

HP WBEM Services Version A.02.00, Release Notes

HP-UX



**Manufacturing Part Number: B8465-90030
September 2006**

U.S.A.

© Copyright 2006 Hewlett-Packard Development Company, L.P. All rights reserved.

Legal Notices

© Copyright 2006 Hewlett-Packard Development Company, L.P.

The HP WBEM Services SDK is the software developer's kit for the HP WBEM Services product. It provides application developers with the tools they need to develop CIM client applications and provider modules for HP WBEM Services that are products of Hewlett-Packard Company, L. P., and all are protected by copyright.

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

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

This product includes software developed by The Open Group OpenPegasus Project Copyright (c) 2000, 2001, 2002 BMC Software; Hewlett-Packard Development Company, L. P.; IBM Corp.; The Open Group; Tivoli Systems. Copyright (c) 2003 BMC Software; Hewlett-Packard Development Company, L. P.; IBM Corp.; EMC Corporation; The Open Group. Copyright (c) 2004 BMC Software; Hewlett-Packard Development Company, L. P.; IBM Corp.; EMC Corporation; VERITAS Software Corporation; The Open Group. Copyright (c) 2006 Hewlett-Packard Development Company, L. P.; IBM Corp.; EMC Corporation; VERITAS Software Corporation; The Open Group.

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

1 HP WBEM Services Version A.02.00, Release Notes

Announcement

The following information is for Version A.02.00 of HP WBEM Services.

HP WBEM Services for is available from <http://software.hp.com>.

As the HP-UX implementation of the DMTF WBEM standard, the HP WBEM Services product enables management solutions that deliver increased control of enterprise resources at reduced cost. WBEM (Web-Based Enterprise Management) is a platform and resource-independent DMTF (Distributed Management Task Force) standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.

WBEM is defined by the following standards:

- **Common Information Model (CIM):** CIM is an object-oriented information model for describing managed resources. A CIM object is a representation of a managed resource. CIM objects with similar properties and purposes are represented as CIM classes. A CIM instance is a representation of a managed object that belongs to a particular class. CIM objects can be shared by any WBEM-enabled system or applications. The definitions of CIM classes are grouped into meaningful collections called schemas.

MOF (Managed Object Format) is the language for defining CIM classes and instances. MOF files are ASCII files that use the MOF language to describe CIM objects.
- **Representation of CIM in XML:** XML (eXtensible Markup Language) is a markup language for describing data on the web. The DMTF defines a standard for the representation of CIM elements and messages in XML. Because CIM-XML provides a standard way of describing data, any WBEM client can access CIM data on any WBEM-enabled system.
- **CIM Operations over HTTP:** The CIM Operations over HTTP Specification defines the way HTTP (HyperText Transfer Protocol) is used to transport the CIM information.

System Administrators benefit from the deployment of HP WBEM Services in the reduced cost and greater choice in operating homogeneous and heterogeneous IT environments. HP WBEM Services further supports HP's efforts to deliver multi-platform, multi-operating system management tools that leverage the existing training and knowledge base of today's IT staff, while positioning for heterogeneous environments that may be part of your IT plans. In homogeneous environments, WBEM still offers the advantages of exposing management information and capabilities in a standard way, regardless of architecture or platform specifics (for example, PA-RISC and IPF).

The product includes a set of providers that allow management applications to access information about managed resources in the operating environment.

HP WBEM Services makes it easier for software developers to create management applications that manage HP-UX systems, and makes HP Servers and workstations easier for system administrators to manage.

The following version of the HP WBEM Services product is now being made available:

For HP-UX: B8465BA A.02.00.11

What's in This Version

HP WBEM Services Version A.02.00.11 is now being released.

WBEM Services Version A.02.00.11 is an update to support HP-UX 11i v1 and HP-UX 11i v2 including defect fixes and improvements in efficiency.

WARNING **An upgrade of an HP-UX Operating System for which the version of HP WBEM Services reverts to an earlier version is not supported. For instance, an HP-UX Operating System upgrade from 11i v1 0412 to 11i v2 0409 is NOT supported, as the version of HP WBEM Services would be going from A.02.00.05 to A.02.00.04**

Table 1-1 Support for HP-UX Matrix

WBEM Version	HP-UX
A.02.00	11i v1
A.02.00.02	11i v1
A.02.00.04	11i v1 11i v2
A.02.00.05	11i v1 11i v2
A.02.00.07	11i v1 11i v2
A.02.00.08	11i v1 11i v2
A.02.00.09	11i v1 11i v2
A.02.00.10	11i v1 11i v2
A.02.00.11	11i v1 11i v2

HP WBEM Services Version A.02.00 product contains the following:

- Refer to table 1-1 for WBEM version and OS information
- Support for WBEM Indications
- The HP WBEM Services run-time environment
 - Binary command line executables
 - Shared libraries
 - Configuration files
 - CIM schemas
- Packaged Provider Modules

What's in This Version

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

To install any A.02.00 Version, use the instructions contained in these Release Notes.

Product Documentation

- *HP WBEM Services Administrator's Guide, Second Edition* B8465-90017 available from <http://docs.hp.com/en/netsys.html>.
- Release Notes for this version and for previous versions of HP WBEM Services are available from <http://docs.hp.com/en/netsys.html>.

After installation, refer to the man pages for your system. Man pages are summarized in the Administrator's Guide.

For more information about DMTF, WBEM, and CIM standards, go to <http://www.dmtf.org>.

Security

HP WBEM Services supports four connection points

- HTTP port
- HTTPS (HTTP Secure) port
- HTTPS port for Export Connections
- a Unix domain socket for local connections

HP WBEM Services uses dedicated ports for CIM-XML traffic. The 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 TCP/IP communication) is dedicated for CIM-XML communication between the Indication sender and the CIM Server (Indication receiver). The HTTP and the two HTTPS connection points may be disabled using the `cimconfig` command line utility. However, the Unix domain socket connection is always enabled when the CIM Server is running.

SSL Support

With HTTPS connections enabled, HP WBEM Services uses SSL (Secure Sockets Layer) for all communications, with server-side certificates that are trusted by the management application. HP WBEM Services uses OpenSSL to support HTTPS connections. OpenSSL is an open source 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, go to <http://www.openssl.org>.

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`. Be sure 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.

Local User Authentication

The CIM Server automatically authenticates local connections - that is connections established using the `connectLocal` method in the CIMClient interface. This eliminates the need for the user to specify a 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

For remote users (users on a system sending requests to HP WBEM Services running on another system), CIM Server authenticates the user with a request/challenge mechanism using HTTP Basic Authentication.

HP WBEM Services uses **Pluggable Authentication Modules (PAM)** to authenticate the user.

NOTE 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. WBEM Services will default 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. See example below. For additional information, please refer to the `pam(3)` and `pam.conf(4)` man pages.

```
#
# 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
```

NOTE

HP-UX now uses the `cimservera` executable in HP WBEM Services. Refer to the Administrator's Guide (part number B8465-90017, chapter 3) for more information.

Certificate Verification

CIM Clients

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

wbemexec Client

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

For more information about the `wbemexec` command, see the `wbemexec` man page.

`wbemexec` uses trust store for server certificate verification. Be sure to import the certificate in `/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 into the Trust Store*, below.

`wbemexec`'s SSL connection to CIM Server will fail if the server certificate is not found and verified in the trust store.

`wbemexec` is not recommended for use in high-threat environments because `wbemexec` does not do any additional certificate verifications, such as host-name or certificate-depth verification.

Managing Certificates

During the install process, if `/etc/opt/hp/sslshare/cert.pem` and/or `/etc/opt/hp/sslshare/file.pem` files are found on the system, the following messages will be 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` may have been created by an earlier installation of HP WBEM Services A.02.00 or an installation of other management applications on the system. These files will not be overwritten.

HP-UX example:

Here are two examples of updating certificates when an earlier version of HP WBEM Services was already installed:

- Scenario 1: Using the default installed certificates from WBEM Services Version A.01.05:

It is recommended that after installing HP WBEM Services Version A.02.00, you do the following:

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

OR

— 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 systems, then the certificate in new `/etc/opt/hp/sslshare/cert.pem` should be copied over to the trust store on those other systems replacing the earlier certificate.

NOTE	Use the <code>ssltrustmgr</code> command to add or remove certificates in a trust store. For more information about the <code>ssltrustmgr</code> command, see the <code>ssltrustmgr</code> man page.
-------------	--

Security

- Scenario 2: Using custom certificates:

If using either self-signed or root-signed 512-bit or 1024-bit encryption certificates, it is strongly recommended that you create new certificates with 2048-bit encryption.

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

Importing Server Certificates to the Trust Store

CIM client applications should maintain a trust store in a `<trust_store-name>.pem` file. CIM client applications must import the certificates stored in `/etc/opt/hp/sslshare/cert.pem` into a trust store file on the client machine from various CIM server machines (ones the client wants to connect to).

With C++ CIM client libraries, the trust store should be in 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 <code>/etc/opt/hp/sslshare/file.pem</code> , copy only the public certificate in the <code>/etc/opt/hp/sslshare/cert.pem</code> file.
-------------	--

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

NOTE	The <code>wbemexec</code> command uses the file <code>/etc/opt/hp/sslshare/client.pem</code> as its trust store. Import the server certificates for this client into the <code>/etc/opt/hp/sslshare/client.pem</code> file.
-------------	---

3. Use `ssltrustmgr` command to delete a certificate from the trust store.

Standards Conformance

This version of the HP WBEM Services product complies with the following standards:

- CIM Operations over HTTP, Version 1.1
- Representation of CIM in XML, Version 2.1
- CIM Specification, Version 2.2
- CIM Schema, Version 2.7

For more information about the DMTF WBEM and CIM standards, go to:
<http://www.dmtf.org>.

Compatibility Information and Installing Requirements

- HP-UX 11i v1 or 11i v2 must be installed before installing HP WBEM Services A.02.00.xx.

Table 1-2 Software requirements and OS platform/version compatibility:

HP-UX Version	WBEM Version
11i v1	A.02.00, A.02.00.02, A.02.00.04, A.02.00.05, A.02.00.07, A.02.00.08, A.02.00.09, A.02.00.10, and A.02.00.11
11i v2	A.02.00.04, A.02.00.05, A.02.00.07, A.02.00.08, A.02.00.09, A.02.00.10, and A.02.00.11

WARNING An upgrade of an HP-UX Operating System for which the version of HP WBEM Services reverts to an earlier version is not supported. For instance, an HP-UX Operating System upgrade from 11i v1 0412 to 11i v2 0409 is NOT supported, as the version of HP WBEM Services would be going from A.02.00.05 to A.02.00.04

OpenSSL must be installed before installing HP WBEM Services version A.02.00.04 and beyond. Versions of HP WBEM Services prior to A.02.00.04 contained the necessary OpenSSL files.

NOTE As updates to OpenSSL become available and installed over time, the HP WBEM Services cimserver process must be shutdown and restarted in order to run against any new version of OpenSSL. Please see the HP WBEM Services System Administrator's Guide for more information on shutting down and restarting the cimserver.

- On 11i v2 systems:
 - If Instant Capacity (B9073BA) is installed, the version of B9073BA must be B.11.23.06.03 or greater.
 - If nPar WBEM provider (NPar) is installed, the version of NPar must be B.11.23.01.03 or greater. In addition, PHCO_31559 must be installed. This patch contains updates to the NPar commands.

Disk space required to install:

HP WBEM Services requires the following disk space to install:

/	5 MB
/opt	79 MB
/var	86 MB
/usr	1 MB

Depending on the number of CIM objects to be stored in the CIM Repository, additional disk space may 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 communications between CIM clients and the CIM Server. One port is dedicated for CIM-XML communications between Indication sender and 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 in the `/etc/services` file.

Installing HP WBEM Services

You need to log in to the system as root (uid=0) to install the HP WBEM Services software. Software is available in Software Depot (SD) format as a single SD depot. Before installing the software, be sure your system meets the software and hardware requirements described in the section titled “Compatibility Information and Installing Requirements.”

To install the software, download the product from <http://software.hp.com>. Copy the downloaded depot file to a local directory on your system, then run the HP-UX `swinstall` command and follow the instructions to install the software from the depot.

The filesets that make up the HP WBEM Services product are:

- WBEM-CORE, A.02.00.xx - WBEM Services core
- WBEM-CORE-COM, A.02.00.xx - WBEM Services core
- WBEM-MAN, A.02.00.xx - WBEM Services man pages
- WBEM-MX, A.02.00.xx - Reserved

To verify that the software is installed correctly, enter the HP-UX `swverify` command at the end of the install (a `Verification succeeded` message from `swverify` indicates that the software has been installed correctly): `swverify B8465BA`

The following files are installed. Do not move these files!

<code>/etc/opt/wbem</code>	(directory)
<code>/etc/opt/wbem/mof</code>	MOF files
<code>/opt/wbem</code>	(directory)
<code>/opt/wbem/bin</code>	commands, executables
<code>/opt/wbem/lib</code>	shared libraries
<code>/opt/wbem/mx</code>	reserved
<code>/opt/wbem/providers/lib</code>	links to shared libraries for providers
<code>/opt/wbem/sbin</code>	commands and executables that only root user can run
<code>/opt/wbem/share/man</code>	man pages
<code>/var/opt/wbem</code>	configuration files, CIM repository, log files, etc.
<code>/etc/opt/hp/sslshare</code>	shared SSL certificate files and trust store files.

NOTE Upon a re-install of the product, any existing repository in `/var/opt/wbem/repository` will be moved to `/var/opt/wbem/prev_repository` before building a new repository. HP WBEM Services Version A.02.00 upgrades the `/root/cimv2` namespace to CIM v2.7.

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

For HP-UX, there are 7 providers bundled with HP WBEM Services. These providers are:

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

Installing HP WBEM Services

For HP-UX 11i v1, the Computer System, Operating System, Process, and IP providers are registered automatically at installation.

However, you must explicitly register these three providers:

- 1) Domain Name Service provider
- 2) Network Time Protocol provider
- 3) Network Information Service provider

The command to register these three providers is (all on one line): `/opt/wbem/bin/cimmof -I /etc/opt/wbem/mof -n root/PG_InterOp /etc/opt/wbem/mof/HPUX_ManagedSystemSchemaR.mof`

NOTE For HP-UX 11i v1, these three providers are NOT automatically registered because you must install a patch first. See *Required and Recommended Patches* below.

NOTE For HP-UX 11i v2, these three providers ARE automatically registered for you.

Running the HP WBEM Services CIM Server

After installation, the HP WBEM Services CIM Server process (`cimserver`) is active. To restart it, first *stop* `cimserver` with the `cimserver -s` command. Use the `cimserver` command, with no options to *start* the `cimserver` daemon on the system where the command is issued.

Once the CIM Server has been installed, the CIM Server will be automatically started as part of the system reboot process.

When starting the CIM Server using the `cimserver` command, the `<configProperty=value>` syntax can be used to set configuration property values to be used by the CIM Server. It is important to note that the values specified in the `cimserver` command apply only to the current CIM Server process that gets started. The `cimconfig` command can also be used to set configuration property values to apply each time the CIM Server is started. For more information about starting and stopping the CIM Server, refer to the HP WBEM Services Administrator's Guide or the man page for the `cimserver` command.

To see if the CIM Server is running, issue the following command to check for the `cimserver` process: `ps -ef | grep cimserver`. You should see three processes: `cimserver`, `cimservera`, and `cimserverd` (`cimserverd` is a daemon process that monitors `cimserver` to ensure it remains available).

Removing HP WBEM Services

Before removing the software, back up any files that you want to keep (i.e. repository, log files, configuration files, certificate files, etc.). If they are removed or overwritten during the re-installation, you can restore them.

To remove the HP WBEM Services software, run the HP-UX `swremove` command.

```
# swremove B8465BA
```

Patches and Fixes in this Version

The following sections detail the known problems, required patches, and fixes for this release of HP WBEM Services

Required and Recommended Patches

This lists patches that are required or recommended for HP WBEM Services Version A.02.00. This list is subject to change without notice. Contact your HP support representative for up-to-the-moment information. Patches can be superseded or withdrawn at any time, so always be sure to check the status of any patch before downloading it.

An updated list of patches is available on the Hewlett-Packard IT Resource Center: <http://itrc.hp.com> (Americas and Asia Pacific) and <http://europe.itrc.hp.com> (Europe).

To support the Domain Name Service, Network Time Protocol, and Network Information Service providers, and to avoid potential problems with multi threaded process deadlocks when stressing `fork(2)` and `directory(3C)` (see JAGae84101), the following patch level is required on HP-UX 11i v1 platforms:

- For HP-UX 11i v1 platforms, install LIBC cumulative patch PHCO_29495.
- For HP-UX 11i v1 platforms, install Strong Random Number Generator depot KRNG11i.

Fixes in this Release

The following issues have been addressed and fixed in this release.

checkinstall message in /var/adm/sw/swagent.log

- *What was the problem?* After you cold-install the HP-UX 11i v2 June 2006 release, you may see the following messages in the swagent.log file:

```
/var/tmp/BAAa00208/catalog/WBEMServices/WBEM-CORE/checkinstall[nm] :
```

```
/var/opt/wbem/revision-tmp.txt: cannot create
```

```
/var/tmp/BAAa00208/catalog/WBEMServices/WBEM-CORE/checkinstall[pq] :
```

```
/var/opt/wbem/revision.txt: cannot create
```

Known Problems and Workarounds

The following are known problems and suggested workarounds for the A.02.00 version of HP WBEM Services.

Failure to configure WBEM-CORE fileset (Updating from A.02.00.08 and earlier to A.02.00.09 and later)

- *What is the problem?* Use of the `usePAMAuthentication` configuration option will result in failure to configure the WBEM-CORE fileset during an update of the WBEM Services. The `usePAMAuthentication` configuration option has been obsoleted and is no longer supported.
- *What is the workaround or available patch?* You must do the following:
 1. Before updating the WBEM Services, check if the `usePAMAuthentication` configuration option is present in the following WBEM configuration files:

```
/var/opt/wbem/cimserver_current.conf
```

```
/var/opt/wbem/cimserver_planned.conf
```

2. If the `usePAMAuthentication` configuration option is present, then run the following command before updating the WBEM Services product.

```
# cimconfig -u usePAMAuthentication -p
```

Inefficient Memory Use in CIM Server Daemon

- *What is the problem?* In earlier versions of `libc` on PA, `libc` used a single lock in the `malloc` routines to make them thread-safe. In a multi-threaded application, there could be contention on this single lock if multiple threads are calling `malloc` and `free` at the same time. On HP-UX 11i Version 1.5 (B.11.20), `libc` provides multiple arenas, where `malloc` can allocate space from, and a lock for each arena. Threads are distributed among the arenas. Two new environment variables are introduced: `_M_ARENA_OPTS` and `_M_SBA_OPTS`.

`_M_ARENA_OPTS` can be used to tune the number of arenas and the arena expansion factor for threaded applications. In general, the more threads in an application, the more arenas should be used for better performance. By default, eight (8) arenas are assigned to multi-threaded applications. However, for certain types of multi-threaded applications, the use of multiple arenas can lead to very inefficient memory use. In particular, configuring the CIM Server process, `cimserver`, to use more than one arena can cause the process to grow extremely large.

Please refer to the `malloc(3C)` man page for additional information on the `_M_ARENA_OPTS` environment variable.

- *What is the workaround or available patch?* Starting with HP WBEM Services A.02.00.11 on HP-UX, the CIM Server process will use a single arena. This was done by setting the following environment variables prior to starting the `cimserver`.

```
export _M_ARENA_OPTS=1:8
```

```
export _M_SBA_OPTS=512:100:16
```

To implement this fix in earlier releases of HP WBEM Services execute the following step:

1. Create a new directory `/opt/wbem/lbin`.
2. Verify that the `/opt/wbem/lbin` directory has the same permissions as the `/opt/wbem/sbin` directory.
3. Move the file `/opt/wbem/sbin/cimserver` to `/opt/wbem/lbin`.
4. Create a new `/opt/wbem/sbin/cimserver` file that contains the following script.

```
#!/sbin/sh
```

```
export _M_ARENA_OPTS=1:8
```

```
export _M_SBA_OPTS=512:100:16
```

```
/opt/wbem/lbin/cimserver $*
```

CIM Property of type String with whitespaces compressed

- *What is the problem?* When a provider returns a property of type `String` whose value contains more than one consecutive white space character, the multiple spaces get compressed to a single space on the way to the client.
- *What is the workaround or available patch?* There is no workaround or patch for this problem.

OpenSSL Certificates with expiration dates \geq 2050 are rejected (A.02.00.04 and earlier)

- *What is the problem?* Verification against an OpenSSL certificate with an expiration date greater than or equal to 2050 will return the error "Invalid time and date format". The certificate will not pass authentication.
- *What is the workaround or available patch?* Generating certificates with expiration dates using the year 2049 or before will pass the test for the time and date formatting.

The cimserver may abort if using NPar and Instant Capacity on 11i v2

- *What is the problem?* The cimserver may abort when running with older versions of nPar WBEM provider (NPar) and/or Instant Capacity (formerly known as iCOD).
- *What is the workaround or available patch?* Newer versions of Instant Capacity and NPar need to be installed. Please see the “*Compatibility Information and Installing Requirements for HP-UX*” section of this document for more information.

Incorrect values returned by operating system provider (A.02.00.05 and earlier)

- *What is the problem:* The values for the FreePhysicalMemory and TotalVisibleMemory properties are incorrect.
- *What is the workaround or available patch?* There is no workaround at this time.

Client cannot access hostname with under bar (“_”) in hostname (A.02.00.05 and earlier)

- *What is the problem?* Clients accessing systems that have hostnames including the “_” character (for example: sys_17) will fail with the following error. CIM_ERR_FAILED: A general error occurred that is not covered by a more specific error code: “malformed object name: [hostname]”
- *What is the workaround or available patch?* Avoid making use of an under bar (“_”) character in the hostname.

Wrong hardware description when using WBEM to discover an rx2600 (A.02.00.05 and earlier)

- *What is the problem?* Three values returned by the Computer System Provider are incorrect. These items are 1) Serial Number, 2) Description and 3) Caption.
- *What is the workaround or available patch?* There is no workaround or patch for this problem

Starting with HP WBEM Services A.02.00.07 on HP-UX, the three items have been changed as indicated in the following paragraphs. Additionally, an Identification Number is now also available as described below.

(1) On HP-UX, with the release of HP WBEM Services A.02.00.07, the value of PG_ComputerSystem.SerialNumber will be populated with the Serial Number (i.e., _CS_MACHINE_SERIAL) returned by confstr() rather than an ID Number. See man 3 confstr for more info on _CS_MACHINE_SERIAL.

- (2) On HP-UX, with the release of HP WBEM Services A.02.00.07, the value of `PG_ComputerSystem.IdentificationNumber` will be populated with the Identifier (i.e., `_CS_MACHINE_IDENT`) returned by `confstr()`. See `man 3 confstr` for more info on `_CS_MACHINE_IDENT`. Prior to the A.02.00.07 release, this property was not supported.
- (3) On HP-UX, with the release of HP WBEM Services A.02.00.07 the value of the `Description` property for `CIM_ComputerSystem` objects will be populated with the value returned by the model command. Prior to the A.02.00.07 release, the `Description` property was assigned the fixed value "This is the `CIM_ComputerSystem` object".
- (4) On HP-UX, with the release of HP WBEM Services A.02.00.07, the value of the `Caption` property for `CIM_ComputerSystem` objects will be populated with the value returned by the model command. Prior to the A.02.00.07 release, the `Caption` property was assigned the fixed value "Computer System".

Software Availability in Native Languages

HP WBEM Services is available only in English.