEM SSL certificate permissions.....[PASS]
Verifying WBEM files and directories.....[PASS]
Total number of checks performed: 10
Total number of Errors: 0
```

To check the compatibility versions for HP WBEM Services, run the following command:

```
fsweb2# wbemassist -c -ov 11.23 -pn utilProvider -pv A.01.08.02.01.
```

The following output is displayed:

```
Compatible WBEMServices Versions A.02.09
```

NOTE: The `wbemassist` utility checks and recommends solutions for problems encountered while using HP WBEM Services only. It does not perform any check on WBEM providers or other services that use other CIM Server.

Backing up repositories and files

HP recommends that you back up appropriate HP WBEM Services directory structures and files on a regular basis. If these directories or files are deleted, moved, or corrupted, you will need to restore these files from the backup.

If you do not have a back-up of these repositories and files, especially SSL certificates files such as `file.pem` and `cert.pem`, then you will need to re-install HP WBEM Services or re-create certificates using the OpenSSL toolkit.

For more information on recreating certificates, see http://www.openssl.org/docs.

NOTE: When you re-install HP WBEM Services, only the default providers available with HP WBEM Services are installed and registered. Any additional providers that were registered with the previous installation of HP WBEM Services must be installed and registered again.

For HP-UX systems, you must back-up the following files:

- SSL certificate files
  - `/etc/opt/hp/sslshare/cert.pem`
  - `/etc/opt/hp/sslshare/file.pem`
- Directories for the repository files.

Table 2 Directories for the repository files

HP WBEM Services version A.02.07	HP WBEM Services version A.02.09
`/var/opt/wbem/repository/`	`/var/opt/wbem/repository/`
	`root#cimv2#hpvm.db`
	`root#cimv2#npar.db`
	`root#cimv2#vpar.db`
	`root#cimv2.db`
	`root#pg_internal.db`
	`root#pg_interop.db`
	`root.db`

For taking backups of files and repositories, HP recommends that you use the `cimreparchive` tool that is available with HP WBEM Services. The `cimreparchive` tool creates an archive copy

of the CIM Server repository in a specified archive file. The archive copy contains a consistent repository state even if it is created while the CIM Server is running.

Create the archive file using the `cimreparchive` tool. To restore the repository from the archive file, you must first stop the CIM Server and move the active repository files to a different location. Use the `tar<2>` command to extract the archived repository files and restart the CIM Server. For more information on the `cimreparchive` tool, see *cimreparchive(1M)*.

Prerequisites

Following are the prerequisites for installing HP WBEM Services:

- HP-UX 11i v1, HP–UX 11i v2, or HP-UX 11i v3
- OpenSSL

  HP recommends that you install the OpenSSL version available with the HP-UX operating environment before installing HP WBEM Services.

  NOTE: As updates to OpenSSL become available and installed over time, the HP WBEM Services `cimserver` process must be shutdown and restarted to run against any new version of OpenSSL. For more information on shutting down and restarting the CIM Server, see the "Starting and stopping the CIM Server" (page 26).

- Disk space requirements

  HP WBEM Services requires the following disk space to install:

`/`	5 MB
`/opt`	46 MB
`/var`	184 KB
`/usr`	1 MB

  Depending on the number of CIM objects to be stored in the CIM repository, additional disk space might be needed for the`/var/opt/wbem` directory.

- Port requirements

  HP WBEM Services uses dedicated ports for CIM-XML traffic. Two ports are dedicated for CIM-XML communication between the CIM clients and the CIM Server. One port is dedicated for CIM-XML communication between the Indication sender and the Indication receiver (a CIM Server).

  - HTTP port 5988
  - HTTPS (HTTP Secure) port 5989
  - HTTPS port for Export Connections

    NOTE: The list of port assignments is located in the `/etc/services` file.

Installing HP WBEM Services

HP WBEM Services is part of the HP-UX OE and is installed automatically when you start the HP-UX system. However, you can install HP WBEM Services at a later point by downloading the software from http://software.hp.com.

NOTE: To install HP WBEM Services, log in to the HP-UX system as `root` (`uid=0`).

IMPORTANT: Before installing the software, ensure that your system meets the requirements described in the section "Prerequisites" (page 19).

Complete the following procedure to install HP WBEM Services:

1. Download the product from http://software.hp.com –>Security and manageability.
2. Copy the downloaded depot file to a local directory on the system.
3. Log in to the HP-UX system as `root` and go to the directory where the depot is downloaded.
4. Start the installation.

   `swinstall -s <downloaded depot name> WBEMServices`

   The following files are installed:

`/etc/opt/hp/sslshare`	Shared SSL certificate files and trust store files.
`/etc/opt/wbem`	(directory)
`/opt/wbem`	(directory)
`/opt/wbem/bin`	commands, and executables
`/opt/wbem/lbin`	Executables that are not intended to be used directly by users.
`/opt/wbem/lib`	Shared libraries.
`/opt/wbem/mof/CIM`	MOF files.
`/opt/wbem/mof`	MOF files.
`/opt/wbem/mx`	Reserved.
`/opt/wbem/providers/lib`	Links to shared libraries for providers.
`/opt/wbem/sbin`	Commands and executables that only a `root` user can run.
`/opt/wbem/share/man`	Manpages.
`/var/opt/wbem`	Configuration files, CIM repository, log files, and so on.

IMPORTANT: Do not move the installed files from the default location. If these files are moved, it might result in problems in the functioning of the CIM Server.

5. Run the `swlist` command to determine if HP WBEM Services is installed.

   If the installation is successful, HP WBEM Services is listed in the output.

6. Run the `swverify` command to determine if HP WBEM Services is installed correctly.

   `# swverify WBEMServices`

   If HP WBEM services is correctly installed, the output of `swverify` does not show any errors or warnings.

After installing HP WBEM Services, the CIM Server is in a running state.

After installing HP WBEM Services, the following filesets that make up the product are visible on the system:

- WBEM-CORE, *<version number>* - WBEM Services core fileset for HP Integrity servers and HP 9000 servers.
- WBEM-CORE-COM, *<version number>* - WBEM Services core fileset for HP Integrity servers and HP 9000 servers
- WBEM-MAN, *<version number>* - WBEM Services manpages
- WBEM-MX, *<version number>* - Reserved for future use
- WBEM-TOOLS, *<version number>* - Available only from HP WBEM Services version A.02.09 and it contains tools for troubleshooting HP WBEM Services.

To ensure that the files installed by HP WBEM Services are not tampered with, run the following command:

```
swverify WBEMServices
```

If the files are not tampered, and are functioning as expected, then the following message is displayed:

```
Verification succeeded
```

Upgrading HP WBEM Services

HP WBEM Services can be upgraded to a more recent version without having to stop the OE. All information on the previous version of HP WBEM Services will still be available.

Run the following command to upgrade the HP WBEM Services version:

```
# swinstall -s <depot-name> WBEMServices
```

NOTE: This command automatically aborts all current client connections and stops the CIM Server. After the version is upgraded, HP WBEM Services automatically restarts the CIM Server and any indication providers that are installed are restarted. Also, the disabled providers are enabled.

IMPORTANT: After upgrading the HP WBEM Services version in your environment, you must upgrade the versions of the providers that are compatible with the HP WBEM Services version that you have upgraded to.

Downgrading HP WBEM Services

HP recommends that you do not downgrade to minor versions of HP WBEM Services.

Re-installing HP WBEM Services

The HP WBEM Services version that is currently installed in your environment might be corrupted. In such instances, you must re-install the software. To re-install the software, you must know of the current version that is installed. Run the following command to determine the currently installed version of HP WBEM Services:

```
# swlist -l product WBEMServices
```

After determining the version, complete the following procedure to re-install HP WBEM Services:

1. Download the HP WBEM Services version from the following location:

   http://software.hp.com –>Security and manageability.
2. Copy the downloaded depot file to a local directory on the system.
3. Log in to the HP-UX system as `root` and go to the directory where you downloaded the depot file.
4. Run the following HP-UX command to start the installation:

   ```
   swinstall -x reinstall=true -s <Downloaded Depot Name>\ WBEMServices
   ```

Providers and clients for HP WBEM Services

This section describes the default providers and clients that are available with HP WBEM Services.

NOTE: To view a list of all the provider modules on your system, run the `cimprovider -l` command. To view the providers in a specific module, run the `cimprovider -l -m <module_name>` command.

Providers available with HP WBEM Services

Following are the default providers available with HP WBEM Services:

Operating System Provider

The Operating System Provider gives operating system information, such as OS type, version, last boot up time, local date and time, number of users, swap space size, and free physical memory. This provider is used by clients to determine the basic understanding of the identity of the managed system on which it is running.

This provider uses the `CIM_OperatingSystem` class and the `PG_OperatingSystem` subclass.

- `SystemUpTime` is a convenience property. It provides direct access to this value, versus having client/providers calculate the value from `LastBootUpTime` and the `LocalDateTime`.
- `OperatingSystemCapability` indicates whether the OS is 32-bit or 64-bit capable.

NOTE: This provider does not support the reboot and shutdown methods of the `CIM_OperatingSystem` class. The `PG_OperatingSystem` subclass adds the `SystemUpTime` and `OperatingSystemCapability` properties.

Computer System Provider

The Computer System Provider makes available basic computer system information, such as computer name, status, and administrator contact information.

The Computer System provider uses the following classes:

- `CIM_ComputerSystem`
- `CIM_UnitaryComputerSystem`
- `PG_ComputerSystem`

  The `PG_ComputerSystem` class is a subclass of the `CIM_UnitaryComputerSystem` class. It adds the following properties:

  - `PrimaryOwnerPager`

    The pager number for the primary system owner.

  - `SecondaryOwnerName`

    The name of the secondary owner of the system.

  - `SecondaryOwnerContact`

    The phone number of the secondary owner of the system.

  - `SecondaryOwnerPager`

    The pager number of the secondary owner of the system.

  - `SerialNumber`

    The serial number of the system.

  - `IdentificationNumber`

    The corporate asset number of the system.

  These properties are typically on an HP-UX system using DMI.

NOTE: The `PG_ComputerSystem` class follows the industry convention of naming `CIM_UnitaryComputerSystem` subclasses without including `Unitary` in the class name. This practice is an exception to the normal practice used for creating non-DMTF defined subclasses (simply changing the prefix of the superclass `CIM_` to some organization-specific string).

Process Provider

The Process Provider makes available the basic UNIX process information, such as name of the executable image, process ID, priority, execution state, and various process resource utilization statistics. Client applications can use this provider to give clients an understanding of the processes running on the managed system within the context of its operating system.

In addition to implementing the properties of `CIM_Process`, these providers implement the properties of `CIM_UnixProcess` and `CIM_UnixProcessStatisticalInformation` in CIM v2.6 as `PG_UnixProcess` and `PG_UnixProcessStatisticalInformation`.

IP Provider

The IP Provider makes available information on the IP addresses that can be used to access a platform.

Client applications can use this provider to determine all the IP addresses for a platform, determine which LAN interface is associated with a given IP address, and to determine which IP routes are supported by the platform. For platforms that have the LAN provider installed, you can relate a given IP address to its LAN interface, MAC address, logical port, and network interface card (NIC).

NOTE: The current implementation is for HP-UX only.

This provider uses the following classes:

- `CIM_IPProtocolEndpoint`
- `PG_BindsIPToLANEndpoint`
- `PG_IPRoute`

Domain Name System Provider

The Domain Name System (DNS) Provider makes available the domain name information. This provider uses the `PG_DNSService` subclass of the `CIM_Service` class by adding properties, such as `SearchList` and `Addresses`:

- `SearchList` specifies the search list for hostname lookup.
- `Addresses` specifies the names or IP addresses, in dot notation format, of the name servers that the resolver must query.

NOTE: Currently, this provider does not support all properties of the `CIM_Service` class or its superclasses. This provider extends the `CIM_Service` class that describes a stem DNS.

Network Time Protocol Provider

The Network Time Protocol (NTP) Provider makes available server information used by the network time protocol service. The current implementation is for HP-UX only.

This provider uses the `PG_NTPService` subclass of the `CIM_Service` class by adding the `ServerAddress` property.

The `ServerAddress` property specifies the names or IP addresses, in dot notation format, of the servers that provide time to clients when requested.

NOTE: Currently, the provider does not support all the properties of the `CIM_Service` class or its superclasses. This provider extends the `CIM_Service` class to describe a NTP service.

Network Information Service Provider

The Network Information Service (NIS) provider makes available NIS information. The current implementation is for HP-UX only.

The Network Information Service provider instruments the PG_NISServerService subclass of the CIM_Service class by adding the properties ServerType and ServerWaitFlag:

- The ServerType property specifies if the instance is a master or slave server.
- The ServerWaitFlag property specifies the NIS server wait state (wait/no wait).

NOTE: Currently, the provider does not support all properties of the CIM_Service class or its superclasses. This provider extends the CIM_Service class that describes a NIS.

Software Distributor Provider

The Software Distributor (SD) Provider makes available information about software objects managed by the Installed Products Database (IPD).

The following software objects are supported by this provider:

- **Bundles** - Collections of filesets from several different products, encapsulated for a specific purpose. Bundles can consist of groups of filesets or products.
- **Products** - Collections of filesets, or (optionally) subproducts, and control scripts. Different versions of a product can be defined for different platforms and operating systems, as well as different revisions (releases) of the product.
- **Filesets** - Filesets include all the files and control scripts that make up a product. Filesets can only be part of a single product, but they can be included in several different HP-UX bundles or subproducts. Different versions of a fileset can be defined for different platforms. Filesets are the lowest level of object managed by SD-UX.

IOTree Provider

The IOTree provider makes available basic HP-UX PCI subsystem information such as the number and the various characteristics of the PCI slots, PCI cards, PCI devices, and PCI bridges. This IOTree provider uses the HPUX_PCIDevice, HPUX_PCIBridge, HPUX_PCISlot and HPUX_PCICard classes. Clients can use this provider to understand the PCI I/O subsystem of the HP computer system (typically a server or an appliance).

NOTE: The current implementation is for HP-UX only.

Clients available with HP WBEM Services

HP WBEM Services includes some clients that you can use to test the infrastructure in your environment. After installing HP WBEM Services, and registering the providers, you can run a basic verification check using these clients to determine if things are running as expected.

Following are the clients available with HP WBEM Services:

- The osinfo command

  Using this osinfo command, a client request is invoked to the Operating System provider that is available with HP WBEM Services. If the configuration is accurate, then a response such as the following is received:

```
Host: MySystem.com
Name: HP-UX
Version: B.11.11
UserLicense: Unlimited user license
Number of Users: 3 users
Number of Processes: 147 processes
OSCapability: 32 bit
LastBootTime: Jul 17, 2002  16:18:35 (-0700)
```

```
LocalDateTime: Aug 9, 2002  15:57:47 (-0700)
SystemUpTime: 1985952 seconds = 22 days, 23 hrs, 39 mins, 12 secs
```

- The `wbemexec` command

  This command is available with A.02.05 and later versions of HP WBEM Services. The `webemexec` command accepts a CIM-XML formatted file as input and sends it to the CIM Server as a CIM Request. The following is a sample CIM-XML input file:

```
<?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="1000" PROTOCOLVERSION="1.0">
<SIMPLEREQ>
<IMETHODCALL NAME="EnumerateInstances">
<LOCALNAMESPACEPATH>
<NAMESPACE NAME="root"/>
<NAMESPACE NAME="cimv2"/>
</LOCALNAMESPACEPATH>
<IPARAMVALUE NAME="ClassName">
<CLASSNAME NAME="PG_OperatingSystem"/>
</IPARAMVALUE>
<IPARAMVALUE NAME="LocalOnly">
<VALUE>FALSEVALUE>FALSE>
</IPARAMVALUE>
</IMETHODCALL>
</SIMPLEREQ>
</MESSAGE>
</CIM>
```

  If a configuration problem occurs with HP WBEM Services, then an error message is displayed.

  For more information on `wbemexec`, see the *wbemexec(1)*.

An error message from the `wbemexec` or the `osinfo` commands indicates a configuration problem with either the HP WBEM Services installation or configuration. In such cases, you must troubleshoot the problem and rectify it. For more information on troubleshooting such errors, see "Troubleshooting HP WBEM Services" (page 42)

Before starting HP WBEM Services

Before starting HP WBEM Services, ensure that the following are present:

- Ports are configured

  HP WBEM Services supports ports 5988 (`wbem_http`) and 5989 (`wbem_https`). These two ports are specified by DMTF and are registered with the Internet Assigned Numbers Authority (IANA) at http://www.iana.org.

IMPORTANT: Hewlett-Packard supports only these two port configurations: HTTP on port 5988, and HTTPS on port 5989.

  By default, the HTTP server of HP WBEM Services listens for Secure Sockets Layer (SSL) encrypted communications on the HTTPS (secure) port, 5989. If you are sure your environment is secure, you can set the configuration such that the server listens at the HTTP (non-SSL) port, 5988. For more information on ports, see Chapter 3 (page 33).

  When HP WBEM Services receives an HTTP request over the configured port, it checks user authentication, parses the request, looks up the resource, and contacts the registered provider, if applicable. The provider sends a response to HP WBEM Services, and HP WBEM Services sends it back to the client through this port.

- HP WBEM Services infrastructure

  For information about installing your version of HP WBEM Services, see the *HP WBEM Services Release Notes* at www.hp.com/go/hpux-networking-docs and select HP-UX 11i WBEM Software collection.

NOTE: If you already have HP WBEM Services installed, check your release notes before removing or re-installing it. You can remove all the files associated with HP WBEM Services and make all your providers unavailable.

IMPORTANT: Do not move or change HP WBEM Services files. Their locations are predetermined.

Starting and stopping the CIM Server

The CIM Server receives requests from management clients, and interacts with the respective providers to gather information that is requested by the management clients. The CIM Server receives information from the providers and sends it back to the management clients.

The CIM Server is designed to be constantly running, unless you manually stop it. In addition, it is designed to automatically restart when the operating environment is restarted, and continues to run as long as the OE is running.

IMPORTANT: HP recommends that you do not disable the CIM Server from running when the OE is restarted. If you disable the automatic restart of the CIM Server, it will impact other HP products such as HP Instant Capacity, HP Instant Capacity on Demand, HP SIM, VSE, and System Fault Management. These products on HP WBEM Services (`cimserver`) must be running.

If the CIM Server fails on an HP-UX system, the `cimserverd` daemon restarts it. For more information on the `cimserverd` daemon, see the section, "Using the cimserverd daemon" (page 27).

To determine if the CIM Server is running, enter the `ps -ef|grep cimserver` command.

Although it is designed to automatically restart with the OE, the CIM Server does not restart automatically in the following cases:

- If you have installed HP WBEM Services for the first time in your environment.
- If you have intentionally stopped the CIM Server with the `cimserver -s` command.
- If you have disabled HTTP and HTTPS connections using the `cimconfig` command, by setting the `enableHTTPconnection` and `enableHTTPSconnections` properties to `false`.

NOTE: CIM Server starts automatically if HP WBEM Services has stopped abruptly. HP recommends not to directly modify the files `/var/opt/wbem/cimserver_current.conf` and `/var/opt/wbem/cimserver_planned.conf` .

If the CIM Server is not running, restart the CIM Server with the `cimserver` command for HP-UX systems.

IMPORTANT: You must have `root` permissions to use the `cimserver` command to stop or start the CIM Server.

While shutting down the CIM Server with the `cimserver -s` command, you can also specify a value for the shutdown property on the command line interface (`shutdownTimeout=value`). For example, if the CPU utilization of the system is very high, you might want to let the shut down process to take a longer time. The value that you specify is applicable only for the current shutdown instance.

While starting the CIM Server with the `cimserver` command, you can specify several properties and value pairs on the command line interface. The values that you specify are applicable only for the current instance. After the CIM Server is restarted, the values of the properties revert to those specified in the current and planned configuration files.

For information on the options that you can set, see "CIM Server properties" (page 29). You can also view the manpage for the `cimconfig` command.

If you attempt to start the CIM Server when it is already running, the following message appears:

```
/opt/wbem/lbin/cimserver: cimserver is already running (the PID found
in the file "/etc/opt/wbem/cimserver_start.conf" corresponds to an
existing process named "cimservermain").
```

NOTE: This message is displayed with HP WBEM Services version A.02.05 and later.

In versions prior to A.02.05, you can determine the version number with `cimserver` command only when the CIM Server is running. Starting with A.02.05, you can determine the version number with the `cimserver` command irrespective of whether the CIM Server is running or not.

Using the cimserver command

On HP-UX systems, if the CIM Server is stopped manually, then the `cimserverd` daemon cannot restart it, and the CIM Server will not restart when the HP-UX system is restarted. In such cases, use the `cimserver` command to restart the CIM Server.

To stop the CIM Server, use the `cimserver -s` command. To view the version of the CIM Server, use the `cimserver -v` command.

On HP-UX systems, when the `cimserver` command is used without specifying any options, it starts the CIM Server. While starting the CIM Server, you can specify the values for several configuration parameters. To set the configuration properties, use the following format:

`cimserver <property_name> = <value>`

But these configuration values will last only as long as the current process. To ensure that these configuration values last beyond the current process, you need to add required configuration values to the `cimserver_planned.conf` file. This can be done manually or by using the `cimconfig` command. The `shutdownTimeout` property is the only property that can be used along with the `cimserver -s` command while shutting down the CIM Server. The value of the `shutdownTimeout` property specifies the time, in seconds, for a shutdown for the CIM Server. After the time specified for this property elapses, the CIM Server terminates all the processes and shuts down.

Verifying status of Cimserver

The `–status` option verifies whether or not the Cimserver is running.

`# cimserver --status` (when Cimserver is running)

```
CIM Server is running.
```

`# cimserver –status` (when Cimserver is not running)

```
CIM Server is not running.
```

Using the cimserverd daemon

The `cimserverd` daemon periodically checks the status of the CIM Server. By default, the daemon checks the CIM Server every 30 seconds. The time between the checks can be modified by editing the `/etc/opt/wbem/cimserver_retry.conf` file. You must have `root` permissions on the local system to edit this configuration file.

After editing the file, complete the following steps to terminate all the processes and force `cimserverd` to read the updated file:

1. Find the Process Identification Number (PID) of the `cimserverd` daemon.

   ```
   ps -ef | grep cimserverd
   ```

2. Terminate the processes.

   ```
   kill -9 <PID>
   ```

   The `cimserverd` daemon is automatically re-spawned by *init(1M)* because it has an entry in the `/etc/initttab` file.

NOTE: The `cimserverd` daemon automatically restarts the CIM Server when it fails on a system, but not in cases where the CIM Server is manually halted.

Using the cimconfig command

The `cimconfig` command manages properties that are used to configure the CIM Server. The configuration operations are executed on the CIM Server running on the local host. Use the `cimconfig` command to view, set, or clear the CIM Server property values. Use the `-l c` (list current) option to view all the properties and the current values.

An operation on a property using the `cimconfig` command with the `-c` (current) option takes effect immediately. An operation on a property using the `cimconfig` with the `-p` (planned) option takes affect only after the CIM Server is restarted with the `cimserver` command.

Dynamic properties can be set with either the current or planned property. Non-dynamic properties must be set using the planned property. Modifications made with the `cimconfig` command remain in effect until they are changed again with the `cimconfig` command. HP WBEM Services must be up and running prior to using the `cimconfig` command.

You can temporarily modify property values when HP WBEM Services is down by entering options as a `propertyname=value` pair at startup on the `cimserver` command line. However, these modifications last only as long as the CIM Server is running. At shutdown, you can temporarily modify just one property value, `shutdownTimeout`, by entering a value on the `cimserver shutdown` command line. The timeout value can be changed dynamically. The value of other properties cannot be changed dynamically. For all other properties, you must use the `-p` parameter to indicate your change, after which you must stop and restart the CIM Server.

IMPORTANT: Do not edit the configuration files directly. Always use the `cimconfig` command to change the values of the properties in the files. If you manually edit the configuration files, then `cimserver` will not be able to identify the changes made to the properties.

Using the cimtrust command

Use the `cimtrust` command to list, add, or remove x509 certificates in a PEM format to or from the trust-store. Ensure that the CIM Server is running, before using this command.

NOTE: This command only performs these actions on the trust-store of the local system.

TIP: To view the list of certificates in the trust-store of the local system, use the `cimtrust` command with the `-l` option. You can filter the list of certificates based on the issuer, along with either the serial number or the subject.

To add an x509 certificate of a specified type to the trust-store, use the `cimtrust` command with the `-a` option. You also need to specify a username, using the `certuser` option, to be associated with the certificate in the file. If no user is specified, then the certificate cannot be used to authenticate a user.

To remove an x509 certificate from the trust-store, use the `cimtrust` command with the `-r` option. This option removes the x509 certificates that matches the specific issuer and either the serial number or subject from the trust store.

If an error occurs when you are adding or removing x509 certificates, then an error message is written to the standard output.

For more information on using this command, see *cimtrust(1M)*.

CIM Server properties

After HP WBEM Services is installed, you can configure the properties listed in this section using the `cimconfig` command. You must have privileged user (`root`) permissions to modify the values of these properties.

You must regularly backup the following property configuration files:

For HP-UX:

- `/var/opt/wbem/cimserver_current.conf` contains the *current* values that are not defaulted.
- `/var/opt/wbem/cimserver_planned.conf`contains *planned values*, not yet in effect and not defaulted.

Following are the properties of the CIM Server that you can modify:

- `authorizedUserGroups` - Set to user group names, group names are separated by a comma. The default is not set to any user group, which implies that all users on the system are authorized (if not restricted by setting enableNamespaceAuthorization) to access CIM resources.

  You can use user group authorization if you need the extra security of restricting access to CIM resources.

  A privileged user (user with `root` permissions on the local system) is always authorized. A privileged user can grant user group authorizations to other users. For more information, see Chapter 3 (page 33).

- `enableHttpConnection` - Set to true or false. The default is false, which means that HP WBEM Services listens at port 5989 HTTPS connection only. Setting it to true enables user access through port 5988, using HTTP TCP/IP communication. Use HTTP connections only if you are certain your environment is secure. For more information, see Chapter 3 (page 33).
- `enableHttpsConnection` - Set to true or false. The default setting, true, enables users to access through port 5989, using the HTTPS TCP/IP communication. HTTPS connection has better security than HTTP. For more information, see Chapter 3 (page 33).
- `enableNamespaceAuthorization` - Set to true or false. The default setting, false, means that users are authorized across all namespaces. If `enableNamespaceAuthorization` is set to true, you must authorize each user, namespace by namespace, with the `cimauth` command.

  You can use namespace authorization when you need the extra security of restricting access to certain namespaces. Users with `root` permission on the local system are privileged users. A privileged user can grant namespace authorizations to others. For more information, see Chapter 3 (page 33).

- `enableRemotePrivilegedUserAccess` - Set to true or false. The default setting is true as of the 1.5 version of HP WBEM Services. (In earlier versions, it was false.) A true setting means that an authenticated user, with privileged access to the system running HP WBEM Services, is allowed to issue requests to HP WBEM Services from a remote system.
- `shutdownTimeout` - Set to a number of seconds. When a `cimserver -s` shutdown command is issued, the timeout is the maximum number of seconds allowed for the CIM Server to complete outstanding CIM operation requests before shutting down. If the specified timeout period expires, the CIM Server will shut down, even if there are still CIM operations in progress. The minimum value is 2 seconds and the maximum value is 30 seconds. By default, the value is set to 30 seconds.

- `enableSubscriptionsForNonprivilegedUsers` - Set to true or false. The default, false, means that only a privileged user (superuser) will be allowed to create Indication Subscriptions.
- `sslClientVerificationMode`

  Describes the required level of support for certificate-based authentication. This property is only used when `enableHttpsConnection` is set to true.
- `idleConnectionTimeout`

  If set to a positive integer, this value specifies a minimum timeout value for idle client connections. If set to zero, idle client connections do not time out. A client connection is considered idle when it is not in the process of sending a request and the CIM Server is not processing a request from that connection.
- `enableAuditLog`

  Set to true or false. The default value is set to false as of A.02.09 version of HP WBEM Services. The value true means additional information such as AuditType(Authentication) , AuditSubType(Local Authentication, Basic Authentication, and so on), AuditEvent(startup, shutdown, and so on) , log level (WARNING, INFORMATION, and so on), user (`root`, guest, and so on) and system IP address is logged in the `syslog.log` file.
- `socketWriteTimeout`

  Specifies the number of seconds that the CIM Server waits for a client connection to be ready and receive data. If the CIM Server is unable to write to a connection within this time, then the connection is closed.
- `maxFailedProviderModuleRestarts`

  The new release includes a new config property called `maxFailedProviderModuleRestarts`. This value by default is zero. If set to a positive integer (maximum 3), this value specifies the number of times the failed provider module with indications enabled is restarted automatically before being moved to Degraded state. If set to zero, the failed provider module is not restarted with indications enabled automatically and is moved to Degraded state immediately.

  ```
  #cimconfig –lc
  maxFailedProviderModuleRestarts=0
  ```

  To set to positive integer:

  ```
  cimconfig -s maxFailedProviderModuleRestarts =3  -c
  # cimconfig –lc
  maxFailedProviderModuleRestarts=3
  ```

  This method of setting the `maxFailedProviderModuleRestarts` value to 3 is a temporary setup. After Cimserver is restarted, the `maxFailedProviderModuleRestarts` value is changed to 0.

  To set the value of `maxFailedProviderModuleRestarts` permanently:

  ```
  # cimconfig –lc
  maxFailedProviderModuleRestarts=0
  #cimconfig -s maxFailedProviderModuleRestarts=3 –p
  # cimserver –s; cimserver
  # cimconfig –lc
  maxFailedProviderModuleRestarts=3
  ```

  NOTE: To set the value of `maxFailedProviderModuleRestarts` permanently, you must restart the Cimserver.
- `sslCipherSuite`

  Strong ciphers are enabled in Cimserver by adding the config property `sslCipherSuite`. This string contains the OpenSSL cipher specifications required to configure the cipher suite.

As a result, the client is permitted to negotiate with the server during the SSL handshake phase. The default value of this property is DEFAULT.

The other configurable values are HIGH and LOW.

For more information, see the `cimconfig` command manpages.

This is not a dynamic property. Hence, it requires a cimserver restart.

Configuring Insight Remote Support (IRS) for WBEM Services

HP WBEM Services version A.02.09.08 and later supports Insight Remote Support (IRS) configuration on HP-UX 11i v2 and HP-UX 11i v3 operating systems.

To configure `root` privileges for IRS users on an HP-UX system, perform the following steps:

1. Install HP WBEM Services version A.02.09.08 or later on HP-UX 11i v3 and 11i v2 operating systems.
2. Edit the IRS configuration file located at: `/var/opt/wbem/hp_irs_users.conf` on an HP-UX system and enter the required user name. By default, the `hp_irs` user name is added in the IRS configuration file.

   NOTE: Only system administrators can modify or create user names in the IRS configuration file. Ensure that the user name exists on the HP-UX system before configuring in the IRS configuration file.

3. Stop WBEM Services.

   ```
   cimserver -s
   ```

4. Restart WBEM Services.

   ```
   cimserver
   ```

   NOTE: Users configured in the IRS configuration file can perform WBEM operations with `root` privileges. However, these users can still continue to have system privileges as defined in the HP-UX `/etc/passwd` file.

Maintaining the repository

HP WBEM Services stores definitions of the data on managed objects and their providers in its repository. The location of these repository files vary depending on the version of HP WBEM Services. The following information is valid for versions prior to HP WBEM Services A.02.09.

The repository files located in `/var/opt/wbem/repository/` for HP-UX are created as a by-product of the HP WBEM Services installation. Do not delete or move these files.

Four namespaces are installed with HP WBEM Services. Others can be added by clients and providers. The four namespaces that are automatically installed are:

- `root`: The root namespace exists to conform to the DMTF specifications.
- `root/cimv2`: The standard CIM schemas go here. Also, the schemas for the bundled providers.
- `root/PG_Interop`: This is for provider registration. This space is reserved exclusively for providers, and all providers must register here. Fore more information, see the `cimprovider` manpage.
- `root/PG_Internal`: This space is reserved for use by HP WBEM Services only.

You must schedule frequent backups of the repository. If the repository is moved or lost or corrupted, you must restore the files you backed up. To take backups, HP recommends that you use the `cimrepoarchive` command.

If you cannot restore the files, the `init_repository` script will restore the files to the way they were when you first installed HP WBEM Services. The default providers that installed with HP WBEM Services will be intact. However, any managed objects, providers, or namespaces that you added since you first installed HP WBEM Services will be removed. You will need to re-register (or re-install) all the added providers.

To run the `init_repository` script, enter the following commands:

1. Shut down the CIM Server.

   ```
   cimserver -s
   ```

2. Move the repository directory.

   ```
   mv /var/opt/wbem/repository
   /var/opt/wbem/repository.bak
   ```

3. Start the CIM Server.

   ```
   cimserver
   ```

4. Run the `init_repository` script.

   ```
   /opt/wbem/sbin/init_repository
   ```

   The following list of errors and warnings is displayed. Ignore these warning:

   PGS04838: Warning: Class CIM_ManagedElement already exists in the repository

   PGS04838: Warning: Class CIM_ManagedSystemElement already exists in the repository

   PGS04838: Warning: Class CIM_LogicalElement already exists in the repository

   PGS04838: Warning: Class CIM_OperatingSystem already exists in the repository

   PGS04838: Warning: Class CIM_System already exists in the repository

   PGS04838: Warning: Class CIM_ComputerSystem already exists in the repository

   PGS04838: Warning: Class CIM_UnitaryComputerSystem already exists in the repository

Removing HP WBEM Services

To remove HP WBEM Services, run the following command:

```
# swremove WBEMServices
```

When products are in your environment, which have a dependency on the file sets of HP WBEM Services, then this command might result in an error. In this error occurs, run the following command to remove HP WBEM Services:

```
# swremove -x enforce_dependencies=false WBEMServices
```

3 Security considerations

This chapter describes the security aspects of working with HP WBEM Services.

In any network, security is always of prime importance. For HP WBEM Services, security is first checked at the communication channels. HP WBEM Services supports the following connection points:

- HTTP port 5988
- HTTP Secure (HTTPS) port 5989
- HTTPS port for Export Connections
- A UNIX domain socket for local connections

Ports 5988 (HTTP TCP/IP communication) and 5989 (HTTPS TCP/IP communication) are dedicated for CIM-XML communications between CIM clients and the CIM Server. The port defined by the service name `wbem-exp-https` (HTTPS port for Export Connections) is dedicated for CIM-XML communication between the Indication sender and the CIM Server which acts as the Indication receiver. You can disable the HTTP and the two HTTPS connection points using the `cimconfig` command line utility. However, the UNIX domain socket connection is always enabled when the CIM Server is running.

Guidelines for using SNMP, PRM, and WLM

For HP WBEM Services, you can make use of SNMP as well as Process Resource Manager (PRM) and Workload Manager (WLM). Following are some of the security considerations that you must keep in mind while using SNMP as well as PRM and WLM:

- You can use the tools available with Process Resource Manager (PRM) and Workload Manager (WLM) to limit computing resources used by the processes of HP WBEM Services. You can purchase these products from http://www.software.hp.com.

  However, by limiting or restricting the computing resources of the WBEM Services processes, depending on the configured limits and WBEM Services utilization, it might constantly reach its limits, resulting in issues.

- Due to known security vulnerabilities and limitations of the SNMP protocol, HP does not recommend the use of the SNMP indication handler.

Configuring SSL

When HTTPS connections are enabled, HP WBEM Services uses the Secure Sockets Layer (SSL) for communication. To enable this communication, the server-side certificates are trusted by the management application. HP WBEM Services uses OpenSSL to support HTTPS connections.

NOTE: OpenSSL is an open source cryptography toolkit that implements network protocols and related cryptography standards of SSL v2/v3 and Transport Layer Security (TLS). For more information on OpenSSL, see the information available at: http://www.openssl.org.

HP WBEM Services supports only SSL v3 and TLS protocols.

On the HTTPS port, CIM clients are required to use SSL to establish connections with the CIM Server and to send CIM requests.

To disable the HTTPS port, use the `cimconfig` command to set the planned value of the CIM Server configuration property `enableHttpsConnection` to `false`. Ensure that the planned value for `enableHttpConnection` is set to `true` and restart the CIM Server.

To disable the Export HTTPS port, use the `cimconfig` command to set the planned value of the configuration property `enableSSLExportClientVerification` to `false` and restart the CIM Server.

HP WBEM Services configuration options security disclaimer

As a security best practice, HP recommends that you disable any network daemon that you do not use in your environment. Any daemon that is in use must be configured securely according to the threat environment in which they are located. This is a functionality vs. security risk tradeoff. The optimal configuration varies depending on local threats and functionality requirements.

Default security information

For ease-of-manageability, HP WBEM Services defaults to a 'functional' out-of-the-box configuration, but also provides you with several configuration options such that security risks are minimized. Following are some of these options:

- You can configure the CIM Server to only accept connections from the local UNIX domain sockets. This is appropriate if you have users on your network who are not trusted and if you do not plan to use HP WBEM Services for remote management.
- You can configure HP WBEM Services to only allow access from a trusted subset of system users such as `root`, and application users such as Oracle, using a UNIX group.

  Setting up this user group is recommended if you intend to use HP WBEM Services in an environment where local users are not trusted, or if HP WBEM Services acts as a second line of defense against break-ins and other security threats.

  NOTE: After creating a UNIX group, if an application fails to authenticate, you might have to add an application or associated system users.

- HP WBEM Services supports the use of other protective measures for high-threat environments. For example, IPSEC, HP-UX Secure Shell, or hardware solutions can be used to create a VPN to increase security. A VPN is recommended if you intend to use HP WBEM Services for management across a network that is not trusted, such as, an exposed DMZ or the public Internet.

4 Authentication methods in HP WBEM Services

This chapter elaborates on the authentication methods in HP WBEM Services.

HP WBEM Services supports the following authentication methods:

- Local authentication:

  This method is used to authenticate requests from local users. In this scenario, if the user is on the same system as HP WBEM Services, then the authentication already performed by the system is used by HP WBEM Services. For more information, see "Local user authentication" (page 35).

- Remote Authentication:

  This method is used to authenticate remote users that send requests. If the user request is from a remote system, then it is first directed to the HTTP server of HP WBEM Services. The HTTP server receives only valid CIM requests and all other requests are rejected. User information is included in the XML-encoded HTTP message header and the CIM Server checks the user-password and SSL certificate information. For more information, see "Remote user authentication" (page 36).

- Providers: HP WBEM Services interacts with its registered providers through shared libraries.

NOTE: CIM providers can run as privileged users. Be cautious while installing a provider that does not come from a trusted source.

After HP WBEM Services passes on a request to a provider, the provider is responsible for checking its own security. The provider sets the rules about which requests it considers, and the conditions for granting or refusing them. If a provider requires authorization beyond that checked by HP WBEM Services, the provider supplier is responsible for documenting its own rules.

HP WBEM Services uses dedicated ports for CIM-XML traffic. Two ports are specified by DMTF and registered with IANA for CIM-XML communication between the remote clients and the CIM Server:

- HTTP TCP/IP communication on port 5988 (wbem_http)
- HTTPS TCP/IP communication on port 5989 (wbem_https)

HP supports only these two port configurations.

User authentication

When a user request comes through the HTTP or HTTPS port, the CIM Server determines if the user is a legitimate user on the system or not. If the request does not pass authentication, the request is rejected without processing it any further.

Local user authentication

For local users, the CIM Server uses a local authentication mechanism. The CIM Server uses the existing file system security to authenticate the user. HP WBEM Services accepts the authentication already done by the system. As a result, local requests include only the login name of the user. The password information is not required.

The CIM Server automatically authenticates local connections. Local connections are those connections that are established using the `connectLocal` method in the `CIMClient` interface. This authentication method eliminates the need for specifying the user name or password when issuing management commands on the local system.

The UNIX domain socket connection point is used for local connections, so this traffic is not visible on the network interconnect.

Remote user authentication

The CIM Server can authenticate remote users with one of the following methods:

- HTTP Basic Authentication
- Certificate Based Authentication

Table 3 describes these authentication methods.

Table 3 Remote User Authentication Methods

Certificate Based Authentication (CBA)	HTTP Basic Authentication
Description	
The CIM Server requests the client certificate while HTTPS connection is in progress.	Using a request/challenge mechanism and authenticating the user-supplied username and password through Pluggable Authentication Modules (PAM).
Benefits and Considerations	
• Requires a one-time server configuration. • Does not require the remote user to provide a password each time to access the WBEM data. The benefits of not requiring a password include: • Prevents intruders from gaining access to internal network resources by "spoofing" passwords. • Additional configuration or updates to applications is not required whenever a password is changed.	• Easier to setup, as it does not require any server configuration. • Requires the remote user to provide a password each time to access the WBEM data. • You will have to update the client application each time the password is changed.
For more information, see	
"Additional information on Certificate Based Authentication" (page 37)	"Additional information on HTTP basic authentication" (page 36)

The default value for the configuration parameter `enableRemotePrivilegedAccess` has been changed to `TRUE` with the release of HP WBEM Services version A.01.05.02. This implies that, by default, an authenticated user with privileged access to the system running HP WBEM Services is allowed to issue requests to HP WBEM Services from a remote system.

When HP WBEM Services is installed, the CIM Server is configured with a randomly-generated, self-signed certificate. If a self-signed server certificate does not provide a sufficient level of trust, you can use a central Certificate Authority such as Verisign to issue certificates.

Additional information on HTTP basic authentication

The `/etc/pam.conf` file is the configuration file for PAM. The `/etc/pam.conf` file contains a list of services and each service is mapped to a corresponding service module. When a service is requested, its associated module is invoked. HP WBEM Services defaults to the authentication mechanism specified in the `OTHER` directive of the `/etc/pam.conf` file.

To use other authentication methods, you must edit the`/etc/pam.conf` file and add a `wbem` service entry.

For example:

```
#
# Example of /etc/pam.conf file with WBEM services (using LDAP)
#
# Authentication management
wbem auth required libpam_hpsec.so.1
wbem auth sufficient libpam_unix.so.1
```

```
wbem auth required libpam_ldap.so.1 try_first_pass
# Account management
wbem account required libpam_hpsec.so.1
wbem account sufficient libpam_unix.so.1
wbem account required libpam_ldap.so.1
# Session management
wbem session required libpam_hpsec.so.1
wbem session sufficient libpam_unix.so.1
wbem session required libpam_ldap.so.1
# Password management
wbem password required libpam_hpsec.so.1
wbem password required libpam_ldap.so.1 try_first_pass
wbem password required libpam_ldap.so.1 try_first_pass
```

For more information, see the `pam(3)` and `pam.conf(4)` manpages.

NOTE: HP-UX uses the `cimservera` executable in HP WBEM Services to provide the CIM Server with PAM Authentication services.

Additional information on Certificate Based Authentication

Before using Certificate Based Authentication (CBA), you must complete the following steps:

1. Enable CBA using the `cimconfig` command.

   By default, CBA is disabled. For more information on enabling CBA, see the *cimconfig*(1M) and *cimtrust*(1M) manpages.
2. Use the `cimtrust` command to include client certificates from the trust store in the `cimserver` and associate that certificate with a system user.
3. Enable the HTTPS connections so that the certificate of the client is authenticated by HP WBEM Services.

NOTE: HP System Insight Manager (HP SIM) version 5.1 or later supports the Certificate-Based remote user authentication. For more information on certificate based remote user authentication, see the HP SIM documentation.

HTTPS and HTTP

By default, `enableHttpsConnection` is set to `true`, and HP WBEM Services listens on port 5989. You can set the HTTPS connection to `false`, and set the property `enableHttpConnection` to true to make HP WBEM Services listen on port 5988.

Use the `cimconfig` command to reset the property file. To change properties temporarily, for just one session, start the CIM Server with the `cimserver` command and use the command-line properties option.

If you set both, HTTPS and HTTP to *true* then HP WBEM Services will listen on ports 5988 and 5989.

If you set both to `false`, HP WBEM Services will listen only on the domain socket and will only accept requests from local clients, i.e. connections established using the `connectLocal` method in the `CIMClient` interface.

By default, HP WBEM Services uses Secured Socket Layer (SSL) for all communications, with server-side certificates that are trusted by the management application. This provides both spoof protection and confidentiality.

NOTE: Basic Authentication requires the client to pass both the user name and password, in Base64 encoding. This encoding is not secure. SSL (`enableHttpsConnection`) must be disabled only in a highly secure environment where transferring clear text passwords does not pose a security threat.

HP WBEM Services uses OpenSSL to support HTTPS connections. OpenSSL is a cryptography toolkit that implements the network protocols and related cryptography standards of SSL v2/v3 and TLS (Transport Layer Security). For more information about OpenSSL, see http://www.openssl.org/docs.

On the HTTPS port, CIM clients are required to use SSL (Secure Socket Layer) to establish connections with the CIM Server and to send or receive CIM requests.

Managing certificates

During the install process, if `/etc/opt/hp/sslshare/cert.pem` and `/etc/opt/hp/sslshare/file.pem` files are found on the system, the following messages are generated in the install log:

```
NOTE: /etc/opt/hp/sslshare/cert.pem - SSL Certificate file already
exists. New certificates are not created.
```

The existing files, `/etc/opt/hp/sslshare/cert.pem` and `/etc/opt/hp/sslshare/file.pem` might have been created by an earlier installation of HP WBEM Services A.02.05 or an installation of other management applications on the system. These files will not be overwritten.

Following are a couple of scenarios that illustrate updating certificates when an earlier version of HP WBEM Services is already installed on an HP-UX system:

- **Scenario 1**

  Using the default installed certificates from HP WBEM Services version A.01.05.

  HP recommends that after installing HP WBEM Services version A.02.07, you complete the following steps:

  1. Delete the existing `/var/opt/wbem/server_2048.pem` and `/var/opt/wbem/server.pem` files and use the certificates in `/etc/opt/hp/sslshare` directory.

     OR

  2. Overwrite the new certificate in `/etc/opt/hp/sslshare/cert.pem` and the private key in `/etc/opt/hp/sslshare/file.pem` with the existing certificate and key in either `/var/opt/wbem/server_2048.pem` or `/var/opt/wbem/server.pem` files. Before overwriting `/etc/opt/hp/sslshare/cert.pem` and `/etc/opt/hp/sslshare/file.pem` make sure other products are not using the certificates in these files.

     If the server certificate was copied to any other system, then the new certificate in `/etc/opt/hp/sslshare/cert.pem` must be copied over to the trust store on those other systems to replace the earlier certificate.

     NOTE: Use the `ssltrustmgr` command to add or remove certificates in a trust store. For more information about the `ssltrustmgr` command, see the *ssltrustmgr* manpage.

- **Scenario 2**

  Using custom certificates:

  If using either self-signed or root-signed 512-bit or 1024-bit encryption certificates, HP recommends that you create new certificates with 2048-bit encryption.

If using CA certificates that are using 2048-bit encryption, HP recommends that you keep them. If the CA certificates are not using 2048-bit encryption, HP recommends that you get new CA certificates with 2048-bit encryption.

Importing server certificates to the Trust Store

CIM client applications must maintain a trust store in a `<trust_store-name>.pem` file. The CIM client applications must import the certificates stored in the `/etc/opt/hp/sslshare/cert.pem` file, from all CIM Server systems that it needs to connect to, into a trust store file on the client system.

With C++ CIM client libraries, the trust store must be in the PEM format.

To import a server certificate, copy the public certificate from the server to the client:

1. Copy the certificate (`/etc/opt/hp/sslshare/cert.pem`) from the system where HP WBEM Services is installed.

   NOTE: Do not copy the key in the `/etc/opt/hp/sslshare/file.pem` file. Copy only the public certificate in the `/etc/opt/hp/sslshare/cert.pem` file.

2. Use the `ssltrustmgr` command to add the certificate from `cert.pem` file to the trust store `<trust_store-name>.pem` on the client machine.

   NOTE: The `wbemexec` and the `osinfo` commands use the file `/etc/opt/hp/sslshare/client.pem` as their trust store. Import the server certificates for these clients into this file.

Verifying certificates

This section discusses the methods in which you can verify certificates.

Using CIM clients

The CIM Client Interface supports the trust store and verification callback function as mechanisms for server certificate verification. The CIM Client applications can use one or both of these mechanism to verify the server certificate.

Using the `wbemexec` client

The `wbemexec` command provides a command-line interface to a CIM Server.

The `wbemexec` command uses the trust store for server certificate verification. Be sure to import the certificate in the `/etc/opt/hp/sslshare/cert.pem` from the system where the CIM Server is running to the client system's trust store.

For more information about certificates, see "Importing server certificates to the Trust Store" (page 39).

The SSL connection of the `wbemexec` client to the CIM Server fails if the server certificate is not found and verified in the trust store.

For more information about the `wbemexec` command, see the *wbemexec* manpage.

IMPORTANT: The use of the `wbemexec` client is not recommended in high-threat environments because this client does not perform any additional certificate verifications, such as host-name or certificate-depth verification.

Using the `gen_wbem_certs` command

The `gen_wbem_certs` command is used in HP WBEM Services Version A.02.07.04 to verify certificates. Use the following command:

```
# gen_wbem_certs -verify
```

User group authorization

User group authorization consists of establishing the already authenticated user is a member of one of the configured groups in the `authorizedUserGroups` configuration property. If the user is not authorized, the client request is rejected without processing it and an authorization failure message is sent back.

A user with `root` permissions (`uid 0`) on the local system can use the `cimconfig` command to set the HP WBEM Services `authorizedUserGroups` property to one or more user groups on the local system.

NOTE: A user with `root` permissions (uid 0) on the local system always has authorization to access CIM resources.

When the `authorizedUserGroup` property is set to valid group names on the system and a user who is not a member of the configured group submits a request, the following error message is displayed:

```
User <user name> is not authorized to access CIM data.
```

For more information on setting authorized user groups, see the manpage for the `cimconfig` command.

Namespace authorization

CIM Services provides authenticated users controlled access to the entire CIM schema. It does not check security for specific resources such as individual classes and instances.

However, you can choose to control each user's access by requiring authorization for each user on each namespace. A user with `root` permissions (`uid 0`) on the local system can first use the `cimconfig` command to set the `enableNamespaceAuthorization` property of HP WBEM Services to `true`, and then use the `cimauth` command to set each user's access authorization on each namespace.

NOTE: A user with `root` permissions on the local system (`uid 0`) always has full permissions on all namespaces.

When namespace authorization is set to `true`, and users submit a request for a namespace that they are not authorized on, the following error message is displayed:

```
Not authorized to run <requesting operation> in the namespace <requesting namespace>.
```

For more information about authorization, see the manpages for the `cimauth` and `cimconfig` commands.

Authorization permissions include `Read`, `Write`, or `Read and Write`. Note that `Write` permission does not automatically include `Read` permission.

The following CIM operations require `Write` authorization:

```
CreateClass
CreateInstance
DeleteClass
DeleteInstance
DeleteQualifer
InvokeMethod
ModifyClass
ModifyInstance
SetProperty
SetQualifier
```

The following CIM operations require `Read` authorization:

```
EnumerateClasses
EnumerateClassNames
EnumerateInstances
EnnumerateInstanceNames
EnumerateQualifiers
GetClass
GetInstance
GetProperty
GetQualifier
```

5 Troubleshooting HP WBEM Services

This chapter elaborates on how to troubleshoot HP WBEM Services in your environment.

This chapter is for people who are having trouble while trying to use HP WBEM Services.

Checklist for troubleshooting HP WBEM Services

Before contacting the support, read the checklist for troubleshooting HP WBEM Services.

- Is CIM Server running? Enter the command `ps -ef|grep cimserver`. If it is not running, then you must start it.

  For HP-UX: enter `cimserver` (no options).

- Is HP WBEM Services installed correctly? For HP-UX, enter: `swverify WBEMServices`.
- Do you have the essential files? These directories and files are created as a by-product of the HP WBEM Services installation. Do not move these files. The first two files are the SSL certificates files. The next four are the directories for the repository files.

  For HP-UX:

  - `/etc/opt/hp/sslshare/cert.pem`
  - `/etc/opt/hp/sslshare/file.pem`
  - `/var/opt/wbem/repository/root.db`
  - `/var/opt/wbem/repository/root#PG_InterOp.db`
  - `/var/opt/wbem/repository/root#PG_Internal.db`
  - `/var/opt/wbem/repository/root#cimv2.db`

- If any of these files are missing, restore all the repository directories and files from your backup.

  If you cannot restore the repository directories, you will have to re-initialize the repository. This will return it to the state it was in when you installed HP WBEM Services, and you will lose any changes made since then. For more information on the repository, see "Maintaining the repository" (page 31).

- Are you trying to process a request when the provider is not registered or enabled?

  Run the `cimprovider -l -s` command to list the name and status of the registered provider modules. Run the `cimprovider -l-m <modulename>` command to view the individual providers in each module.

- Exercise the path that requests follow: Run the `osinfo` command. This invokes a simple request. It processes and displays a response when it is completed.
- Check the `syslog` files. HP WBEM Services messages are listed.
- Are you seeing SSL certificate related messages on a CIM Client request failure? Make sure the remote CIM Server certificate `/etc/opt/hp/sslshare/cert.pem` is added to the trust store file on the client system. For information on adding certificates to the trust store file, see the *ssltrustmgr* manpage.

HP WBEM Services messages

The HP WBEM Services messages are listed in four groups: Syslog messages, standard CIM messages, command messages, and SSL errors.

General Syslog messages

HP WBEM Services puts the following messages in Syslog:

- When CIM Server starts up, it logs a message, for example:

  ```
  fsweb2 cimserver[1593]: PGS10026: The CIM Server is listening on
  HTTPS port 5989.
  ```

  ```
  fsweb2 cimserver[1593]: PGS10028: The CIM server is listening on
  the local connection socket.
  ```

  ```
  fsweb2 cimserver[1593]: PGS10030: Started HP-UX WBEM Services version
  A.02.09.10.
  ```

- When CIM Server shuts down, it logs a message, for example:

  ```
  fsweb2 cimserver[1593]: PGS10019: CIM server is stopped.
  ```

- When CIM Server receives a request to disable both HTTP and HTTPS connections, it logs a message, for example:

  ```
  Jun 17 13:58:42 mysystem cimserver[9624]: Neither HTTP nor HTTPS
  connection is enabled. CIMServer will not be started.
  ```

  You can disable both connections in the planned configuration, using `cimconfig`. However, default is HTTPS.

  You must restart the CIM Server for the planned configuration to take effect. (For example, enter: `cimserver enableHttpsConnection=TRUE`.) After starting the CIM Server, use `cimconfig` to set a port type in a more lasting way.

- On HP-UX, when `cimserverd` detects that `cimserver` is not running, but it was not shut down by the `cimserver -s` it logs a message, for example:

  ```
  Jun 17 20:55:18 mysystem cimserverd[6991]: cimserver not running,
  attempting restart
  ```

- If an error occurs in the process-to-process communication between the `cimserver` and `cimservera`, it logs a message, for example

  HP WBEM Services puts the following messages in Syslog:

  ```
  Dec 03 23:55:18 mysystem cimserverd[12517]: Error processing PAM
  Authentication request (OPERATION)
  ```

  where OPERATION could be on of: write, read, pipe, fork or dub2

Indication Service Syslog messages

- Message: `"One or more invalid Subscription instances were ignored"`

  This message might be logged upon CIM Server startup (IndicationService initialization), if an invalid Subscription instance is found in the repository.

  Invalid instances could exist if instances in the repository have been directly created or modified by circumventing the IndicationService.

  In such cases, the IndicationService detects such corruption, ignores invalid subscription instances, and continues to make a best effort at processing requests on valid subscription instances. You must remove invalid instances from the repository and be careful so that the invalid instances are not introduced into the repository by circumventing the IndicationService.

- Message: `"Subscription ($0) has no provider"`

  This message might be logged upon CIM Server startup (IndicationService initialization), if no provider, currently can serve an existing enabled subscription.

The substitution data $0 identifies the subscription, and contains the values of the subscription Filter and Handler Name properties in the form "FilterName, HandlerName".

This message might indicate that one or more indication providers has been removed or disabled, and you might have to re-install, re-register, and re-enable one or more indication providers to avoid missing indications.

- Message: `"Provider ($0) is now serving subscription ($1)"`

  This message might be logged upon a provider registration change (creation or modification of a PG_ProviderCapabilities instance), or when a provider has been enabled ("cimprovider -e" command).

  The substitution data $0 identifies the provider, and contains the value of the Provider Name property. The substitution data $1 identifies the subscription, and contains the values of the subscription Filter and Handler Name properties in the form "FilterName, HandlerName". This message indicates that additional indications can now be generated by the specified provider for the specified subscription.

- Message: `"Provider ($0) is no longer serving subscription ($1)"`

  This message might be logged upon a provider registration change (deletion or modification of a PG_ProviderCapabilities instance), or when a provider has been disabled ("cimprovider -d" command). The substitution data $0 identifies the provider, and contains the value of the Provider Name property.

  The substitution data $1 identifies the subscription, and contains the values of the subscription Filter and Handler Name properties in the form "FilterName, HandlerName". This message indicates that no indications will be generated by the specified provider for the specified subscription.

  Other indication providers might still be serving the specified subscription. You might have to re-install, re-register, and re-enable one or more indication providers to avoid missing indications.

Standard CIM messages

Each CIM exception has a message string. Additional message content can be after this standard code and format but that varies.

CIM Status Codes are defined by DMTF.

In addition to these error codes, a text description of the error is returned

Two lists of error messages follow. This first list is ordered by error number. The second list has the same messages, but they are ordered alphabetically.

Following the lists, two examples of a return with a CIM error are:

- 0 = CIM_ERR_SUCCESS

  The operation completed without error.

- 1 = CIM_ERR_FAILED

  A general error occurred that is not covered by a more specific error code.

- 2 = CIM_ERR_ACCESS_DENIED

  Access to a CIM resource was not available to the client.

- 3 = CIM_ERR_INVALID_NAMESPACE

  The target namespace does not exist.

- 4 = CIM_ERR_INVALID_PARAMETER

  One or more parameter values passed to the method were invalid.

- 5 = CIM_ERR_INVALID_CLASS
  The specified class does not exist.
- 6 = CIM_ERR_NOT_FOUND
  The requested object could not be found.
- 7 = CIM_ERR_NOT_SUPPORTED
  The requested operation is not supported.
- 8 = CIM_ERR_CLASS_HAS_CHILDREN
  Operation cannot be carried out on this class because it has subclasses.
- 9 = CIM_ERR_CLASS_HAS_INSTANCES
  Operation cannot be carried out on this class because it has instances.
- 10 = CIM_ERR_INVALID_SUPERCLASS
  Operation cannot be carried out because the specified superclass does not exist.
- 11 = CIM_ERR_ALREADY_EXISTS
  Operation cannot be carried out because an object already exists.
- 12 = CIM_ERR_NO_SUCH_PROPERTY
  The specified property does not exist.
- 13 = CIM_ERR_TYPE_MISMATCH
  The value supplied is not compatible with the type.
- 14 = CIM_ERR_QUERY_LANGUAGE_NOT_SUPPORTED
  The query language is not recognized or supported.
- 15 = CIM_ERR_INVALID_QUERY
  The query is not valid for the specified query language.
- 16 = CIM_ERR_METHOD_NOT_AVAILABLE
  The extrinsic method could not be executed.
- 17 = CIM_ERR_METHOD_NOT_FOUND
  The specified extrinsic method does not exist.

This list has the same messages as above; however, it is ordered alphabetically, and without the error number:

- CIM_ERR_ACCESS_DENIED
  Access to a CIM resource was not available to the client
- CIM_ERR_ALREADY_EXISTS
  Operation cannot be carried out because an object already exists
- CIM_ERR_CLASS_HAS_CHILDREN
  Operation cannot be carried out on this class because it has subclasses
- CIM_ERR_CLASS_HAS_INSTANCES
  Operation cannot be carried out on this class because it has instances
- CIM_ERR_FAILED
  A general error occurred that is not covered by a more specific error code

- CIM_ERR_INVALID_CLASS
  The specified class does not exist
- CIM_ERR_INVALID_NAMESPACE
  The target namespace does not exist
- CIM_ERR_INVALID_PARAMETER
  One or more parameter values passed to the method were invalid
- CIM_ERR_METHOD_NOT_AVAILABLE
  The extrinsic method could not be executed.
- CIM_ERR_METHOD_NOT_FOUND
  The specified extrinsic method does not exist.
- CIM_ERR_INVALID_QUERY
  The query is not valid for the specified query language.
- CIM_ERR_INVALID_SUPERCLASS
  Operation cannot be carried out because the specified superclass does not exist.
- CIM_ERR_NO_SUCH_PROPERTY
  The specified property does not exist.
- CIM_ERR_TYPE_MISMATCH
  The value supplied is incompatible with the type.
- CIM_ERR_NOT_FOUND
  The requested object could not be found.
- CIM_ERR_NOT_SUPPORTED
  The requested operation is not supported.

Examples of CIM responses

For example, consider a client requesting a createInstance operation on the PG_OperatingSystem class, when this operation is not supported by the Operating System provider. The requestor will receive the following response:

<?xml version="1.0" encoding="utf-8"?>

<CIM CIMVERSION="2.0" DTDVERSION="2.0">

<MESSAGE ID="53000" PROTOCOLVERSION="1.0"> <SIMPLERSP>

<IMETHODRESPONSE NAME="CreateInstance">

<ERROR CODE="7" DESCRIPTION="CIM_ERR_NOT_SUPPORTED: The requested operation is not supported: "OperatingSystemProvider does not support createInstance"/>

</IMETHODRESPONSE>

</SIMPLERSP>

</MESSAGE>

</CIM>

In the above example, you see these four components of the response:

1. CIM error code of 7
2. Translation to CIM_ERR_NOT_SUPPORTED

3. Expanded text message `The requested operation is not supported`
4. The non-standard additional message `OperatingSystem Provider does not support createInstance`

As a second example, consider a client that mistakenly provides too few or too many keys to a GetInstance operation on the PG_OperatingSystem class. The following response is sent:

<?xml version="1.0" encoding="utf-8"?>

<CIM CIMVERSION="2.0" DTDVERSION="2.0">

<MESSAGE ID="35002" PROTOCOLVERSION="1.0"> <SIMPLERSP>

<IMETHODRESPONSE NAME="GetInstance">

<ERROR CODE="4" DESCRIPTION="CIM_ERR_INVALID_PARAMETER: One or more parameter values passed to the method were invalid: "Wrong number of keys"/>

</IMETHODRESPONSE>

</SIMPLERSP>

</MESSAGE>

</CIM>

In the above example, you see these four components of the response:

1. CIM error code of 4
2. Translation to CIM_ERR_INVALID_PARAMETER
3. Expanded text message: `One or more parameter values passed to the method were invalid`
4. The non-standard additional message: `Wrong number of keys`

HP WBEM Services command messages

These messages come from the HP WBEM Services commands. They are written to stdout.

cimauth command messages

- Message: `You must have superuser privilege to run this command.`

  If you do not have `root` permissions `(uid=0)` on the local system, get a privileged user to give you permission. (See Chapter 3; see the *cimauth* manpage.)

- Message: `Failed to add authorizations. Please make sure that the authorization schema is loaded on the CIMOM.`

  Essential information is missing from the repository. For more information, see the "Maintaining the repository" (page 31).

- Message: `Failed to add authorizations. Specified user authorization already exists.`

  By default, the authorization is added. To modify user authorization, use the `-m` option. To remove user authorization, use the `-r` option.

- Message: `Failed to modify authorizations. Specified user authorizations were not found.`

  Enter `cimauth -l` to list all the authorizations. Locate the one you want to modify and verify that you have spelled it correctly. If it's not in the list, you must add it with the `-a` option, then re-issue the command.

- Message: `Failed to remove authorizations. Specified user authorizations were not found.`

  Enter `cimauth -l` to list all the authorizations. Locate the one you want to remove and verify that you have spelled it correctly. If it is not in the list, you need to add it with the `-a` option, then re-issue the command.

- Message: `CIM Server might not be running.`

  To see if cimserver is running, enter: `ps -ef|grep cimserver`

  Perhaps an operator stopped it by command, but did not restart it. To start it.

  HP-UX: `cimserver` (no options).

cimconfig command messages

- Message: `Current value of properties cannot be listed because the CIM Server is not running`

  Check for `cimserver` using `ps -ef|grep cimserver`. The server might not have started during installation, or someone might have stopped it with `cimserver -s` for HP-UX. You must restart the server by using the following:

  HP-UX: `cimserver` (no options).

- Message: `Failed to get property. Please make sure that the config schema is loaded in the CIM Server.`

  Essential information is missing from the repository. For more information, see the "Maintaining the repository" (page 31).

- Message: `Failed to set the config property. Please make sure that the config schema is loaded in the CIM Server.`

  Essential information is missing from the repository. For more information, see the "Maintaining the repository" (page 31).

- Message: `Failed to unset the config property. Please make sure that the config schema is loaded in the CIM Server.`

  Essential information is missing from the repository. For more information, see the "Maintaining the repository" (page 31).

- Message: `Failed to list the config properties. Please make sure that the config schema is loaded in the CIM Server.`

  Essential information is missing from the repository. For more information, see the "Maintaining the repository" (page 31).

- Message: `Specified property name was not found.`

  Check the spelling of the property name. Re-issue the command specifying a valid config property. For a list of properties, enter: `cimconfig -l`

- Message: `Specified property value is not valid.`

  See the `cimconfig` manpage for the range of allowed values for the property, and reissue the command with a valid value.

- Message: `Specified property cannot be modified.`

  You are trying to modify a property that is not dynamic. Dynamic properties can be changed immediately, while CIM Server is running.

  To modify a non-dynamic property you must modify the planned value, then stop and start CIM Server (with cimserver command). For more information, see the `cimconfig` manpage.

- Message: `Current value cannot be determined because the CIM Server is not running.`

  To see if cimserver is running, enter: ps -ef|grep cimserver

  Perhaps an operator stopped it by command, but did not restart it. To start it, do the following:

  HP-UX: `cimserver`

- Message: `Planned value cannot be determined because the CIM Server is not running.`

  To see if cimserver is running, enter: `ps -ef|grep cimserver`

  Perhaps an operator stopped it by command, but did not restart it. To start it, do the following:

  HP-UX: `cimserver (no options).`

- Message: `CIM Server might not be running.`

  To see if cimserver is running, enter: ps -ef|grep cimserver cimserver

  Perhaps an operator stopped it by command, but did not restart it. To start it do the following:

  HP-UX: `cimserver`

cimmof command messages

- Message: `Warning: class already in repository (OK to ignore)`

  The same class is already loaded, so you do not have to reload it. To replace this class, first delete it, and then load your new MOF file.

- `Message: Cannot connect to: mysystem: 5989. Command failed.`

  CIM Server is not running. An operator might have stopped the CIM Server. To restart it, enter `cimserver`. Then re-issue the `cimmof` command.

- Message: `Cannot open file <filename>.`

  Check the MOF file that you specified. The file could not be opened, it might not exist, the pathname might be incomplete, or there might be a typing error. Re-issue the command specifying a valid MOF file.

- Message: `Could not open include file <filename>.`

  Check the MOF include file that you specified. The file could not be opened, it might not exist, the pathname might be incomplete, or there might be a typing error. Reissue the command specifying a valid MOF file.

- Message: <*filename*>:<*lineNumber*>: parse error before 'string'.

  A parsing error occurred before 'string.' If it is your file, edit the invalid syntax, and then re-issue the command. If you received the file from a provider, contact the provider's support team.

- Message: `Error adding class <classname> to the repository: CIM_ERR_INVALID_SUPERCLASS: Operation cannot be carried out since the specified superclass does not exist.`

  The file you specified contains schema definition for a class with a superclass, but its superclass is not in the CIM Repository now. You must load the superclass *before* you load its subclasses.

6 Support and other resources

About this document

This document explains the architecture of HP WBEM Services for HP-UX. It also contains information on installing and administering HP WBEM Services in your environment. This document is intended for system administrators who are responsible for installing and administering HP WBEM Services. Readers of this document are expected to have knowledge on the following topics prior to using this document:

- Management applications such as HP Systems Insight Manager (HP SIM) and HP System Management Homepage (HP SMH)
- Basic knowledge of providers and clients that work with HP WBEM Services

New and changed information in this edition

The *HP WBEM Services for HP-UX system administrator guide* has been updated to the current versions that you are using in your environment. The information in this guide is applicable for HP WBEM Services version A.02.05 and later versions. Table 4 describes the printing history of the document.

Table 4 Printing History

Publishing Date	Part Number
March 2013	5900-2999
September 2011	5900-1802
April 2011	5900-1624
March 2011	B8465-90046
December 2003	B8463-90017
September 2003	B8463-90012
September 2002	B8463-90001

The printing date changes when a new edition is printed. (Minor corrections and updates which are incorporated at reprint do not cause the date to change.) The part number is revised when extensive technical changes are incorporated.

New editions of this manual incorporates all material updated since the previous edition.

HP encourages your comments

HP encourages your comments concerning this document. We are truly committed to providing documentation that meets your needs.

Send comments to docsfeedback@hp.com.

Please include document title, manufacturing part number, and any comment, error found, or suggestion for improvement you have concerning this document. Please also include what we did right so we can incorporate it into other documents.

Related information

In addition to this document, the following documents are available for HP WBEM Services:

- *HP WBEM Services Release Notes*
- *HP WBEM Service Software Development Kit Release Notes*
- *HP WBEM Services Software Developer's Kit for HP-UX Provider and Client Developer's Guide*

These documents are available at _www.hp.com/go/hpux-networking-docs and select HP-UX 11i WBEM Software collection.

A Representation of resources

The HP WBEM Services repository stores information about the managed resources.

To register with HP WBEM Services, a provider must define its resource by the classes and subclasses that define it. Then the provider must describe the properties that it will expose, and the methods that it will support.

The properties describe what a class is, the methods describe what it can do. Properties are attributes or characteristics of the resource. Methods are its actions, capabilities, or behaviors.

To make a request, the client must first identify, by its classes and subclasses, the resource it wants to manage.

The resource descriptions are done using object-oriented modeling. Object- oriented modeling represents real things in an abstract schema. Objects are arranged from most general to most specific. Many attributes of the more general parent are inherited by their more specific children.

Like object-oriented programming languages, the subclasses inherit the definitions of properties and methods from the parent class. Unlike some object-oriented programming, they do not inherit the implementations.

This section briefly describes basic concepts about object representation. As system administrator, you do not need to understand this to install HP WBEM Services or maintain it. However, it is the language that is used to explain resources. These are the terms that are used to describe what providers and clients do, and how resources can be managed.

For more information about object representation, see the tutorial at: http://www.dmtf.org/education/cimtutorial.php.

The schema is the most general abstraction that represents real things in the HP WBEM standard. A schema is a collection of classes. Each class in a schema can only belong to that schema. Each class name must be unique within a schema; a schema cannot have two classes with the same name.

The class is the basic modeling unit. It is a collection or set of objects that have similar properties and purposes. Each class defines a certain type of managed object, for example operating systems or system memory. Objects in the class contain properties (describing what it is) and methods (what it can do). A class can contain other classes (its subclasses). It can also contain instances.

Subclasses are grouped by similarities. Subclasses inherit properties and methods from their parent (their superclass), and can also add their own local properties and methods. Subclasses are classes and they can have their own subclasses.

CIM_SoftwareElement, for example, is a class. It has several subclasses, like HPUX_SoftwareElement, Win32_SoftwareElement, and so on.

An instance can be a discrete occurrence of any object, such as your computer's hard drive or the printer on your desk. It is the specific member of the hierarchy. An instance cannot have any subclasses. All instances in a class share the same properties and methods. Each instance has a unique name (see key properties).

Methods are the behaviors of the class, for example, the OperatingSystem class has a Reboot method and a printer has an EnableDevice method to put it online. However, not all classes have methods.

An intrinsic method models a CIM operation. Standard intrinsic methods (such as enumerateInstances, getInstance, modifyInstance) are relevant to all classes.

An extrinsic method is defined on a CIM Class in some Schema that is unique to that class.

Properties are the attributes of a class. For example, there is a ParticipatingCS association exists between a CIM_ComputerSystem and a CIM_Cluster. This association has two properties, RoleOfNode and StateOfNode, to describe attributes of the ComputerSystem as a node within the Cluster.

Key properties (one or more properties defined with a "key" qualifier) are identifiers. Keys in classes and subclasses provide a way to uniquely identify the instance that inherits them. All instances inherit a key, or a set of keys, from their superclass. The value that the instance gives

these keys is its own identification. It is the only instance in its namespace that is allowed to have that “name.” More than one key property is a compound key.

Consider how to uniquely identify a user account on a UNIX system. You can use two key properties: the value of the user account’s Name property and the value of the system’s Name property. Also, you can identify with the pair used to route your email to you: user-name@domain-name.

Classes are either concrete or abstract. A concrete class (like CIM_Operating System) has real instances, particular computer systems. A concrete class must have at least one key property. An abstract class like CIM_ManagedElement cannot have any instances, and it is not required to have key properties. Its subclasses can have keys as they get more specific.

Associations can be defined between classes. For example, there is a ParticipatingCS association exists between CIM_ComputerSystem (the entire computer system) CIM_Operating System (the OS software that exists on that system).

The association is a class, so it can have properties and methods. For example, two properties of ParticipatingCS are RoleOfNode and StateOfNode.

Namespaces can give you a logical way to group things, in order to control their scope and visibility. A namespace is not a physical location; it is more like a logical database containing specific classes and instances. Namespace grouping can be used to separate instances and make sure no collisions occur with others of the same name. Namespaces also can be used to limit access.

HP WBEM Services installs with four predefined namespaces.

- root (in /root directory): The root namespace exists to conforms to the DMTF specifications.
- root#cimv2 (in /root/cimv2): The standard CIM schemas go here. Also, the schemas for the bundled providers.
- root#PG_Interop (in /root/PG_Interop): This is for provider registration. This space is reserved exclusively for providers, and all providers must register here. (See cimprovider manpage.)
- root#PG_Internal (in /root/PG_Internal): This is a private space, for use by HP WBEM Services only.

B Sample client request

This appendix provides a sample of a client request and the response.

The request is for the `EnumerateInstances` operation on the `PG_OperatingSystem` class.

Requests and responses are encoded in XML. For more information about XML, see http://www.dmtf.org/standards/WBEM.

The information is represented in a table format. The first column has line numbers for the actual request and response. The middle column can group several related lines. The right-hand column is a comment on the corresponding middle column.

The first part is the request which spans to about 16 lines. The request is followed by the response, which is actually 172 lines long, but lines 81 to 170 have been omitted for brevity.

Example request

Table 5 EnumerateInstances Request for PG_OperatingSystem Class

1	`<?xml version="1.0" ?>`	Begin specifying that this is an XML-encoded CIM message. (See end at line 15 and 16)
2	`<CIM CIMVERSION="2.0" DTDVERSION="2.0">`	
3	`  <MESSAGE ID="51000" PROTOCOLVERSION="1.0">`	
4	`    <SIMPLEREQ>`	This is a simple request for the operation: method `EnumerateInstances`
5	`      <IMETHODCALL NAME="EnumerateInstances">`	
6	`        <LOCALNAMESPACEPATH>`	Line 6 begins (and 9 ends) specifying the `/root/cimv2` namespace for the CIM operation
7	`          <NAMESPACE NAME="root"/>`	
8	`          <NAMESPACE NAME="cimv2"/>`	
9	`        </LOCALNAMESPACEPATH>`	
10	`        <IPARAMVALUE NAME="ClassName">`	Line 10 begins (and 12 ends) specifying the class name (required) for `EnumerateInstances: PG_OperatingSystem`
11	`          <CLASSNAME NAME="PG_OperatingSystem"/>`	
12	`        </IPARAMVALUE>`	
13	`      </IMETHODCALL>`	Ending of the method call and simple request.
14	`    </SIMPLEREQ>`	
15	`  </MESSAGE>`	Ending of the CIM operation request message.
16	`</CIM>`	

- Lines 1-3: This is checked when the request comes to the HTTP Server. At this point, several things have to happen to continue:
  - The client must be able to connect to the system on the authorized port.
  - CIM Server must be running.
  - The user/password pair must pass authorization.
  - The request must have a properly formed header.
  - When the request is parsed, it must not contain xml errors.
- Lines 4 and 5: At this point, HP WBEM Services considers the operation that is requested. If it is a supported operation, the process continues.

- Lines 6 - 9: Two criteria must be met to continue:
  - This namespace must be valid.
  - If `enableNamespaceAuthorization` property is enabled, this user must be authorized to access this namespace
- Lines 10 - 12: The classname must exist, and it must have a provider registered. The provider must respond to the request. Here, the OS Provider is registered for the `PG_OperatingSystem` class. Checking the provider documentation, you can see that it supports the `EnumerateInstances`method.

Now it is up to the provider to process the request and send a response. If the resource does not respond, HP WBEM Services will send a message to the client. If the resource sends its own error, HP WBEM Services will pass this on to the client in its response. Often, these messages will be appended to a standard CIM error.

Example response

The table shows the response to the request to `EnumerateInstances` for `PG_Operating System`.

The return value is a named instance. Named instances include both INSTANCENAME (the instance with its key properties) and INSTANCE (*all* the properties). Because this instance has so many properties, some of them have been omitted from the example text.

Table 6 EnumerateInstances Response for PG_OperatingSystem Class

1	`<?xml version ="1.0" encoding="utf-8"?>`	Lines 1 - 3 indicate this is an XML-encoded message. (See end at lines 171 and 172.)
2	`<CIM CIMVERSION="2.0" DTDVERSION="2.0">`	
3	`<MESSAGE ID="51000" PROTOCOLVERSION="1.0"`	
4	`<SIMPLERSP>`	This is simple response to Enumerate Instances method
5	`<IMETHODRESPONSE NAME="EnumerateInstances">`	
6	`<IRETURNVALUE>`	Return value is named instance (*all* properties)
7	`<VALUE.NAMEDINSTANCE>`	
8	`<INSTANCENAME CLASSNAME="PG_OperatingSystem">`	Begin *keys* of class name
9	`<KEYBINDING NAME="CreationClassName"`	One key for this instance. It is CreationClassName, a string, and its value is "CIM_Operating System"
10	`<KEYVALUE VALUETYPE="string">`	
11	`CIM_OperatingSystem`	
12	`</KEYVALUE>`	
13	`</KEYBINDING>`	
14	`<KEYBINDING NAME="CSCreationClassName"`	Next key is CSCreationClassName, a string, with value "CIM_UnitaryComput erSystem"
15	`<KEYVALUE VALUETYPE="string">`	
16	`CIM_UnitaryComputerSystem`	
17	`</KEYVALUE>`	
18	`</KEYBINDING>`	
19	`<KEYBINDING NAME="CSName">`	The next key is CSName, also a string, with value "mycomputer.hp.com"
20	`<KEYVALUE VALUETYPE="string">`	
21	`mycomputer.hp.com`	

Table 6 EnumerateInstances Response for PG_OperatingSystem Class *(continued)*

22	</KEYVALUE>	
23	</KEYBINDING>	
24	<KEYBINDING NAME="Name">	The next key is Name, also a string, with the value of "HP-UX"
25	<KEYVALUE VALUETYPE="string"	
26	HP-UX	
27	</KEYVALUE>	
28	</KEYBINDING>	
29	</INSTANCENAME>	End of keys for instance
30	<INSTANCE CLASSNAME="PG_OperatingSystem">	Begin all *properties* of instance
31	<PROPERTY NAME="CSCreationClassName" TYPE="string">	First key property is CSCreationClassName, a string, with value = "CIM_UnitaryComputerSystem"
32	<VALUE>	
33	CIM_UnitaryComputerSystem	
34	</VALUE>	
35	</PROPERTY>	
36	<PROPERTY NAME="CSName" TYPE="string">	Next key property
37	<VALUE>	
38	mycomputer.hp.com	
39	</VALUE>	
40	</PROPERTY>	
41	<PROPERTY NAME="CreationClassName" TYPE="string">	Next key property
42	<VALUE>	
43	CIM_OperatingSystem	
44	</VALUE>	
45	</PROPERTY>	
46	<PROPERTY NAME="Name" TYPE="string">	Next key property
47	<VALUE>	
48	HP-UX	
49	</VALUE>	
50	</PROPERTY>	
51	<PROPERTY NAME="Caption" TYPE="string">	
52	<VALUE>	Next property
53	The current Operating System	
54	</VALUE>	
55	</PROPERTY>	
56	<PROPERTY NAME="Description" TYPE="string">	
57	<VALUE>	

Table 6 EnumerateInstances Response for PG_OperatingSystem Class *(continued)*

58	This instance reflects the Operating System on which the CIMOM is executing (as distinguished from instances of other installed operating systems that could be run).	Next property
59	</VALUE>	
60	</PROPERTY>	
61	<PROPERTY NAME="Status" TYPE="string">	Next property
62	<VALUE>	
63	Unknown	
64	</VALUE>	
65	</PROPERTY>	
66	<PROPERTY NAME="OSType" TYPE="unint16">	Next property (unsigned integer, 16 bit) (DMTF specifies that 8 = HP-UX)
67	<VALUE>	
68	8	
69	</VALUE>	
70	</PROPERTY>	
71	<PROPERTY NAME="LastBootUpTime" TYPE="datetime">	Next property (datetime data type)
72	<VALUE>	
73	2010924091618.000000-420	
74	</VALUE>	
75	</PROPERTY>	
76	<PROPERTY NAME="CurrentTimeZone" TYPE="sint16">	Next property (signed integer, 16 bit)
77	<VALUE>	
78	-420	
79	</VALUE>	
80	</PROPERTY>	
	... Several properties of the instance were removed from this example. ...	
171	</INSTANCE>	End of this instance properties
172	</VALUE.NAMEDINSTANCE>	End of named instance
173	</IRETURNVALUE>	End return value
174	</IMETHODRESPONSE>	End method response
175	</SIMPLERSP>	End simple response
171	</MESSAGE>	End message
172	</CIM>	End CIM XML message

Glossary

C

CIM (Common Information Model) A hierarchical object-based model developed by the DMTF that defines a large number of concepts common to most computer systems.

CIM Client A client application that issues CIM operation requests over HTTP and processes the responses.

CIM Object Manager (CIMOM) Manages CIM objects in an HP WBEM-enabled system. CIMOM receives and processes CIM operation requests and issues responses.

CIM Object Manager repository A central storage area managed by the Common Information Model Object Manager (CIM Object Manager). This repository contains the definitions of classes and instances that represent managed objects and the relationships among them.

CIM schema A collection of class definitions used to represent managed objects that occur in every management environment. Also see core model, common model, and extension schema.

cipher A key-selected transformation between plain text and cipher text. With a good cipher, the secret information inside the cipher remains hidden, even when the cipher text is stored or transmitted.

Class A collection of instances, all of which support a common type; that is, a set of properties and methods. The common properties and methods are defined as features of the class. For example, the class called Modem represents all the modems present in a system.

Common Information Model (CIM) A common data model of an implementation-neutral schema for describing overall management information in a network/enterprise environment.

CIM is comprised of a Specification and a Schema. The Specification defines the details for integration with other management models defined by the DMTF, such as SNMPs MIBs or the DMI's MIFs. The Schema provides the actual model descriptions.

Common Information Model Object Manager (CIM Object Manager) A component in the CIM management infrastructure that handles the interaction between management applications and clients.

common model The second layer of the CIM schema, which includes a series of domain-specific but platform-independent classes. The domains are systems, networks, applications, and other management-related data. The common model is derived from the core model. Also see extension schema.

core model The first layer of the CIM schema, which includes the top-level classes and their properties and associations. The core model sets the conceptual framework for the schema of the rest of the managed environment. Systems, applications, networks and related information are modeled as extensions to the core model.

The core model is both domain- and platform-independent. Also see common model and extension schema.

D

Desktop Management Interface (DMI) Desktop Management Interface is an initiative by the DMTF. The DMI enables desktop computers, hardware and software products, and peripherals, whether they are standalone systems or linked into networks to be manageable. It enables them to communicate their system resource requirements and to coexist in a manageable PC system. The DMI is independent of operating system and processor, and enables the development of manageable PC products and applications across platforms.

Desktop Management Task Force (DMTF) An industry-wide consortium committed to making computing devices easier to use, understand, configure, and manage. For more information, see http://www.dmtf.org.

domain The class to which a property or method belongs. For example, if status is a property of Logical Device, it is said to belong to the Logical Device domain.

E

extensible markup language (XML) A simplified subset of SGML that offers powerful and extensible data modeling capabilities. An XML Document is a collection of data represented in XML. An XML Schema is a grammar that describes the structure of an XML Document.

extension schema The third layer of the CIM schema, which includes platform-specific extensions of the CIM schema such as Microsoft Windows NT, UNIX, and Microsoft ExchangeServer. Also see common model and core model.

extrinsic method A method defined on a CIM Class in some Schema that is unique to that class (versus intrinsic methods which apply across all classes). Also see intrinsic method.

H

HP WBEM (Web-Based Enterprise Management) An initiative based on a set of management and Internet standard technologies developed to unify the management of enterprise computing environments. HP WBEM provides the ability for the industry to deliver a well-integrated set of standard-based management tools leveraging the emerging technologies such as CIM and XML.

HP WBEM Services A Hewlett-Packard product that uses WBEM to manage HP-UX system resources.

HTTP (Hypertext Transfer Protocol) An application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic stateless protocol that can be used for many tasks through extensions of its request methods, error codes and headers.

HTTP Server HP WBEM Services uses a small-footprint special-services "light-weight" server that processes HTTP requests and returns standard HTTP responses. The server is not intended as a replacement for a web server. The server does not serve up HTML web pages and does not run CGI applications.

I

indication An operation executed as a result of some action such as the creation, modification, or deletion of an instance, access to an instance, or modification or access to a property. Indications can also result from the passage of a specified period of time. An indication typically results in an event.

inheritance The relationship that describes how classes and instances are derived from parent classes, or superclasses. A class can spawn a new subclass, also called a child class. A subclass contains all the methods and properties of its parent class.

Inheritance is one of the features that enables the CIM classes to function as templates for actual managed objects in the CIM environment.

Insight Remote Support (IRS) A software solution that monitors managed systems, detect events, and transmits the data to HP for analysis.

instance A representation of a real-world managed object that belongs to a particular class, or a particular occurrence of an event. Instances contain actual data.

instance provider A type of provider that supports instances of system- and property-specific classes. Instances providers can support data retrieval, modification, deletion, enumeration, or query processing. Instance providers can also invoke methods Also see class provider and property provider.

intrinsic method A method defined for the purpose of modeling a CIM operation. Standard intrinsic methods (such as enumerateInstances, getInstance, modifyInstance) are relevant to all classes. Also see extrinsic method.

K

Kerberos A security mechanism that provides authentication, data integrity, data privacy, and mutual authentication. (Available through PAM in HP-UX)

key A property that is used to provide a unique identifier for an instance of a class. Key properties are marked with the Key qualifier. A compound key has more than one property, with a Key qualifier.

key qualifier A qualifier that must be attached to every property in a class that serves as part of the key for that class.

L

light-weight HTTP server A small footprint server that processes HTTP requests and returns standard HTTP responses. The server is not intended as a replacement for a web server. The server does not serve up HTML web pages and does not run CGI applications.

local property A non-system property defined for a class but not inherited from a superclass.

M

managed object A hardware or software system component that is represented as an instance of the CIM class. Information about managed objects is supplied by data and event providers, as well as by the CIM Object Manager.

managed object format (MOF) A compiled language for defining classes and instances. A MOF compiler takes information from a .mof formatted text file and adds the data to the CIM Object Manager repository. MOF eliminates the need to write code, thus providing a simple and fast technique for modifying the CIM Object Manager repository. DMTF makes their schemas available as MOF files.

management application An application or service that uses information originating from one or more managed objects in a managed environment. Management applications retrieve this information and perform operations through calls to the CIM Object Manager from the CIM Object Manager.

management information base (MIB) A database of managed objects, written in text.

management information format (MIF) database Part of DMI that stores and manages information and passes it to management applications on request. MIFs define the standard manageable attributes of PC products in categories including PC systems, servers, printers, LAN adapters, modems, and software applications.

Management Interface (MI) The MI enables DMI-enabled applications to access, manage and control desktop systems, components and peripherals.

metamodel A CIM component that describes the entities and relationships representing managed objects. For example, classes, instances, and associations are included in the metamodel.

metaschema The metaschema is a formal definition of the model. It defines the terms used to express the model and its usage and semantics.

method

1. A function describing the behavior of a class. Including a method in a class does not guarantee an implementation of the method. The Implemented qualifier is attached to the method to indicate that an implementation is available for the class.
2. A function included in a CIM Object Manager API interface.

MOF file A text file that contains definitions of classes and instances, using Managed Object Format (MOF) formatting.

multiple inheritance The ability of a subclass to derive from more than one superclass.

N

named element An entity that can be expressed as an object in the meta schema.

namespace A unit for grouping classes and instances to control their scope and visibility. Namespaces are not physical locations; they are more like logical databases containing specific classes and instances. Objects located within a namespace must have unique names (specified by one or more key values) within that namespace. Objects in a different namespaces can be unique even if they have the same keys, because the two objects reside in separate namespaces.

O

object path A formatted string used to access namespaces, classes, and instances. Each object on the system has a unique path which identifies it locally or over the network. Object paths are conceptually similar to Universal Resource Locators (URL).

Open Database Connectivity (ODBC) A specification for an API that defines a standard set of routines with which an application can access data in a data source.

operational semantics The formalization of real objects by putting them into a common language.

override Indicates that the property, method, or reference in the derived class overrides the similar construct in the parent class in the inheritance tree or in the specified parent class.

P

PAM (Pluggable Authentication Model) A product that coordinates user authentication tools for system security.

property A name or value pair that describes a unit of data for a class. Property names cannot begin with a digit and cannot contain white space. Property values must have a valid Managed Object Format (MOF) data type.

property provider A type of provider that supports the retrieval and modification of the CIM properties.

provider An executable that can return and/or set information, execute methods, generate indications, or respond to other requests regarding a given managed object.

provider data sheet (PDS) Provides basic provider information to software professionals who will design, implement, enhance, and support client applications that will use this provider. It contains information about what this provider does, what interfaces it uses, how to install it and what platforms and operating systems are supported.

provider registration A provider needs to register with the CIMOM so that the CIMOM will know what properties and methods are supported. A special object is created during registration to relate the information about the provider to the classes in the CIM schema that it supports.

Q

qualifier A modifier containing information that describes a class, an instance, a property, a method, or a parameter.

R

reference A special string property type that is marked with the reference qualifier, indicating that it is a pointer to other instances.

repository This repository contains the definitions of classes and instances that represent managed objects and the relationships among them. The HP WBEM Services repository is not available for use by clients or providers for static or persistent data storage. Also see CIM Object Manager repository.

required property A property that must have a value.

S

schema A collection of class definitions that describe managed objects in a particular environment.

Simple Network Management Protocol (SNMP) A protocol of the Internet reference model used for network management.

standard schema A common conceptual framework for organizing and relating the various classes representing the current operational state of a system, network, or application. The standard schema is defined by the Desktop Management Task Force (DMTF) in the Common Information Model (CIM).

subclass A class that is derived from a superclass. The subclass inherits all features of its superclass, but can add new features or redefine existing ones.

subschema A part of a schema owned by a particular organization. The Win32 schema is an example of a subschema.

superclass The class from which a subclass inherits.

W

web server Full-service web servers act as HTTP servers. In addition, they have many other capabilities, like running CGI scripts. Understanding the distinction between a limited-service HTTP server and a full-service Web server is critical to understanding security on HP WBEM Services for HP-UX. HP WBEM Services uses its own embedded HTTP server (a light-weight server), not a web server.

Acknowledgement: This information was gathered from: http://dmtf.org/education/cimtutorial.php, and more information is available there.

Index