HP WBEM Services Version A.02.11.00 Release Notes

HP-UX 11i v3

HP Part Number: 5900-2557
Published: March 2013

Legal Notices

Contents

1 HP WBEM Services Version A.02.11.00 Release Notes

Announcement

The following information is for HP WBEM Services Version A.02.11.00:

HP WBEM Services for HP-UX is available from http://software.hp.com.

HP-UX implements the Distributed Management Task Force (DMTF) WBEM standard and this enables HP WBEM Services to deliver increased control of enterprise resources at reduced cost. WBEM (Web-Based Enterprise Management) is a platform and resource-independent DMTF standard that defines a Common Information Model (CIM) and communication protocol to monitor and control resources from diverse sources.

WBEM is defined by the following standards:

- **Common Information Model (CIM)**: The Common Information Model (CIM) is an object-oriented information model that describes managed resources. The CIM specification includes the following:
  - CIM Object — A representation of a managed resource.
  - 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 a managed object that belongs to a particular class. These objects can be shared by any WBEM-enabled system or application.

  MOF (Managed Object Format) is the language used to define the CIM classes and instances. MOF files are ASCII files that use the MOF language to describe the CIM objects.
- **Representation of CIM in Extensible Markup Language (XML)**: Extensible Markup Language (XML) is the language used to describe data on the web. The DMTF defines a standard for using the CIM elements and messages in XML. Because CIM-XML provides a standard method of describing the data, any WBEM client can access the CIM data on any WBEM-enabled system.
- **CIM Operations over HTTP**: The CIM Operations over HTTP specifications defines how HTTP is used to transport the CIM information.

HP WBEM Services can operate in both the homogeneous and heterogeneous IT environments. HP WBEM Services supports multi-platform and multi-operating system management tools. In a heterogeneous environment, HP WBEM Services leverages the existing training and knowledge base of the current IT staff. In a homogeneous environment, HP WBEM Services optimizes management information and capabilities, using a standard method, regardless of the architecture or platform 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.

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

The HP WBEM Services product, WBEMServices A.02.11.00 is now available on HP-UX 11i v3.

What's new in this version?

HP WBEM Services Version A.02.11.00 for HP-UX is a major update to the HP WBEM Services. This release of the product is based on the OpenPegasus 2.11.1 source base and CIM Schema 2.28.

This release includes defect fixes and enhancements. For information about the defect fixes in this release, see Table 4 (page 16).

Following are the key differences between the HP WBEM Services version A.02.09.14 and A.02.11.00:

- **New config property**

  `maxFailedProviderModuleRestarts`: The new release includes a new config property called "maxFailedProviderModuleRestarts". By default, this value 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
  ```

- **New option for Cimserver**

  `-status`: This option is introduced to verify whether or not the Cimserver is running.

  ```
  # cimserver --status
  ```

  ```
  CIM Server is running.
  ```

For more information, see the *HP WBEM Services for HP-UX System Administrator Guide*.

Table 1 HP WBEM Services releases

WBEM version	HP-UX version
A.02.11.00	HP-UX 11i v3
A.02.09.14	HP-UX 11i v2
A.02.09.12	HP-UX 11i v3
A.02.09.10	HP-UX 11i v3
A.02.09.08 (Web release)	HP-UX 11i v2 HP-UX 11i v3
A.02.09.06	HP-UX 11i v3
A.02.09.04	HP-UX 11i v2 HP-UX 11i v3
A.02.09.02	HP-UX 11i v2 HP-UX 11i v3
A.02.09	HP-UX 11i v2 HP-UX 11i v3
A.02.07.06	HP-UX 11i v1

NOTE: HP WBEM Services version A.02.09.06, A.02.09.10, A.02.09.12, and A.02.11.00 are not available on HP-UX 11i v2.

IMPORTANT: HP WBEM Services Version A.02.11.00 is not available on HP-UX 11i v1. Starting with the September 2009 Application Release (AR), no new features or enhancements for HP WBEM Services is addressed on HP-UX 11i v1. Only defects that are critical in nature are addressed.

HP WBEM Services Version A.02.11.00 contains the following:

- Support for WBEM Indications
- HP WBEM Services run-time environment
  - Binary command line executables
  - Shared libraries
  - Configuration files
  - CIM schemas
- Packaged provider modules
  - Computer System
  - Operating System
  - Process
  - Domain Name Service
  - Network Time Protocol
  - Network Information Service
  - IP
  - SD
  - IOTree

For information on installing HP WBEM Services Version A.02.11.00, see "Installation information" (page 13).

Security

HP WBEM Services supports the following connection points:

- HTTP port
- HTTPS (HTTP Secure) port
- HTTPS port for Export Connections
- 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 the CIM clients and the CIM Server. The port `wbem-exp-https` (HTTPS TCP/IP communication) is dedicated for CIM-XML communication between the Indication sender and the CIM Server. The HTTP point and the two HTTPS connection points can be disabled using the `cimconfig` command line utility. However, the UNIX domain socket connection is always enabled when the CIM Server is running.

Security considerations

When you use the Simple Network Management Protocol (SNMP), Process Resource Manager (PRM), and Workload Manager (WLM) tools, consider the following security conditions:

- You can use tools such as PRM and WLM to limit computing resources used by the WBEM Services processes. You can purchase these products from http://www.software.hp.com.

  However, limiting or restricting the computing resources of the WBEM Services processes, depending on the configured limits and WBEM Services utilization, can cause WBEM Services processes to constantly reach the limits.

- Due to security limitations of the SNMP protocol, HP does not recommend using the SNMP indication handler.

SSL support

HP WBEM Services uses SSL (Secure Sockets Layer) for all communications, with server-side certificates that are trusted by the management application, when using HTTPS connections. HP WBEM Services uses OpenSSL to support HTTPS connections.

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

On the HTTPS port, the CIM clients uses 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 value of the CIM Server configuration property `enableHttpsConnection` to *`false`*. Be sure the value for the `enableHttpConnection` property is set to *`true`* and restart the CIM Server.

To disable the Export HTTPS port, use the `cimconfig` command to set the 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 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, hence, this traffic is not visible on the network interconnect.

Remote user authentication

The CIM Server can authenticate remote users, using the following methods:

- HTTP Basic Authentication
- Certificate Based Authentication (CBA)

“Remote user authentication methods” lists each remote authentication method in detail.

Table 2 Remote user authentication methods

Certificate Based Authentication (CBA)	HTTP Basic Authentication
Description	
The CIM Server requests the client certificate when the HTTPS connection is in progress.	Using a request/challenge mechanism and authenticating the user-supplied username and password through Pluggable Authentication Modules (PAM).

Table 2 Remote user authentication methods *(continued)*

Certificate Based Authentication (CBA)	HTTP Basic Authentication
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. • Prevents intruders from gaining access to internal network resources by “spoofing” passwords. • Does not require additional configuration or updates to applications whenever a password is changed.	• Does not require any server configuration and hence, easy to set up. • Requires the remote user to provide a password to access the WBEM data. • Requires to update the client application whenever the password is changed.
For more information, see...	
“Using Certificate Based Authentication” (page 9)	“Using HTTP Basic Authentication” (page 8)

Using 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. WBEM Services uses the default authentication method 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 the following example. For additional information, see the *pam*(3) and *pam.conf*(4) manpages.

```
#
# 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 uses the `cimservera` executable in HP WBEM Services to provide the `cimserver` with PAM Authentication services. For more information, see the *HP WBEM Services for HP-UX System Administrator Guide*.

Using Certificate Based Authentication

To use the Certificate Based Authentication (CBA) method, you must do the following:

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

NOTE: HP System Insight Manager (HP SIM) Version 5.1 or later enables you to use CBA for remote user. For more information on CBA for remote users, see the HP SIM documentation.

Certificate verification

CIM Client

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

Using `wbemexec` command

The `wbemexec` command provides a command-line interface to the 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` file from the system where the CIM Server is running to the client system's trust store.

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

For more information about certificates, see "Importing server certificates to trust store" (page 10).

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

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

Managing certificates

During the installation process, if the `/etc/opt/hp/sslshare/cert.pem` and `/etc/opt/hp/sslshare/file.pem` files are found on the system, the following messages is 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.

HP-UX example:

The following examples describe how to update certificates when an earlier version of HP WBEM Services is already installed:

- 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 do the following:

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

   Or

2. Overwrite the new certificate in the /etc/opt/hp/sslshare/cert.pem file and the private key in the /etc/opt/hp/sslshare/file.pem file with the existing certificate and key in either /var/opt/wbem/server_2048.pem or /var/opt/wbem/server.pem files. Before overwriting the /etc/opt/hp/sslshare/cert.pem and /etc/opt/hp/sslshare/file.pem files ensure 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 the /etc/opt/hp/sslshare/cert.pem file should be copied to the trust store on those other systems replacing 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 you are using either the self-signed or root-signed 512-bit or 1024-bit encryption certificates, then HP recommends that you create new certificates with 2048-bit encryption.

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

Importing server certificates to trust store

CIM client applications must maintain a trust store in the <trust_store-name>.pem file. The CIM client applications must import the certificates stored in /etc/opt/hp/sslshare/cert.pem to a trust store file on the client machine from various CIM Server machines (machines that 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 application:

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, 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) to the trust store <trust_store-name>.pem on the client machine.

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

Standard conformance

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

- CIM Operations over HTTP, Version 1.2
- Representation of CIM in XML, Version 2.2
- CIM Infrastructure Specification, Version 2.3
- CIM Schema, Version 2.28

For more information, see the DMTF WBEM and CIM standards at http://www.dmtf.org.

Compatibility information

This section describes the compatibility information for HP WBEM Services Version A.02.11.00.

Compatibility for WBEM providers

Table 3 lists the product bundle and WBEM version information for HP-UX 11i v3. Use this table to determine, which bundle is compatible with your version of HP-UX.

Use the `swlist <product tag>` command to view your product bundle version number.

NOTE: Unless otherwise stated, the tables indicate support for the listed and later versions of WBEM providers that are compatible with HP WBEM Services Version A.02.11.00. This version of HP WBEM Services can work with earlier versions of the providers that are already installed in your environment. However, these earlier versions are not tested with HP WBEM Services Version A.02.11.00.

For information on specific provider versions, see the provider specific release notes and data sheets available at: http://www.hp.com/go/hpux-networking-docs-> *HP-UX 11i WBEM Software*.

Table 3 HP-UX 11i v3 WBEM Solution Compatibility Table

Product Tag	Product Title	Product Version	Supported HP WBEM Services Version
iCOD	HP-UX iCOD (Instant Capacity)	B.11.31.10.07.00	A.02.11.00
NParProvider	nPartition Provider - HP-UX	B.31.02.04	
SW-DIST	HP-UX Software Distributor	B.11.31.1303.390	
WBEMP-LAN	LAN Provider for Ethernet LAN interfaces	B.11.31.1303.04.01	
VParProvider	vPar Provider - HP-UX	B.11.31.01.06	
WBEMP-FCP	WBEM Provider for FC HBAs	B.11.31.1303.05.01	
SCSI-Provider	WBEM Provider for SCSI HBA	B.11.31.1203	
LVM-Provider	CIM/WBEM Provider for LVM	B.11.31.1209	
utilProvider	HP-UX Utilization Provide	A.01.08.08.00	
vmProvider	WBEM Provider for Integrity VM	B.06.20	
WBEMP-Storage	HP-UX WBEM Direct Attached Storage Provider	B.11.31.1303.06.01	
PRM-Sw-Lib	HP PRM Software Libraries	C.03.06	
SGWBEMProviders	HP Serviceguard WBEM Providers	A.03.10.00	
EMS-Core	EMS Core Product	A.04.20.31.08	
WBEMP-FS	HP-UX File System CIM Provider	B.11.31.1009	
SAS-PROVIDER	Serial SCSI provider product	B.11.31.1303.05.01	
olosProvider	OLOS Provider	B.01.04	
WBEMP-IOTreeIP	CIM/WBEM Indication Provider for IOTreesubsystem	B.11.31.1303	
AppDiscMN	Application Discovery Managed Node Agent	A.7.1	
RAIDSA-PROVIDER	Smart Array Provider product	B.11.31.1303.05.01	
KERNEL-PROVIDERS	HP-UX Kernel Providers	C.05.00.05	
SFM-CORE	HPUX System Fault Management	C.07.10.06	
Cluster-OM	HP Cluster API	B.07.00.00	
OS-Core	Core Operating System	B.11.31	
CM-Provider-MOF	CM Provider and MOF	B.07.00.00	

Additional compatibility information

From the A.02.05 release, HP WBEM Services for HP-UX supports an option that allows a WBEM Provider (management instrumentation) to run as the user who issued the management request.

Prior to this release, all WBEM Providers executed in a privileged context. With the release of HP WBEM Services Version A.02.05.02 for HP-UX 11i v3, WBEM Providers will, by default, be invoked in the context of the user requesting an operation (i.e., “Run-As-Requestor”). This default setting can break backward compatibility for certain types of providers.

This means that existing providers that run in the user context of the CIM Server can break. To resolve this situation, you have the following two alternatives:

Alternative 1

To continue running the provider in a privileged context, you need to explicitly register the provider to run in a “Privileged User” context. This is a configuration file change and does not require a change to the Provider library. You do not require to recompile/re-link your provider, to continue running in a privileged context.

To register your provider to run in a “Privileged User ” context, you need to modify the `PG_ProviderModule` instance definition in the Provider Registration MOF as follows:

1. Change the InterfaceVersion from “2.1.0” to “2.5.0”.
2. Add the new property UserContext = 4.

   Example using an updated PG_ProviderModule instance definition for the Operating System Provider Module:

   instance of PG_ProviderModule

   ```
   {
   Name = "OperatingSystemModule";
   Vendor = "OpenPegasus";
   Version = "2.0.0";
   InterfaceType = "C++Default";
   InterfaceVersion = "2.5.0";
   Location = "OSProvider";
   UserContext = 4;
   };
   ```

Alternative 2

To support running in the “Requestor” context, ensure that the provider is written to allow multiple instances of the provider to run at the same time (in different user contexts). In some cases, the provider might need to coordinate the actions of the provider instances. When the provider is a “pass-through” to a managed resource, no coordination might be necessary.

In addition, providers running in the “Requestor” context must only perform privileged operations. If those operations are only expected/required to succeed, when invoked by a user who already has the necessary privileges.

Installation information

This section describes the prerequisites and the procedures for installing HP WBEM Services.

Prerequisites for installing HP WBEM Services

Following are the prerequisites for installing HP WBEM Services Version A.02.11.00:

- HP-UX 11i v3
- OpenSSL must be installed before installing HP WBEM Services Version A.02.11.00.

  HP recommends that the OpenSSL version available with HP-UX OE is installed before installing HP WBEM Services Version A.02.11.00. For HP-UX 11i v3, install OpenSSL version A.00.09.08x.003.

  NOTE: After the OpenSSL updates are installed, the HP WBEM Services `cimserver` process must be shutdown and restarted in order to run against any new version of OpenSSL. For more information on shutting down and restarting the `cimserver`, see the *HP WBEM Services System Administrator Guide*.

- 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 communications between CIM clients and the CIM Server. One port is dedicated for CIM-XML communications between the Indication sender and the Indication receiver (a CIM Server).

  - HTTP port 5988
  - HTTPS port 5989
  - HTTPS port for Export Connections

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

Installing HP WBEM Services

HP WBEM Services is part of the HP-UX Operating Environment and is installed automatically when you start the HP-UX system. However, you can choose to install HP WBEM Services at a later time by downloading the software from http://software.hp.com. HP WBEM Services is available at this link as a single depot.

To install HP WBEM Services, you must login to the HP-UX system as `root` (`uid=0`).

IMPORTANT: Before installing the software, ensure that your system meets the software and hardware requirements described in the section "Compatibility information" (page 11).

Complete the following procedure to install HP WBEM Services:

1. Download the product from http://software.hp.com.
2. Copy the downloaded depot file to a local directory on the system.
3. Log in to the HP-UX system as `root` and locate the directory where the depot is downloaded.
4. Run the following HP-UX command to start the installation.

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

   At installation, 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, executables
`/opt/wbem/lbin`	Executables that are not intended to be used directly by customers.
`/opt/wbem/lib`	Shared libraries
`/opt/wbem/mof/CIM228`	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 `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 these files from the default location. If these files are moved, it can result in problems in the functioning of the CIM Server.

5. Run the following HP-UX command to verify that HP WBEM Services is installed:

   ```
   swverify WBEMServices
   ```

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

   After the successful installation of HP WBEM Services, the `cimserver` process automatically starts. You can verify this using the following command:

   ```
   cimserver --status
   ```

For HP-UX, the following providers are bundled with HP WBEM Services:

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

After installing HP WBEM Services version A.02.11.00, the following filesets are visible on the system:

- WBEM-CORE, A.02.11.00 - WBEM Services core fileset for HP Integrity servers
- WBEM-CORE-COM, A.02.11.00 - WBEM Services COM fileset for HP Integrity servers and HP 9000 servers
- WBEM-MAN, A.02.11.00 - WBEM Services manpages
- WBEM-MX, A.02.11.00 - Reserved for future use
- WBEM-TOOLS, A.02.11.00 - Contains tools for troubleshooting HP WBEM Services

NOTE: While re-installing HP WBEM Services, any existing repository in the `/var/opt/wbem/repository` is moved to the `/var/opt/wbem/prev_repository` before building a new repository.

HP WBEM Services Version A.02.09 upgrades the existing repository to CIM schema 2.17.1 by recreating the schema extensions from the old repository (`/var/opt/wbem/prev_repository`) into the new repository (`/var/opt/wbem/repository`) that has been initialized with the new version of the schema.

Running the CIM Server

After installation, the HP WBEM Services CIM Server process (cimserver) is active. To restart it, first *stop* CIM Server 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 automatically starts 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. 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.

To see if the CIM Server is running, use the following command to check for the cimserver process: ps -ef | grep cimserver. You will see the following processes: cimserver, cimservermain, and cimserverd. The cimserverd process is a daemon process that monitors cimserver to ensure it remains available.

⚠ **WARNING!** HP recommends not to disable cimserver at startup. Doing so, will impact other HP products such as; iCOD/iCAP, HP SIM, VSE, and System Fault Management, as these HP solutions depend on HP WBEM Services (cimserver) to be running.

Removing HP WBEM Services

Before removing the software, back up any files that you want to retain, such as the repository, log files, configuration files, and certificate files. If these files are removed or overwritten during the re-installation, you cannot restore them.

To remove HP WBEM Services, run the following HP-UX command:

```
# swremove WBEMServices
```

When there are providers in your environment that have a dependency on the file sets of HP WBEM Services, then this command results in an error. In such cases, run the following command to remove HP WBEM Services:

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

Patches and fixes in this version

This section describes the known problems, required patches, and fixes for this release of HP WBEM Services.

Required and recommended patches

Currently, there are no patches required for HP WBEM Services Version A.02.11.00 for HP-UX 11i v3.

Fixes in this release

Unless listed in the Known Problems and workarounds section, all known problems of previous versions of HP WBEM Services have been fixed in this version.

Table 4 describes the defects fixed in HP WBEM Services Version A.02.11.00 and A.02.09.xx.

Table 4 Defects fixed in HP WBEM Services Version A.02.11.00 and A.02.09.xx

Identifier	Description	Resolution
	Defects fixed in A.02.11.00	
QXCR1001056019	When two constructed “EnumerateInstances” queries, one using PropertyList parameter to	PropertyList filtering implementation aligned with WBEM specification

Table 4 Defects fixed in HP WBEM Services Version A.02.11.00 and A.02.09.xx *(continued)*

Identifier	Description	Resolution
	specify two fields, and one without PropertyList which would select all fields, the resulting WBEM response when compared were identical. The PropertyList parameter did not reduce the network traffic as expected.	
	Defects fixed in A.02.09.14	
QXCR1001219079	cimserver fails to start with duplicate entries in namespace authorization. As the namespace is not case sensitive, multiple entries can be created for namespace authorization for the same user. However, cimserver will fail to restart. The only way to recover from this failure is to recreate repository.	Check is added to avoid duplicate entries in namespace authorization table.
QXCR1001201880	Add Member does not work with skymaster firmware. After installing manually created rule files, Add Member command does not work on skymaster firmware. icapd throws "Unexpected Error" exception. Problem is due to OpenSSL library mismatch between OA and WBEM Services.	WBEMServices is updated with the latest OpenSSL version i.e. moved to 0.9.8r from 0.9.7i.
	Defects fixed in A.02.09.12	
QXCR1001164283	When the permission of the file `/etc/opt/wbem/cimserver_start.conf` is changed to root:sys and also the permission of directories `/etc, /etc/opt and /etc/opt/wbem` changed to root:sys then for next cimserver start up, cimservermain will fall into a deadlock loop resulting in 100 percent cpu consumption. This is because the file `/etc/opt/wbem/cimserver_start.conf` becomes inaccessible.	This defect is fixed by modifying cimserver shutdown and startup path to ensure that cimserver do not start if the permission of `/etc, /etc/opt, /etc/opt/wbem` and `/etc/opt/wbem/cimserver_start.conf` is changed to root:sys.
	Defects fixed in A.02.09.10	
QXCR1001105601	When the `swverify(1M)` command is executed with the `(-x fix=true)` option, CIM Server becomes unstable. Subsequent CIM Server start up fails.	This defect is fixed in the current release. The WBEM configure script is modified to ensure that when the `swverify` command is executed with any options, it does not change any file permissions or affect CIM Server start up.
	Defects fixed in A.02.09.08	
QXCR1001089629	According to the DMTF standards, the WBEM namespaces are not case sensitive, but the `cimauth` command processes namespaces as case sensitive.	This defect is fixed in the current release. The `cimauth` command and the internal WBEM data structures are modified to ensure that the namespace case sensitive error does not occur.
QXCR1001103470	The `StorageNative Provider` module hangs when it is continuously enabled and disabled for one process, while `EnumerateInstances` is running for `StorageNative Provider` in another process. There is a race condition during the provider shutdown.	This defect is fixed in the current release. A mutex has been added to ensure that the race condition does not occur.
QXCR1001106183	The Pegaus core dump error occurs when the `StorageNative Provider` module is continuously enabled and disabled in one	This defect is fixed in the current release. The destruction sequence is modified to ensure that this defect does not occur.

Table 4 Defects fixed in HP WBEM Services Version A.02.11.00 and A.02.09.xx *(continued)*

Identifier	Description	Resolution
	process, while `EnumerateInstances` is running for `StorageNative Provider` in another process. The core dump occurs due to an incorrect destruction sequence in one of the `cimprovagt` objects.	
QXCR1001095699	Multiple instances of the `cimprovagt` processes are created for one provider. This defect occurs when the `StorageNative Provider` module is continuously enabled and disabled in one process, while `EnumerateInstances` is running for `StorageNative Provider` in another process. When a 'disable' request is sent to a provider, it hangs. The `cimprovagt` process incorrectly assumes that the provider threads are down and sends a successfully disabled message to `cimservermain`. This causes `cimservermain` to start a new `cimprovagt` process for a new request.	This defect is fixed in the current release. The destruction sequence has been modified to ensure that `cimprovagt` waits for all provider threads to go down before sending a success message to `cimservermain`.
QXCR1001104350	When disabling a provider module, WBEM Services core dump occurs. The response pointer to a client request is accessed before building a response in certain scenarios, which results in a core dump.	This defect is fixed in the current release. The response pointer is ensured to built in all scenarios.
	Defects fixed in A.02.09.06.01	
QXCR1001113611	When you set the language to Japanese and execute `wbemassist -h`, the output displayed contains the character “`^M`”.	This defect is fixed in the current release. The `wbemassist.cat` file is modified and provided without the “`^M`” character so that the correct output is displayed on the console.
	Defects fixed in A.02.09.06	
QXCR1000586083	The cimserver consumes threads after a cimprovagt process, hosting a provider request, hangs. Eventually, cimserver reaches its process thread limit. This inhibits the cimserver from processing requests received from other providers as well.	This defect is fixed in the current release. Periodically, outstanding requests for a provider module are checked to see if the client is still waiting for the response. If not, the resources used for this request are freed up.
QXCR1001062117	Newly installed software Microsoft SCOM-Agent prevents cimserver from starting after running the following command on the system: `/sbin/init.d/cim_server start`	This defect is fixed in the current release and cimserver starts up normally after installing the new software on the system.
QXCR1001066307	When clients running on the localhost, connecting via the `connectlocal( )` method, terminate the connection before authentication is completed, the authentication token is not removed from `/var/opt/wbem/localauth` file.	This defect is fixed in the current release. With this fix, cimserver now removes any `/var/opt/wbem/localauth` file created for connections that are terminated before authentication is completed.
QXCR1001071978	When upgrading from HP-UX 11i v2 OS to HP-UX 11i v3 OS, the WBEMServices filesets and all filesets dependent on WBEM are not configured correctly in an LDAP environment. During the configure phase of WBEMServices, error messages are seen.	This defect is fixed in the current release.

Table 4 Defects fixed in HP WBEM Services Version A.02.11.00 and A.02.09.xx *(continued)*

Identifier	Description	Resolution
QXCR1001060784	The cimserverd daemon checks if the cimservermain process is running and restarts cimserver if cimservermain is not active.	With the current fix, cimserverd daemon monitors the status of both cimserver and cimservermain processes and restarts cimserver if either one of the process is not active.
QXCR1001064867	During previous release, the `wbeminfo.sh` script does not display all the registered providers and the corresponding classes on a system.	This defect is fixed in the current release. With this fix, the `wbeminfo.sh` script is enhanced to display all the registered providers and the corresponding classes on a system.
	Defects fixed in A.02.09.04	
QXCR1001017205	The `IndicationTime` property of the `HP_AlertIndication` class does not display the Coordinated Universal Time (UTC). The event time in the indications that are received do not match with the local time of the system.	This defect has been fixed such that the `IndicationTime` property displays the accurate local time.
	Defects fixed in A.02.09.02	
QXCR1000962884	A memory leak occurs in the `cimprovagt` process when the loaded provider reaches the value specified for the `max_thread_proc` parameter. Also, all subsequent `pthread_create()` calls fail.	This defect has been fixed such that this memory leak does not occur.
QXCR1000984017	The September 2009 version of the *HP WBEM Services Release Notes* specified incorrect versions of the SCSI provider and SAS provider.	The *HP WBEM Services Release Notes* document has been updated with the correct versions of the SCSI and SAS provider.
	Defects fixed in A.02.09	
QXCR1000890091	In the Networking page of HP System Management Homepage, the following error is displayed: `CIM_ERR_FAILED: Error in ioctl() request SIOCGIFCONF: Invalid argument` When this error message is displayed, no other data can be displayed on the Networking page. This error is noticed only with HP WBEM Services versions prior to A.02.09 on HP-UX 11i v1 and v2 systems on which patch `PHNE_35351` and subsequent patches have been installed.	This defect has been fixed to resolve this error message.
QXCR1000873670	The manpage for the `osinfo` command does not indicate that the `/etc/opt/hp/sslshare/client.pem` file is required for Client Based Authentication (CBA).	The manpage for the `osinfo` command has been updated.
QXCR1000914874	The `cimmof` and other WBEM client commands result in a core dump while accessing ICU libraries. With the cimmof coredump, the following error message is logged in the `swagent.log` file: `/var/tmp/BAAa25429/catalog/`	This defect has been fixed to resolve these error messages.

Table 4 Defects fixed in HP WBEM Services Version A.02.11.00 and A.02.09.xx *(continued)*

Identifier	Description	Resolution

	`WBEMServices/`
	`WBEM-CORE.2/configure[913]:`
	`25842 Memory fault (coredump)`
	`WARNING: Unable to load SD mof files`
	With the cimservermain coredump, the following connection error message is displayed:
	`PGS08001: CIM HTTP OR HTTPS CONNECTOR CANNOT CONNECT TO 10.162.5.25:5989. CONNECTION FAILED`	

Known problems and workarounds

Following known problems and workarounds are for this release.

Issue with enabling, disabling, and enumerating provider module

What is the problem?

While enabling, disabling, and enumerating instances, the provider module sometimes changes to `OK Stopping` state. At this state, it is not possible to enable and disable the provider.

What is the workaround?

To recover from this state, run the following commands in the order listed, in the context of SFM Provider module:

1. `cimprovider -rm SFMProviderModule`
2. `cd /opt/sfm/schemas/mof/`
3. `cimmof -nroot/PG_InterOp SFMProvidersCommonR.mof SFMProvidersHPOnlyR.mof`
4. `cimmof -nroot/PG_InterOp SFMProvidersHPOnlyIaR.mof`

   This is applicable only for IA. This mof will not exist if the machine is other than IA.
5. `cimmof -nroot/PG_InterOp EvmCimProviderR.mof`

   This is applicable only for systems running HP-UX 11i v3.

Users and groups of HP WBEM Services conflict with users and groups of NIS, LDAP and other network services

What is the problem?

During installation, HP WBEM Services creates a user `cimsrvr` and a group `cimsrvr`. If you are using `Network Information Services` (NIS), `Lightweight Directory Access Protocol` (LDAP) or any other network service for managing user and group accounts, there is a possibility that the user ID (UID) and the group ID (GID) created for HP WBEM Services is already in use by other users. The duplication of user and group IDs results in a change in file ownership and can stop applications working correctly.

IMPORTANT: This issue is only applicable for HP WBEM Services A.02.07 and later versions.

What is the workaround?

For systems using `LDAP` or other network services, before installing HP WBEM Services, you must manually add a local `cimsrvr` user and group using a unique UID and GID. You must first determine the available reserved IDs for the group (for example 130) and for the user (for example,

125) ensuring that these IDs are not in use by LDAP or other network services. Run the following command to add the group:

```
/usr/sbin/groupadd -g 130 cimsrvr
```

After creating the group, run the following command to add the user:

```
/usr/sbin/useradd -u 125 -g cimsrvr -d /var/opt/wbem -c "WBEM Services"
cimsrvr
```

NOTE: If you do not manually add the group and the user before installing HP WBEM Services, the installation scripts add a group and user using locally available IDs, returned by useradd(1M) and groupadd(1M), which may already be in use on the network.

For systems using NIS the problem is encountered when HP WBEM Services is installed as part of a custom bundle that requires a system reboot or if NIS is stopped for any other reason whilst the HP WBEM Services installation is performed. In the former case, this is because the HP WBEM Services configure phase (when the user and group are created) is run before NIS is up and running after a system reboot. To avoid this problem on systems that have NIS configured, install the HP WBEM Services upgrade on its own or as part of a custom bundle that does not contain updates that require a system reboot.

This problem does not affect new installations where the `cimsrvr` user and group is present before NIS, LDAP or other network services are configured; or minor upgrades of HP WBEM Services where the `cimsrvr` user and group is present from an earlier HP WBEM Services A.02.07 or later installation.

Related documentation

Following are the documents available with this release of HP WBEM Services:

- *HP WBEM Services Administrator Guide*, 5900-1802 available at www.hp.com/go/hpux-networking-docs and select HP-UX 11i WBEM Software collection.

  Release Notes for this version and for previous versions of HP WBEM Services are available at www.hp.com/go/hpux-networking-docs and select HP-UX 11i WBEM Software collection.

After installing HP WBEM Services, see the manpages for your system. Manpages are summarized in the *HP WBEM Services System Administrator Guide*.

For more information about DMTF, WBEM, and CIM standards, see the information available at http://www.dmtf.org.

Localized version of the software

The product is supported only in English locale (`LANG`=C). Behavior of the product is unpredictable when the `LANG` value is set to any other language code other than C. Documentation support for this product is also available only in English locale.