HP Operations Manager Dependency Mapping Automation

For Windows® and UNIX® Operating Systems

Software Version: 8.10

Installation and User's Guide

Manufacturing Part Number: B7491-90103
Document Release Date: 17 June 2008
Software Release Date: June 2008

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Itanium®, and Xeon® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

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

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

To check for updates, or to verify that you are using the most recent edition of a document, go to:

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

You also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP software support web site at:

www.hp.com/managementsoftware/services

HP software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1 Overview

HP Operations Manager (HPOM) Dependency Mapping Automation (DMA) enables IT operations teams to align their activities more fully with the business services that the IT infrastructure supports. By providing automated dependency mapping and configuration consistency across multiple HPOM servers, HPOM DMA optimizes the ability of IT organizations to support their businesses, and enables enhanced productivity and efficiency within the operations teams.

Advantages of HPOM DMA

HPOM DMA helps you to do the following:

- **Automate Maintenance**

  Automate and simplify the creation and maintenance of business service views within HPOM to enable business-focused impact and root cause analysis for operational incidents.

- **Streamline Analysis**

  Streamline incident analysis activities by providing drill-down from managed nodes or services in HPOM into their change history within the HP Universal CMDB (UCMDB).

- **Consolidate Information**

  Consolidate systems and managed services information in a single place, the UCMDB database, to provide shared and consistent views across multiple HPOM servers.

- **Monitor Infrastructure**

  Rationalize the process of identifying new servers and applications, and the deployment of HPOM monitoring to business-critical infrastructure.

Creating Business Service Views Automatically

Aligning the activities of the IT organization with the needs of the business is an ongoing challenge that is under increasing scrutiny in many companies. IT investments and resources need to be targeted and prioritized so that they maximize the value that they deliver to the business processes and users that IT supports.

In IT operations environments, managing resources is a significant challenge because of the complexity associated with understanding the relationships between the business applications and the IT infrastructure that supports them.

HPOM DMA addresses this exact issue. By connecting HPOM to UCMDB — and the system and application service dependency information within it — HPOM DMA can construct business service views within HPOM. These business service views provide your operations staff with a unique insight into the impact of infrastructure events.

Configuration item (CI) information, such as systems, applications, network devices, business services, and the dependency information that defines the relationships between CIs, can be added to UCMDB in a number of ways:

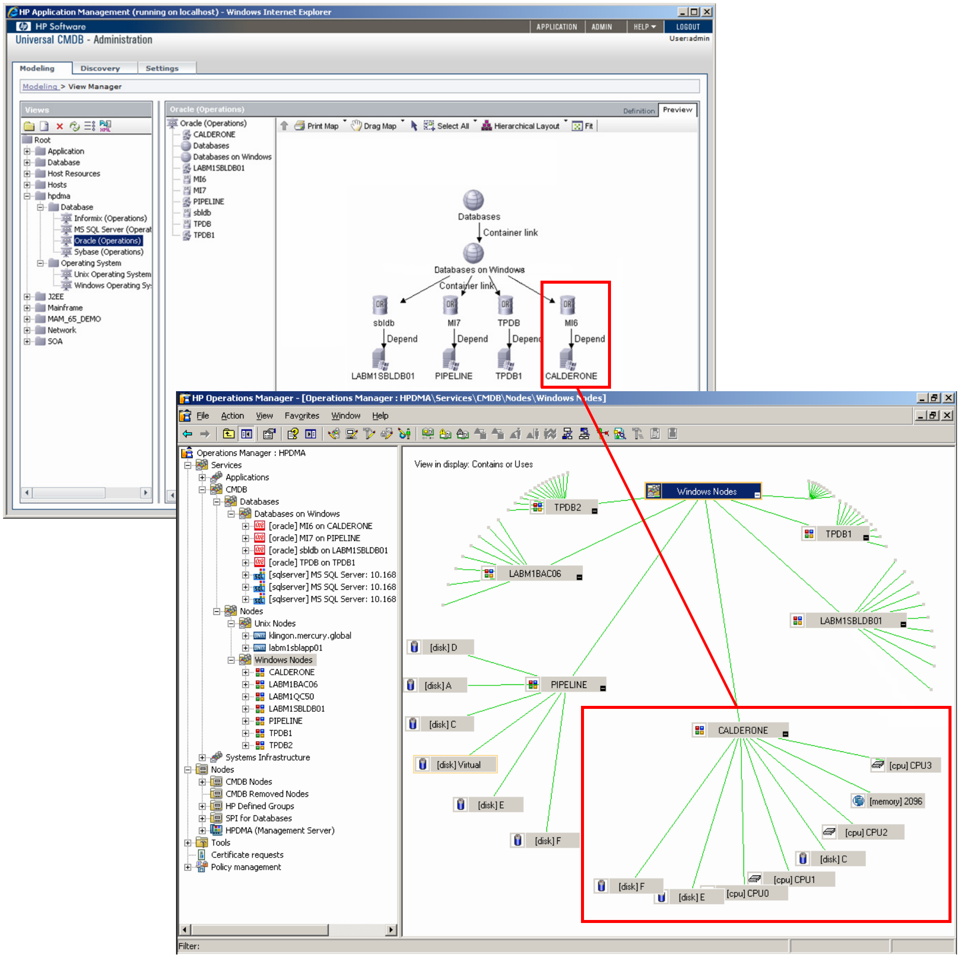
- HP Software Discovery and Dependency Mapping can automatically populate and maintain both CI and dependency information in UCMDB.
- UCMDB federation capabilities can consume CI and dependency information from existing third party CMDBs, and make this information available to HPOM DMA.
- CI information can be manually loaded as part of the initial setup.

HPOM DMA consumes information from UCMDB, and uses it to populate the node banks within HPOM. HPOM DMA also creates service trees that can include discovered applications and the dependencies between these applications. For example, consider an online retail application with web servers situated in a DMZ (De-Militarized Zone) to service customers on the Internet. These web servers communicate with back-end database and application servers in the corporate intranet. The successful processing of customer orders depends on this interaction. HPOM DMA can automatically add this dependency information to the service maps within HPOM.

Service maps within HPOM include much greater business service context. Impact analysis indicates more than just the affected application. It shows the impacted business service. Your operations staff can use business service views to show when incidents are threatening the availability of the business processes which rely on the IT infrastructure.

Figure 1 the upper-left screen shows discovery data within UCMDB. The lower-right screen shows the associated CI information that HPOM DMA has added to the HPOM for Windows Service Map. It also shows some associated hardware dependency details.

Figure 1 Discovery Data in UCMDB and CI Information in HPOM



Launching UCMDB CI Change Information

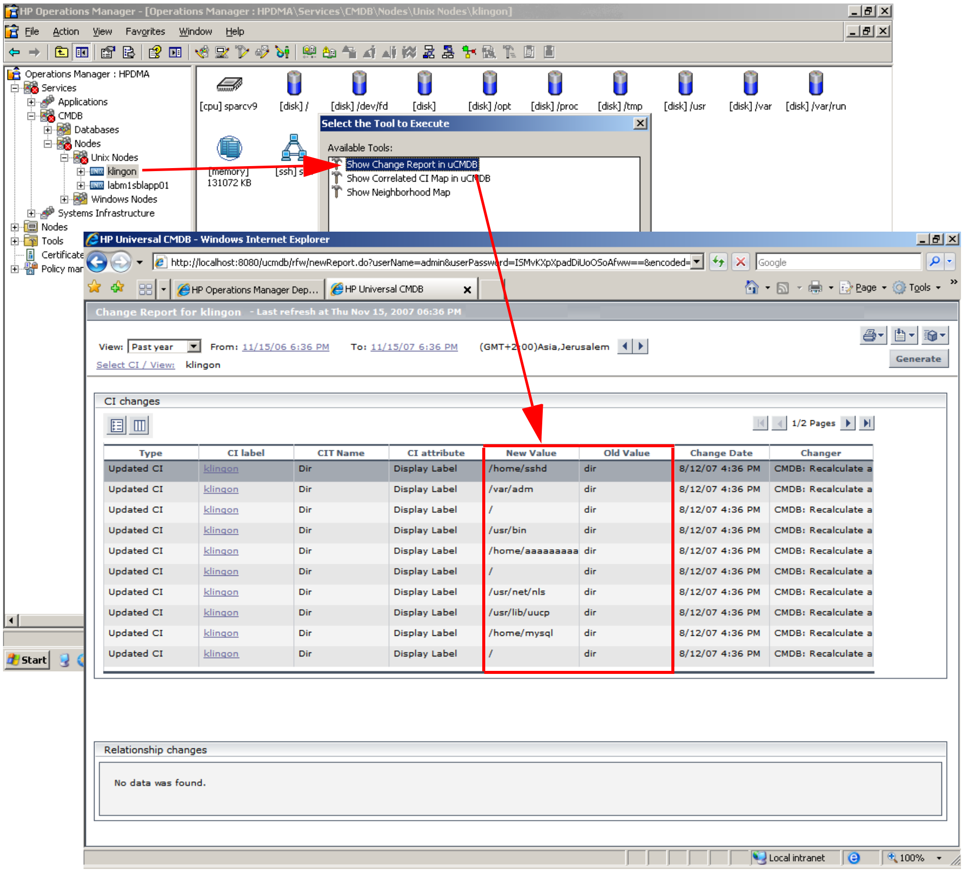
Surveys show that the majority of IT infrastructure incidents are caused by uncoordinated changes, such as equipment moves, configuration changes, or minor software or firmware updates. These changes often happen outside of the sanctioned change management processes, so there is no formal record of them in the change management system.

UCMDB discovery mechanisms have the ability to detect and record a wide variety of configuration changes to infrastructure elements. These changes are stored within UCMDB, and are available from within HPOM when HPOM DMA is installed.

When your operators see a notification of an infrastructure event within HPOM, using UI Launch, they can drill down directly into UCMDB change history. Your operators can review the change history for the impacted CI to determine if a recent change may be the root cause of the event. UI Launch significantly enhances the operator's ability to diagnose an event, and speeds up the problem analysis and resolution processes.

Figure 2 shows that the UNIX node klingon has encountered an issue (klingon is shown with a critical red status). Launching the change history facility enables viewing of UCMDB data. It reveals that a number of directory manes have been changed, and that this may be causing some issues.

Figure 2 UI Launch from HPOM to Show Change Report



Change Report for klingon - Last refresh at Thu Nov 15, 2007 06:36 PM

View: Past year From: 11/15/06 6:36 PM To: 11/15/07 6:36 PM (GMT+2:00)Asia,Jerusalem

Select CI / View: klingon

CI changes

Type	CI label	CIT Name	CI attribute	New Value	Old Value	Change Date	Changer
Updated CI	klingon	Dir	Display Label	/home/sshd	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/var/adm	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/usr/bin	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/home/aaaaaaaaa	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/usr/net/nls	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/usr/lib/uucp	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/home/mysql	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/	dir	8/12/07 4:36 PM	CMDB: Recalculate a

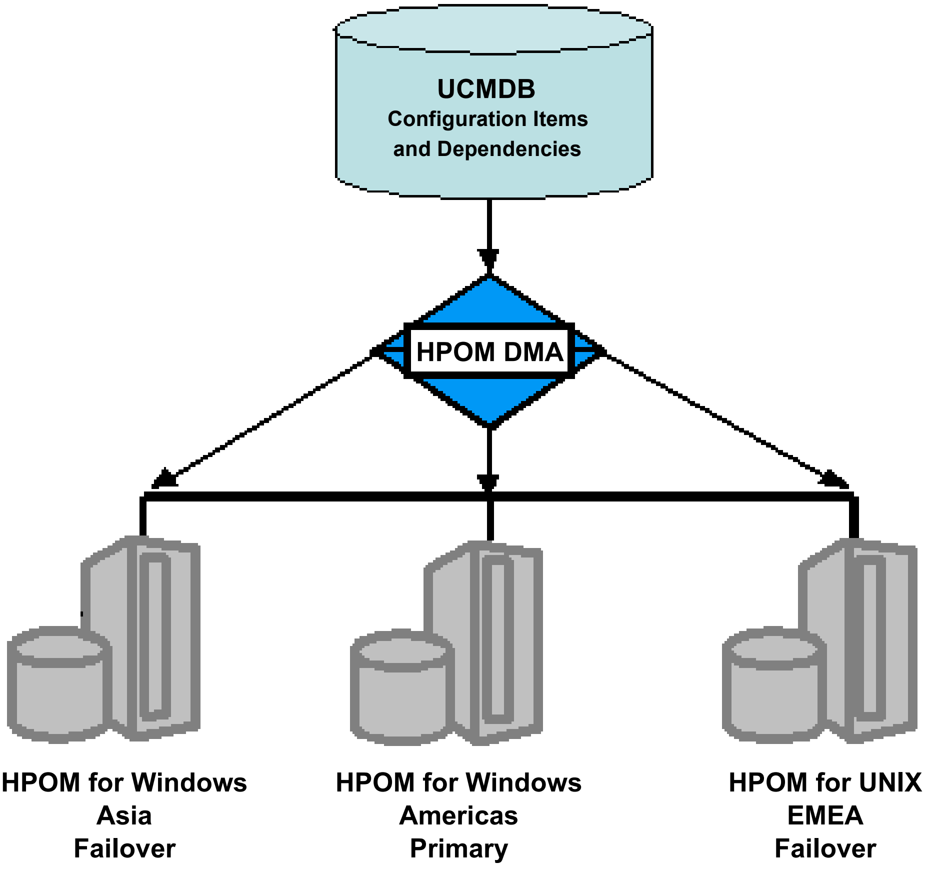
Relationship changes

No data was found.

Sharing Configuration Item Information

In environments where multiple HPOM servers are used in disaster-tolerant and failover configurations, it is vital that node data is replicated across cooperating HPOM servers. Replication of key parts of the service maps is equally important where HPOM servers participate in expert center or follow-the-sun architectures. However, maintaining a consistent set of node lists and service map objects across two or more HPOM servers can involve time-consuming manual processes. Whenever manual processes are involved, discrepancies and errors can occur.

Figure 3 Multiple HPOM Servers Sharing UCMDB Data



Using HPOM DMA, multiple HPOM servers can consume node lists and service object information from a single UCMDB. UCMDB provides the single source for this information. All HPOM servers connected to UCMDB can see exactly the same CIs.

Figure 3 shows three HPOM servers sharing node list and service object information from a single UCMDB.

Identifying New Servers and Applications

Monitoring key servers and the applications that support business processes is a vital step in ensuring that the activities of IT are aligned with the business. In complex environments, tracking and ensuring that all relevant servers are adequately monitored can be a time-consuming manual process.

HPOM DMA can take the guesswork out of this activity. As new servers are installed, updated, or have new applications deployed to them, UCMDB discovery processes detect these changes. New systems and services, and changes to existing ones, are stored in UCMDB and are available to HPOM DMA. HPOM DMA populates the node banks and service maps within HPOM with information about systems and services that are not currently monitored.

Because HPOM DMA derives system, application and business service dependency information from the data in UCMDB, it helps operational staff to identify which new systems are important. Using the business service dependency information in the Service Maps, you can identify new systems (or changed systems) that fulfill a role in delivering key business services and that need specific monitoring.

You can also automate the deployment of monitoring to new or updated nodes.

2 HPOM DMA Users

This chapter contains the following sections:

Service View Designers

Service view designers are responsible for designing service views for HPOM Service Navigator. Service views are used by HPOM operators to fulfill their tasks. Service view designers must also regularly keep the service models up to date. They know the operational management processes of their organizations, and have a solid understanding of the application topologies. They are involved in both testing and production environments and are not expected to have programming skills.

Service view designers create design specifications for applications at the class level. If necessary, they get input on application details and application topology from application experts and HPOM operators. Service Navigator topology requirements are necessary for troubleshooting. They then implement the design specifications into TQL queries, which define the node and service CIs in UCMDB to be synchronized with HPOM. And finally, they map CI types to Service Type Definitions (STD), which are used to identify how CIs from UCMDB are to be handled when building services in HPOM on synchronization.

Service view designers are also responsible for configuring the import schedule for extracting CIs from UCMDB and importing them into HPOM. This task can be delegated to the HPOM administrator.

UCMDB Discovery Administrators

UCMDB discovery administrators configure discovery mechanisms in UCMDB to automatically keep the CMDB up to date through discovery. They must make sure that discovery data fulfills the needs of all UCMDB users. UCMDB discovery administrators are involved in both testing and production environments. They are required to have some programming skills if new discovery scripts need to be developed. UCMDB discovery administrator should also be able to extend discovery.

Integrators

Integrators design and develop the following:

- Management policies
- Discovery policies
- Tools and actions
- Instrumentation
- Report templates
- Graphs
- Service Type Definitions (STD)

Integrators have a very thorough knowledge of the application that they are integrating (for example, Oracle, Exchange, and HPOM components such as policies). They typically work in a separate development environment.

Typically, integrators also work with HPOM DMA to do the following:

- Create Synchronization packages.
- Write scripts to extend the synchronization process.

- Enhance services in HPOM which are not derived from UCMDB with data from UCMDB.

Integrators create synchronization packages with significant value for their partners. They deliver the knowledge of how to manage an application to ensure availability and peak performance. The main integration-specific task is to create the STDs. These can also be created automatically. For details, see Creating Service Type Definitions Automatically on page 100.

Integrators must make sure synchronization packages are updated to work with the latest releases of HPOM, operating systems, and application platforms, and achieve an acceptable balance between time pressures and the required synchronization package functionality. They must also design synchronization packages that can be used in environments of very differing size and complexity, while meeting the monitoring needs of operators and second level support. Integrators should have some “real-world” application administration knowledge.

HPOM Administrators

HPOM administrators are responsible for installing and configuring the HPOM environment including the database and agent setup. Configuration tasks include security configuration with users, user roles, flexible management (for example, manager-to-manager configuration), and backup and database maintenance.

HPOM administrators need to be trained on the administrative aspects of HPOM and related products. They are involved in both testing and production environments.

HPOM administrators are required to guarantee the continuous operation of the management environment and ensure timely adaptation of management systems. They must keep up to date with environmental and organizational changes (for example, security requirements), and monitor expansion of the environment. HPOM administrators need to be able to work with multiple technologies.

HPOM administrators set up node groups and implement the top-level services in Service Navigator. A top-level service can be some generic service or container to give the hierarchy a structure. These include infrastructure services, applications, business services, and regions.

HPOM administrators must also configure the import schedule for extracting CIs from UCMDB and importing them into HPOM. This task may be performed by a specialist service view designer.

HPOM Operators

HPOM operators are responsible for the operational status of the managed environment, including messages. They work on incoming messages, execute predefined actions, and troubleshoot using predefined workflows. More complex problems may require HPOM operators to create trouble tickets.

HPOM operators need to be trained on the operational procedures of managing the IT environment with HPOM and related products. They work in production environments.

HPOM operators must resolve problems as quick as possible with the help of service trees and the message browser. They can use HPOM DMA to drill down into HP Business Availability Center (BAC) or Universal CMDB (UCMDB) to retrieve more detailed information.

Application Support Engineers

Application support engineers work on trouble tickets to solve problems through detailed problem analysis and changing the configuration of managed objects. More complex problems may require HPOM operators to create new trouble tickets.

Application support engineers need in-depth application knowledge to be able to troubleshoot the installation and resolve problems. They work in production environments, ensuring timely adaptation of the managed application, and guaranteeing continuous operation of the system or application. They can use HPOM DMA to drill down into BAC or UCMDB to retrieve more detailed information.

3 Concepts of HPOM DMA

This chapter explains the HPOM DMA concepts in more detail, including:

- Synchronizing Data on page 27
- Mapping HPOM Messages to Services Synchronized from UCMDB on page 40
- Discovering Services on page 44

Synchronizing Data

HPOM DMA uses TQL queries to retrieve data from BAC or UCMDB, and import nodes and create service hierarchies in HPOM. Figure 4 shows the synchronization process.

Figure 4 HPOM DMA Synchronization Process

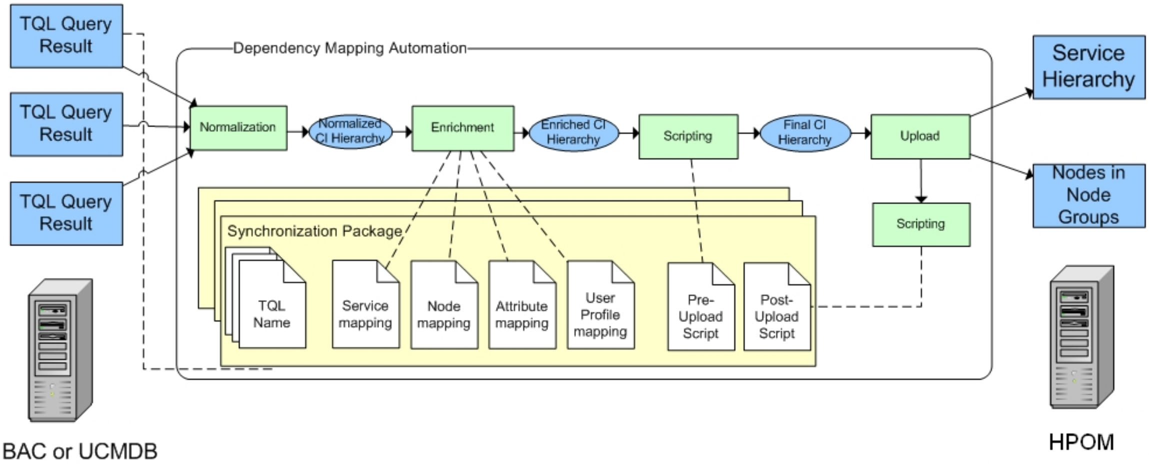
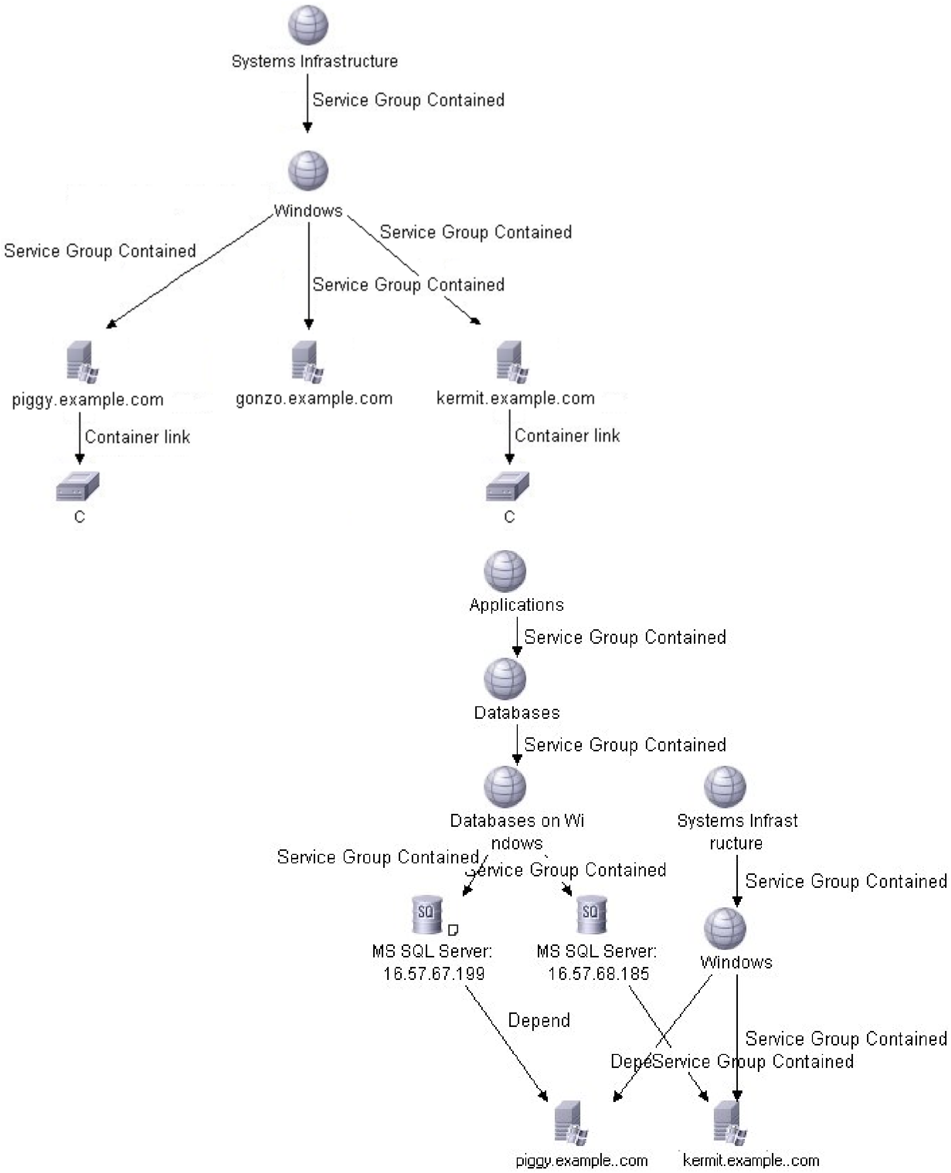


Figure 5 shows the result of two TQL queries: `MS SQL` and `WIN OS`. These are used as examples in the rest of this chapter.

Figure 5 TQL Query Examples



During a synchronization, the following steps are executed by HPOM DMA:

- Configuring Active Synchronization Tasks
- Getting Data from BAC or UCMDB
- Creating CI Hierarchies
- Enriching CI Hierarchies with Mapping Rules
- Manipulating CI Hierarchies with Scripting

These steps are described in the following sections.

Configuring Active Synchronization Tasks

The active synchronization task contains the following information:

- Root service: The service under which the CI data is added. By default, this is `CMDB`.
- The content that you want to synchronize: The possibilities are CIs with services, and CIs with nodes or both. By default, both are selected.
- TQL queries, mapping rules and scripts from all active synchronization packages.

  > Synchronization packages are containers that can have multiple TQL queries, mapping rules, and scripts. Each synchronization package has a priority that determines in which sequence the mapping rules and scripts are executed. The synchronization package concept supports easy extensibility.

In this example, three synchronization packages are active:

- **Databases**
  - Links to the `MS SQL` TQL
  - Contains Mapping rules
- **Systems**
  - Links to the `Win OS` TQL
  - Contains Mapping rules
- **Default**
  - No data
  - Contains mapping rules

Getting Data from BAC or UCMDB

You retrieve data from UCMDB or BAC by getting the result of all active TQL queries. In the example shown in Figure 5 on page 28, you retrieve the result of the `MS SQL` and the `WIN OS` TQL queries.

Creating CI Hierarchies

HPOM Service Hierarchy distinguishes between two relationship types:

- Containment
- Dependency

The mapping from UCMDB relationship types to HPOM relationship types is preset:

> A containment relationship can be configured using the `<containmentrelations>` list of regular expressions. You can choose which relationship types are mapped to containment. This is specified in the `containmentrelation.xml` file. The default configuration maps all relationship types starting with `container`.

All other relationship type in UCMDB is mapped to `dependency`.

The configuration that specifies which CIs are added as nodes in HPOM is done using node types. Node types are specified using an XML file. By default, the node types are `unix`, `nt` and `host`.

Each CI that is not contained within another CI is treated as a top-level CI. A CI hierarchy is created for each top-level CI and all its children are contained in this hierarchy.

The example shows two service hierarchies with the following top-level CIs:

- `Applications`
- `System Infrastructure`

Enriching CI Hierarchies with Mapping Rules

You enrich the normalized CI hierarchies by creating the following mappings:

- Applying Service Mapping on page 31
- Applying Node Mapping on page 33
- Applying Attribute Mapping on page 34
- Assigning User Roles and Profiles on page 37

Applying Service Mapping

For all CIs that are added to HPOM as service, a service mapping is necessary. In UCMDB, CIs are of a specific CI type. In HPOM, services are of a specific service type. Service mappings are a set of rules that defines how to map CI types to service types.

In the example data, there are three CI types:

- `sqlserver`
- `servicegroup`
- `nt`

In the example, HPOM DMA uses service mapping rules to assign service types to CIs as follows:

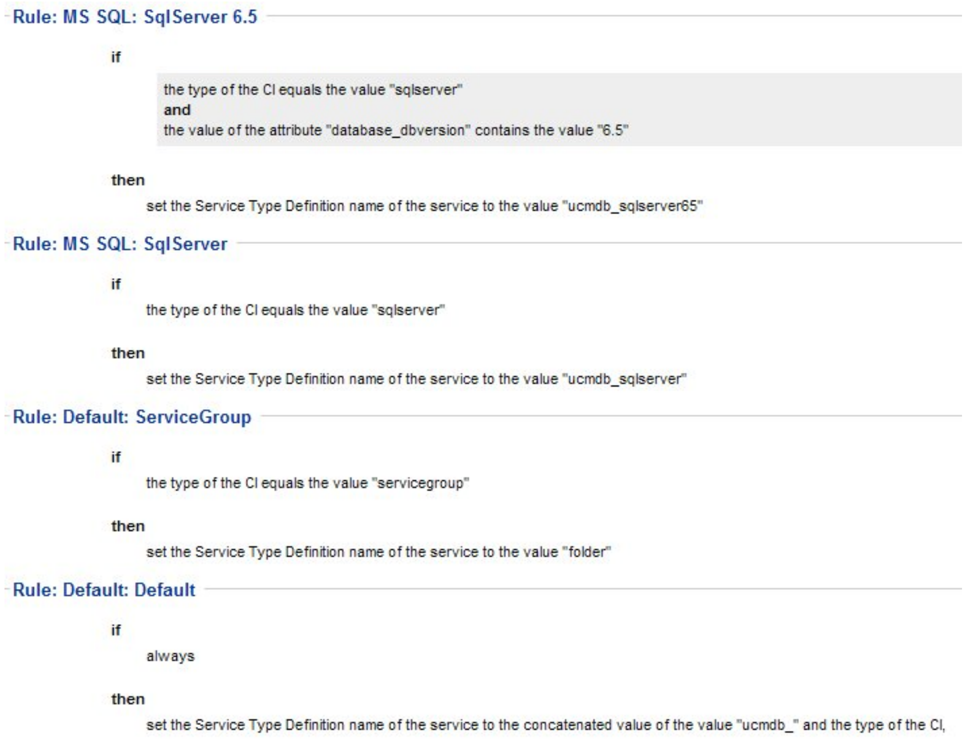
- The `MS SQL: SqlServer 6.5` checks whether a CI is of type `sqlserver` and dbversion is `6.5`.For CIs that meet these criteria, they are assigned the service type `ucmdb_sqlserver65`.
- To all other CIs of type `sqlserver`, the `MS SQL: SqlServer` rule assigns the service type `ucmdb_sqlserver`.
- All CIs of type `service group` are assigned the service type `folder` by the `Default: ServiceGroup` rule.
- For all other CIs, the service type `ucmdb_<CI Type>` is assigned by the `Default:Default` rule.

Service type definitions (STDs) are used to identify how CIs from UCMDB are to be handled when building services in HPOM on synchronization. If an STD for an imported CI is not available in HPOM, it cannot be displayed in the Service Navigator. An error message is displayed explaining that STDs are missing.

HPOM DMA can automatically create STDs to suit non-matching CIs as they are imported into HPOM. For details, see Creating Service Type Definitions Automatically on page 100.

Figure 6 shows examples of service mapping rules.

Figure 6 Service Mapping Rules



Rule: MS SQL: SqlServer 6.5

if

the type of the CI equals the value "sqlserver"
and
the value of the attribute "database_dbversion" contains the value "6.5"

then

set the Service Type Definition name of the service to the value "ucmdb_sqlserver65"

Rule: MS SQL: SqlServer

if

the type of the CI equals the value "sqlserver"

then

set the Service Type Definition name of the service to the value "ucmdb_sqlserver"

Rule: Default: ServiceGroup

if

the type of the CI equals the value "servicegroup"

then

set the Service Type Definition name of the service to the value "folder"

Rule: Default: Default

if

always

then

set the Service Type Definition name of the service to the concatenated value of the value "ucmdb_" and the type of the CI,

The second rule is not actually needed. The rule `Default:Default` produces the same result. If the `ucmdb_<CI Type>` pattern meets your needs, there is no need to write new rules. New rules are needed for specific mappings only. For example, when you add version information to your service type.

The order of rules is important because only one service type can be assigned to a service. The order of rules can be viewed in the HPOM DMA console:

Enrichment Summary → Service Mapping

Rule order is established using the priority of the synchronization packages.

Applying Node Mapping

All UCMDB CIs that are added to the HPOM node bank are assigned to the node group `CMDB`. Nodes that were previously included in the synchronization information from UCMDB, but are no longer present in the synchronization are moved from the `CMDB` node group to the `CMDB_Removed` node group. This cannot be changed.

Additionally, for all CIs that are added to HPOM node bank, a node mapping can be specified. Using these node mapping rules, nodes can be added to matching node groups in HPOM.

By default, HPOM DMA imports all the nodes discovered by UCMDB to node groups `CMDB` and `CMDB_Removed`. However, the nodes which already exist in user-defined node groups in HPOM are also moved to these default node groups. unless you define node mapping rules to place particular nodes in specified node groups, nodes from UCMDB are always placed in the `CMDB` and `CMDB_Removed` node groups.

In this way, the node group assignment process is fully automated. This is especially helpful for environments containing many thousands of nodes arranged in, possibly, hundreds of node groups. In some environments, node assignment may be changing dynamically. In such environments, handling the assignments manually is no longer advantageous.

If a node is synchronized through HPOM DMA, its node group assignments are controlled by HPOM DMA. This avoids conflicts between manual and automated changes. It is not possible to let HPOM DMA decide whether a particular manual change should be overridden. Managing nodes is clearer and easier if a node is either controlled by HPOM DMA or manually.

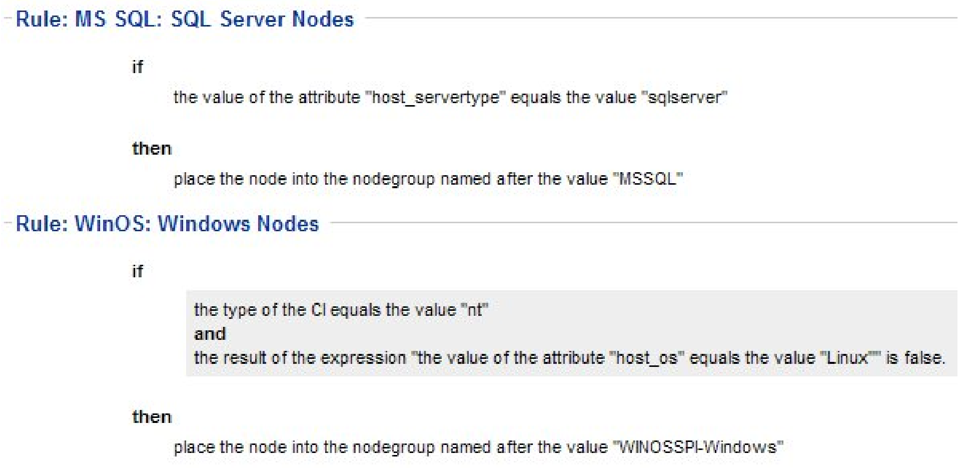
If you do not want HPOM DMA to change the node group of an existing node, this node must be excluded from the TQL and cannot be managed by DMA at all.

For node mapping, the order is not important because a node can be added to many node groups.

In Figure 5 on page 28, the nodes `kermit.example.com` and `piggy.example.com` are placed in the node groups: `MSSQL` and `WINOSSPI-Windows`. The node `gonzo.example.com` is placed only in the node group `WINOSSPI-Windows`.

Figure 7 shows examples of node mapping rules.

Figure 7 Node Mapping Rules



Rule: MS SQL: SQL Server Nodes

if

the value of the attribute "host_servertype" equals the value "sqlserver"

then

place the node into the nodegroup named after the value "MSSQL"

Rule: WinOS: Windows Nodes

if

the type of the CI equals the value "nt"
and
the result of the expression "the value of the attribute "host_os" equals the value "Linux"" is false.

then

place the node into the nodegroup named after the value "WINOSSPI-Windows"

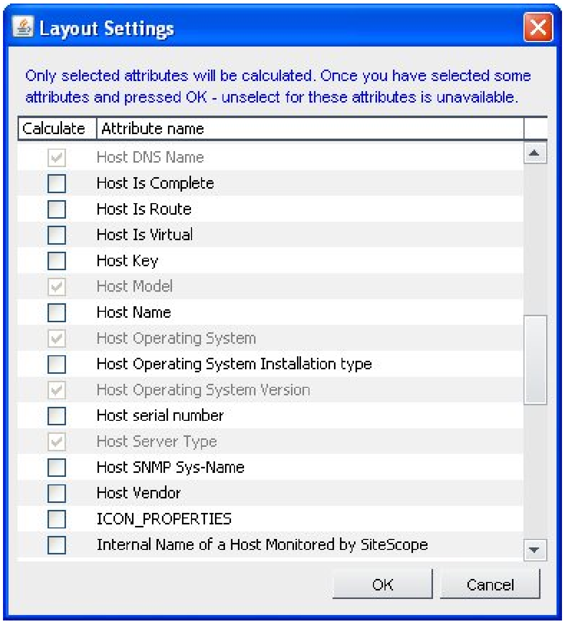
To view the rules in the HPOM DMA console, select:

Enrichment Summary → Node Mapping

Applying Attribute Mapping

All attributes that are selected in the Advanced Layout Settings of the TQL query are available for HPOM. The Advanced Layout Settings are located under the Node Conditions for the associated TQL query. An example is illustrated in Figure 8.

Figure 8 Advanced Layout Settings



Layout Settings

Only selected attributes will be calculated. Once you have selected some attributes and pressed OK - unselect for these attributes is unavailable.

Calculate	Attribute name
☑	Host DNS Name
□	Host Is Complete
□	Host Is Route
□	Host Is Virtual
□	Host Key
☑	Host Model
□	Host Name
☑	Host Operating System
□	Host Operating System Installation type
☑	Host Operating System Version
□	Host serial number
☑	Host Server Type
□	Host SNMP Sys-Name
□	Host Vendor
□	ICON_PROPERTIES
□	Internal Name of a Host Monitored by SiteScope

These UCMDB CI attributes are added to the internal CI hierarchies. Using attribute mapping, they can be changed or new attributes can be added.

Attribute mapping is useful for the following:

- Better matching of messages to services.
- Assigning attributes to existing service or node attributes (for example, display label, propagation and calculation rules, and node attributes).

For the examples, you do not need extra attribute mapping. The default attribute mapping maps some essential node attributes. For example, it sets specific node attributes (`ovo_osType`, `ovo_systemType`, `ovo_osVersion`) on CIs that are nodes. These attributes are required to correctly create the nodes in HPOM.

The order of rules is important if you set the same HPOM service or node attribute twice.

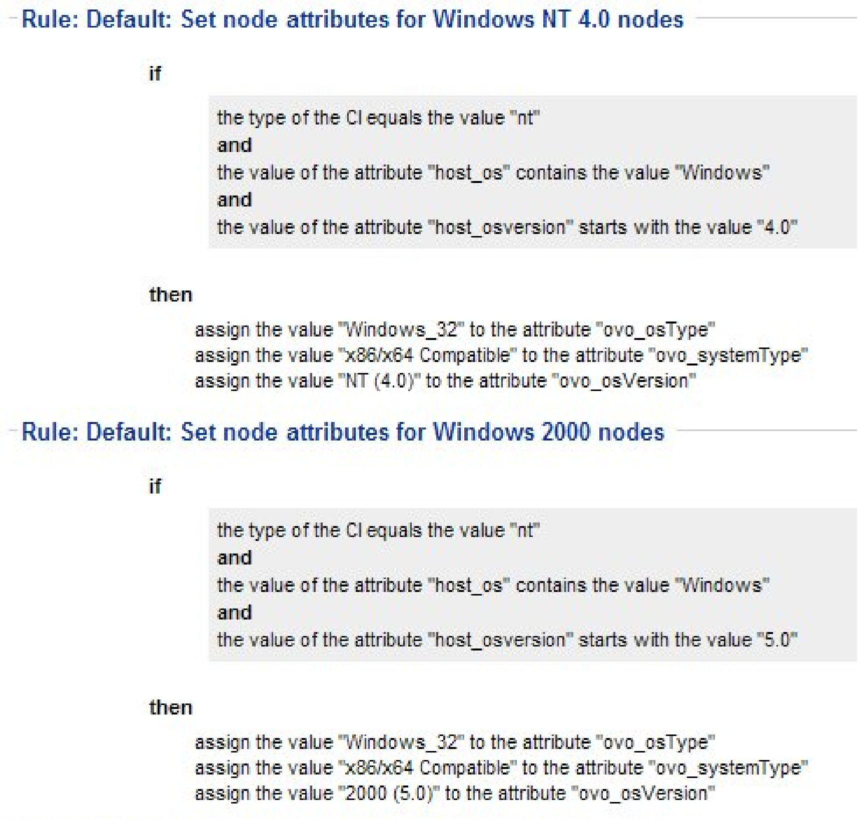
To view the rules in the HPOM DMA console, select:

Enrichment Summary → Attribute Mapping

You can manipulate it by changing the priority of the synchronization packages.

Figure 9 shows examples of attribute mapping rules.

Figure 9 Attribute Mapping Rules



Rule: Default: Set node attributes for Windows NT 4.0 nodes

if

the type of the CI equals the value "nt"
and
the value of the attribute "host_os" contains the value "Windows"
and
the value of the attribute "host_osversion" starts with the value "4.0"

then

assign the value "Windows_32" to the attribute "ovo_osType"
assign the value "x86/x64 Compatible" to the attribute "ovo_systemType"
assign the value "NT (4.0)" to the attribute "ovo_osVersion"

Rule: Default: Set node attributes for Windows 2000 nodes

if

the type of the CI equals the value "nt"
and
the value of the attribute "host_os" contains the value "Windows"
and
the value of the attribute "host_osversion" starts with the value "5.0"

then

assign the value "Windows_32" to the attribute "ovo_osType"
assign the value "x86/x64 Compatible" to the attribute "ovo_systemType"
assign the value "2000 (5.0)" to the attribute "ovo_osVersion"

Assigning User Roles and Profiles

User Profile or User Role Assignment enables you to map a service to an HPOM user profile or role.

After synchronization, the service is assigned to all operators that are included in the specified HPOM user profile or role:

- **HPOM for UNIX**

  User profiles are used for service assignment.

- **HPOM for Windows**

  User roles are used for service assignment.

In the example, all MS SQL database are assigned to the user profile `DatabaseAdmin`.

➤ Differences between UNIX and Windows:

- **In HPOM for UNIX**

  If no user profiles are assigned to a user, the user is not assigned any services or node groups.

  All services are assigned to user profiles.

- **HPOM for Windows**

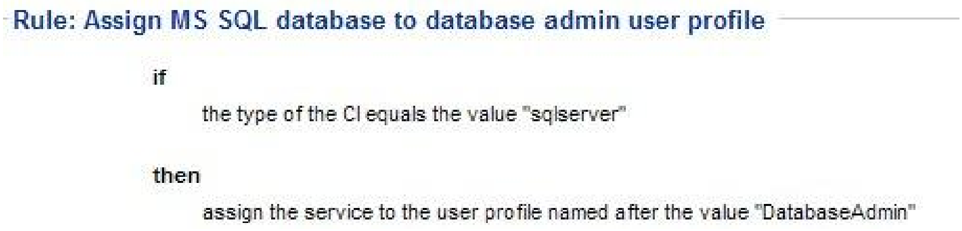
  If no user roles are assigned to a user, the user sees all services, and node groups.

  Use roles can only get services assigned that are of type folder.

For details, see Assigning User Profiles for Services on HPOM for UNIX on page 101 and Assigning User Roles for Services on HPOM for Windows on page 107.

Figure 10 shows examples of user profile mapping rules.

Figure 10 User Profile Mapping Rules



Rule: Assign MS SQL database to database admin user profile

if

the type of the CI equals the value "sqlserver"

then

assign the service to the user profile named after the value "DatabaseAdmin"

To view the rules in the HPOM DMA console, select:

Enrichment Summary → User Mapping

Manipulating CI Hierarchies with Scripting

Scripting enables you to perform additional processing and customization during to the synchronization process before and after the upload of nodes and services to HPOM. This is useful for all customization of the CI hierarchy that is not supported by enrichment, for example, grouping capabilities.

Additionally, there are use cases to trigger specific actions after the synchronization process is done. Typical use cases are:

- Start automatic policy deployment
- Send an email
- Send an `opcmsg` with details about the synchronization

One pre-upload and one post-upload script can be associated with each synchronization package. These optional script files are located in the associated synchronization package directory. For details, see Configuration Files on page 223.

The order of execution of scripts can be arranged by changing the priority of synchronization packages.

Associating script files with synchronization packages simplifies the distribution of scripts and enables script development to be handled independently of the working environment. The execution of synchronization scripts follows the settings of the synchronization packages:

- Only scripts in active synchronization packages are executed.

- Pre- and post-upload scripts are executed in the order of the priority of the synchronization packages.

  ⚠ Script execution is potentially insecure. In particular, the use of `DMA.exec(...)` commands can cause damage to an installation. Therefore script access for editing is allowed on the file system level only. This ensures that only users with log-on credentials to the DMA host can edit scripts. This protects the scripts by the log-on security of the DMA host.

You can view scripts in the HPOM DMA console under **Script Summary**.

➤ You can enable or disable synchronization package script execution from the **Content** page of the HPOM DMA console.

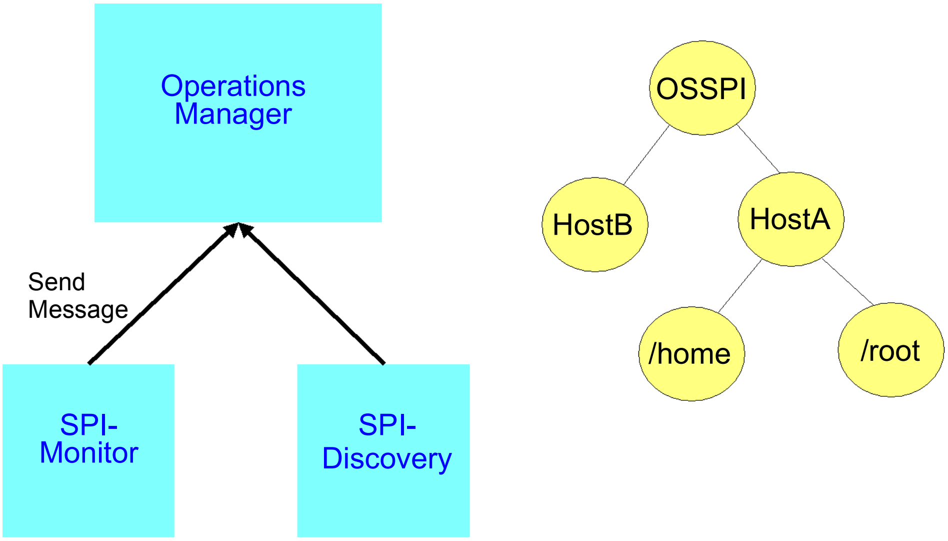
Mapping HPOM Messages to Services Synchronized from UCMDB

HPOM DMA introduces a new mapping approach called Smart Message Mapping (SMM). Using SMM, users can assign messages to services in Service Navigator, even if they do not know the exact service ID of that CI. This is required to match messages from an application (for example, a Smart Plug-In (SPI)) to the corresponding CIs imported into HPOM from UCMDB and, as a result, color the message in accordance with the severity reported by the message.

Traditional Mapping

Figure 11 shows the basic information flow from a SPI to HPOM and how the OSSPI organizes services.

Figure 11 Service Structure in HPOM



Using the traditional approach, you must address every service with an HPOM message containing a fully qualified service ID:

```
service_id="OSSPI:os:svc:filesystem:/home@@HostA"
```

```
service_id="OSSPI:os:filesystem:/home@@testsystem.example.com"
```

➤ The /home directory represent a file system on a UNIX system. A similar service ID from a Windows system would be:

```
service_id="OSSPI:os:svc:filesystem:C@@HostW"
```

The complete HPOM message used to send a message to the given service is handled by the opcmsg command and appears as follows:

```
opcmsg a="HP OSSPI" o="Filesystem" node=testsystem.example.com
service_id="OSSPI:os:filesystem:/home@@testsystem.example.com"
msg_text="Filesystem is down."
```

Service IDs are generated by the SPI discovery and uploaded into the Status Engine using a proprietary API. Using the service ID, SPIs can send HPOM messages to change the service status. Therefore, it is essential to use the exact service ID created during discovery. This process of using exact service IDs is difficult to maintain and hard to use for end users because of the complex service ID structure.

Smart Message Mapping

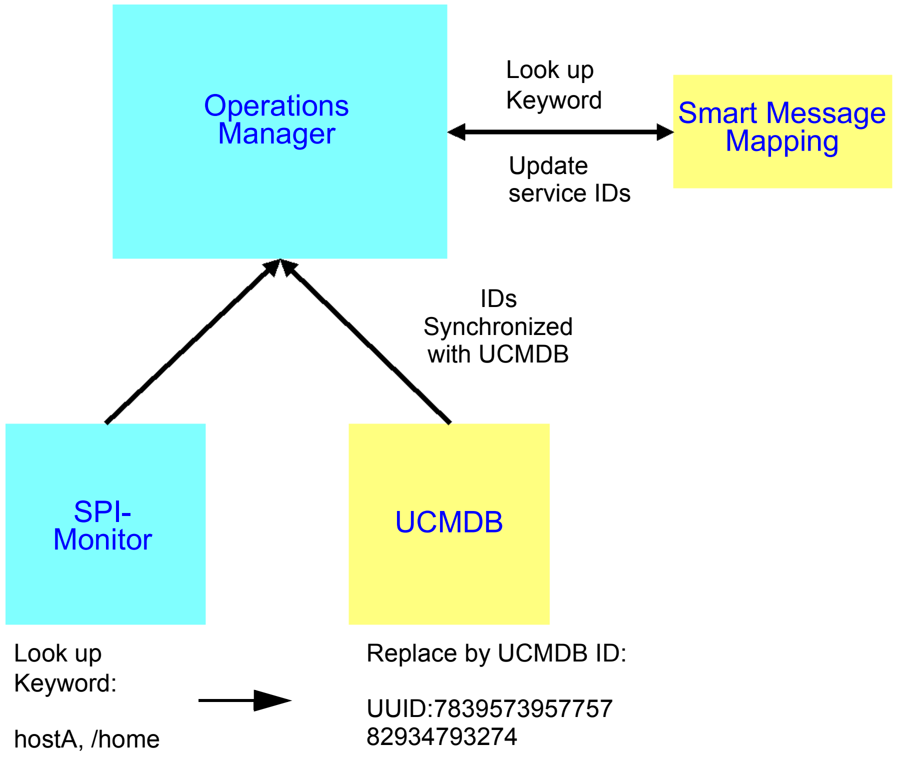
With HPOM DMA, service IDs generated by UCMDB are used to identify services in Service Navigator. Service IDs are no longer governed by HPOM SPIs.

Smart Message Mapping is used to identify services to which a SPI is trying to send a status message. Services can be addressed by keywords that are automatically matched to services by HPOM. The algorithm is used to identify the service by a more intuitive approach. It compares the details or keywords contained in a message with the attributes of all services and selects the one with the best match. The message is then sent to this service.

Smart Message Mapping examines incoming messages. Where necessary, it breaks them down into a collection of attributes. It then compares this set with the available services and finds the best match. The message is then forwarded to the corresponding service in HPOM and its severity value is used to appropriately color the service icon. If no match is found, the message is forwarded unchanged.

Figure 12 shows how Smart Message Mapping identifies the source of message and directs it to the correct service in HPOM.

Figure 12 Keyword Look Up



With Smart Message Mapping, `node=<hostname>` and `object="/home"` is all that is required to identify the service.

```
node=testsystem.example.com object="/home"
```

Service IDs can also be specified using their `@@` notation. The equivalent syntax would then be:

```
service_id=/home@@testsystem.example.com
```

The complete HPOM message used to send a message to the given service is handled by the `opcmsg` command and would appear as follows:

```
opcmsg a="HP OSSPI" o="Filesystem:/home"
node=testsystem.example.com msg_text="Filesystem is down."
```

The advantage of this approach is that you can send a message to a service even when you only know a subset of these keywords. In this case, the best fitting service is selected as the target. However, if the SPI-generated Service ID is available in the message, the message is sent to the specified service without any further processing.

The message can contain a list of multiple keywords, separated by colons:

```
/home:filesystem:device
```

If the service ID of the message already exists in HPOM, no further identification is necessary and the message is forwarded to this service. If the service cannot be initially identified, the Smart Message Mapper tries to match:

- As many keywords as possible.
- At least one keyword.

As a fallback, the Smart Message Mapper uses the host service.

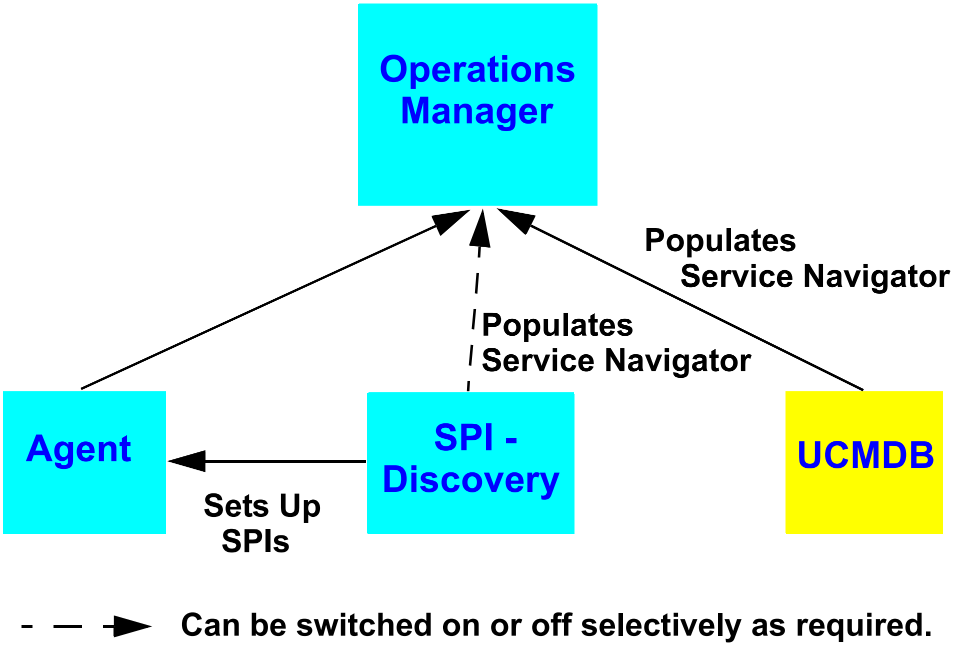
Discovering Services

You can choose how to discover your services in Service Navigator. The two types of discovery sources are:

- SPI discovery
- UCMDB discovery

You are able to use UCMDB-based discovery as the source for displaying services in Service Navigator but continue to use SPIs for monitoring, as shown in Figure 13. If both UCMDB- and the SPI-based discoveries are activated, you see two service trees in Service Navigator. SPI-generated messages are used to identify status in the SPI-based discovery service tree. You are able to use a phased approach to switching to HPOM DMA. You initially import the services and nodes, and then you switch off the upload of the SPI discovery result. SPI monitoring continues to work as originally configured.

Figure 13 Selecting the Discovery Source


Operations Manager
Populates Service Navigator
Populates Service Navigator
Agent
SPI - Discovery
UCMDB
Sets Up SPIs
Can be switched on or off selectively as required.

When you are satisfied that the service tree derived from UCMDB discovery is being correctly displayed, you can disable the service upload of the SPI discovery and delete the service tree generated from the SPI discovery. This avoids displaying two instances of the same service.

4 Preparing HPOM DMA

Installation Distribution

HP Operations Manager Dependency Mapping Automation (HPOM DMA) requires the following three software components:

- HPOM for Windows or HPOM for UNIX installation
- HP Universal CMDB or HP Business Availability Center (BAC) installation
- HPOM DMA installation on the HPOM host system

You can arrange the software on your hardware as follows:

- The HPOM installation must be able to access UCMDB or BAC installations over the network. On Windows, the HPOM and UCMDB or BAC installations can be on the same host system, but this is not recommended because of performance considerations.
- HPOM DMA must be installed on the system hosting the HPOM management server system, with the exception of HPOM for UNIX installations on HP-UX 11.23 and HP-UX 11.31 PA-RISC 64-bit systems. For these installations, HPOM DMA must be installed on a proxy system running a Windows operating system.

Product Prerequisites

This section specifies the hardware and software you require before installing HPOM DMA.

HP Operations Manager

Make sure one of the HP Operations Manager products is installed:

- **HPOM for UNIX**
  - Version 8.27 or higher

    Hosted on a system running one of the following operating systems:

    - HP-UX 11.23 on PA-RISC 64-bit systems (remote access only using a proxy system running a Windows operating system)
    - HP-UX 11.23 (11i v2.0) on Intel Itanium® 64-bit systems
    - HP-UX 11.23 PI on Intel Itanium 64-bit systems
    - HP-UX 11.31 on PA-RISC 64-bit systems (remote access only using a proxy system running a Windows operating system)
    - HP-UX 11.31 on Intel Itanium 64-bit systems
    - Sun Microsystems Solaris 9, Solaris 10
    - MC/Service Guard 11.17 (HP-UX 11.23, 11.31)
    - Sun Microsystems Cluster 3.1 (Solaris 9, Solaris 10)
    - Veritas Cluster Server 5.0 (HP-UX 11.23, 11.31, Solaris 9, Solaris 10)

➤ An X server is required on any UNIX system on which you want to display the HPOM console.

- **HPOM for Windows**
  - Version 8.10

    Hosted on a system running one of the following 32-bit operating systems:

    - Windows Server 2003, Std./Ent./DC Ed. (including SP1, SP2, or R2)
    - Microsoft Windows Server 2008
    - Windows 2003 Compute Cluster Service (including SP1, SP2, or R2)
    - Windows 2008 Compute Cluster Service

Proxy System for HPOM for UNIX on PA-RISC Systems

The proxy system hosting HPOM DMA must be running one of the following 32-bit operating systems:

- Windows Server 2003, Std./Ent./DC Ed. (including SP1, SP2, R2)
- Windows 2003 Compute Cluster Service (including SP1, SP2, R2)

HP Universal CMDB or HP Business Availability Center

Make sure one of the following products is installed:

- **HP Business Availability Center 7.00 or 7.50**
- **HP Universal CMDB 7.00 or 7.50**

Advanced This edition enables discovery of all components at your site and the ability to federate with other data sources and reconcile CIs.

Standard This edition enables discovery of the infrastructure and network.

Free HP Universal CMDB includes the complete class model (all CI types) and all packages. (You populate UCMDB either manually or using integration.) HP Universal CMDB is provided without the discovery or federation features.

Select the Universal CMDB version that most suits your needs. However, to make the most of your HPOM DMA implementation, use the Advanced version. This version enables you to use all of the built-in features (for example, synchronization of database-related data using the synchronization packages) that are part of the HPOM DMA product.

The Operations Manager HTTPS Agent for Windows is assigned free ports at random during start up. This may conflict with the ports required by a UCMDB or BAC installation located on the same Windows System.

To avoid this conflict, start up UCMDB or BAC application before starting up the HTTPS Agent on the Windows System.

Hardware Requirements for HPOM DMA

Extra hardware requirements for installing HPOM DMA on the HPOM host system:

- 700 MB free disk space (maximum)
- 1 GB Additional RAM (during synchronization)

VMware Workstation Installations

HPOM DMA can be installed on a virtual system running in VMware Workstation. The same prerequisites must be met as for an installation on a physical system and support is only possible for problems reproducible on a physical system installation.

Installing HPOM DMA on a VMware virtual system for use in production environments is not recommended.

Browser Requirements for HPOM DMA

The following browsers are supported for displaying the HPOM DMA console:

- Microsoft Internet Explorer, version 6.0.x and 7.0.x
  - Microsoft Windows platforms
- Mozilla Firefox, version 2.0.x
  - HP-UX
  - Linux
  - Solaris
  - Windows

HPOM for UNIX Patches

This section describes the HPOM for UNIX patches you must install on the host system.

Patches are available from the following web site:

http://wtec.cup.hp.com/~patches/catalog/

Hotfixes must be obtained directly from the HP support organization.

HP-UX Itanium

The following HPOM for UNIX patches must be installed on the HPOM management server host system:

- **PHSS_37439**
  s700_800 11.X OV OVO8.X IA-64 consolidated server A.08.29
- **PHSS_37565**
  s700_800 11.X OV OVO8.X IA-64 Java™ GUI client A.08.29
- **PHSS_35416**
  s700_800 11.23 OV OVO8.X IA-64 Java Config API A.08.25 and Hotfix A.08.25 version of QXCR1000471867

HP-UX PA-RISC

The following HPOM for UNIX patches must be installed on the HPOM management server host system:

- **PHSS_37440**
  s700_800 11.X OV OVO8.X PA-RISC consolidated server A.08.29
- **PHSS_37566**
  s700_800 11.X OV OVO8.X PA-RISC Java GUI client A.08.29
- **PHSS_35417**
  s700_800 11.23 OV OVO8.X PA-RISC Java Config API A.08.25 and Hotfix A.08.25 version of QXCR1000471867

Sun Solaris

The following HPOM for UNIX patches must be installed on the HPOM management server host system:

- **ITOSOL_00653**
  sparcSOL 2.X OV OVO8.X consolidated server A.08.29
- **ITOSOL_00658**
  sparcSOL 2.X OV OVO8.X JavaGUI client A.08.29
- **ITOSOL_00528**
  sparcSOL 2.X OV OVO8.X Java Config API A.08.25 and
  Hotfix A.08.25 version of QXCR1000471867

DNS Requirements

You must configure the HPOM host system to use a domain name server (DNS) that can resolve host names and IP addresses correctly.

To test this, execute **`nslookup`** ***`<hostname>`*** at a command prompt on the management server. The command must return a fully qualified host name and IP address.

DNS must be set up so that the HPOM host system can resolve all hosts that are synchronized from UCMDB.

HPOM for UNIX Agents

If you want to import nodes of a particular operating system type, the agent software for that platform must be available on the HPOM for UNIX management server. If it is not included in the HPOM for UNIX media kit, download it from the HPOM for UNIX SSO web site:

http://support.openview.hp.com/patches/ito/ito.jsp

Additional Prerequisites and Configurations

Installing IIS after the .NET Framework on Windows HPOM DMA Systems

HPOM DMA uses Microsoft Active Server Pages .NET (ASP .NET) to connect to the Operations Manager for Windows server. If you install the .NET framework on a system that already has Microsoft Internet Information Services (IIS) installed, IIS is automatically configured to handle ASP .NET requests.

However, if you install IIS after the .NET framework, you must manually register ASP .NET with IIS by executing the following command in a Command Prompt window:

```
%SystemRoot%\Microsoft.NET\Framework\v2.0.50727\
aspnet_regiis -i
```

Set Up Discovery Data

HPOM DMA cannot work without specific UCMDB or BAC attributes. For example, the `Host DNS Name` attribute must be included so that nodes can be created and the `hosted_on` attribute can be set. Without this, Smart Message Mapping does not work. Make sure that discovery is set up correctly.

Information on how to set up discovery can be found in the online help under:

- *UCMDB*

  HELP → **UCMDB Help** → **Main Topics** → **Discovery**

- *BAC*

  HELP → **Documentation Library** → **Main Topics** → **Discovery**

Enable UI Launch from HPOM to BAC or UCMDB

To use BAC/UCMDB UI Launch from HPOM for Windows, you must install the Sun Java Plug-in, version 1.5.0 or higher, with an integration into your web browser.

To use the HPOM for UNIX Java console on Windows, you must install a Java SE Runtime Environment (JRE). It is recommended that you configure HPOM for UNIX applications to use Internet Explorer when accessing URLs.

The latest JRE can be downloaded from the following Sun Microsystems web site:

http://www.java.com

UCMDB or BAC User with CmdbOpenApiQuery Role Permissions

HPOM DMA accesses UCMDB or BAC through web services. For users to access UCMDB or BAC through these web services, they need to be granted web service access. To achieve this, a user account with `CmdbOpenApiQuery` permissions must be used. This user with appropriate permission must be specified during configuration of HPOM DMA.

UCMDB User Configuration

To set up and configure a user account with name and password, and access to the `CmdbOpenApiQuery` role, follow these steps:

1 From the UCMDB console, open the User Manager:

Admin → **Settings** → **User Manager**

2 Click **Add**.

The Add New User dialog box opens.

3 Enter a name and password and click **Next**.

4 *Optional:* Enter descriptive information for the user and click **Next**.

5 Check the `CmdbOpenApiQuery` role.

6 Click **Finish**.

7 To check, whether you have successfully granted web access to a user:

a Enter the connection URL into a browser, for example:

http://<*UCMDB_System_Hostname*>:8080/axis2/services/UcmdbService

If you get:

```
Please enable REST support in WEB-INF/conf/axis2.xml and
WEB-INF/web.xml
```

The user has the required web access.

b If access is denied, check for common errors, such as the name of the machine and the port number, and retry.

For further information, see the UCMDB online help.

BAC User Configuration

To set up and configure a user account with name and password, and access to the `CmdbOpenApiQuery` role, follow these steps:

1 From the BAC console, open the User and Permissions page:

Admin → Platform → Users and Permissions

2 If applicable, select a group and click **Create → Create User**.

The Create User dialog box opens.

3 Enter a name and password, the associated log-on name, and click **OK**.

4 Select the newly created user and click the Permissions tab.

5 Select the context **UCMDB WS API** and the item **cmdb.open.api**.

6 In the Predefined Roles tab, check the `CmdbOpenApiQuery` role.

7 Click **Apply Permissions**

8 Verify that you have successfully granted web access to a user:

a Enter the connection URL into a browser.

Example:

http://<*BAC_System_Hostname*>:8080/axis2/services/UcmdbService

The user has the required web access if you see the following message:

```
Please enable REST support in WEB-INF/conf/axis2.xml and
WEB-INF/web.xml
```

b If access is denied, check for common errors (for example, the hostname of the system and the port number), and retry.

For further information, see the BAC online help.

5 Installing HPOM DMA

The HPOM DMA installation installs the software onto the HPOM host system. This chapter guides you through all the required steps. This process should take approximately 60 minutes to complete.

Read the rest of this guide before you start the installation wizard to plan your decisions and gather the information that you need.

Installing on Clusters

HP Operations Manager Dependency Mapping Automation is cluster aware. It has the capability to switch over automatically to an alternative cluster system (failover) under the same conditions as HPOM. HPOM DMA belongs to the same XPL High Availability (HA) resource group as HPOM.

Applications running in a cluster environment are configured as HA Resource Groups. HA Resource Group is a generic term for cluster objects representing HA Applications. For further details on HPOM running in cluster environments, see the HPOM documentation.

For cluster-related information (for example, how to switch a system move from passive to active mode), see your clustering software documentation.

For enabling Smart Message Mapping in cluster environments, see Configuring Smart Message Mapping in Cluster Environments on page 65.

Applications Stopped and Restarted During Installation

This section describes applications that are stopped and restarted by the HPOM DMA application installation process. The restarts are performed for install, uninstall, and repair.

Applications on HPOM for UNIX

HPOM DMA stops and restarts the following applications:

- Cluster monitoring on cluster systems
- Local HPOM agent
- HPOM for UNIX
- All `ovc` applications including the OV Control Daemon (`ovcd`)

The restarts are performed for install, uninstall and repair.

Applications on HPOM for Windows

HPOM DMA stops and restarts the following applications:

- OV Auto Discovery
- OvTomcatB and any `ovc` applications that requires OvTomcatB

Repairing an HPOM DMA Installation

If your HPOM DMA installation is damaged, execute the installation procedure again and select the `Repair` option. The damaged files are replaced and HPOM DMA should be operational again. Your configuration files are not affected by the repair.

Loading the Installation Media on UNIX

To prepare for the HPOM DMA software installation from the product media, follow these steps:

1. Insert the product media into an appropriate DVD-ROM drive.
2. Create a directory to mount the drive:

   ```
   mkdir /<mount_point>
   ```

   Example:

   ```
   mkdir /dvdrom
   ```

3. Mount the DVD-ROM drive:

   ```
   mount -r -F cdfs /dev/<dvdrom_drive_name> /<mount_point>
   ```

   Example:

   For a local DVD-ROM, you can execute:

   ```
   mount -r -F cdfs /dev/dsk/c0t2d0 /dvdrom
   ```

   On HP-UX systems, you can also run SAM and mount the CD-ROM to a specific path in the Disks and File Systems window.

Installing HPOM DMA

Installing on Cluster Nodes

Installing HPOM DMA on a system participating in a cluster is supported on the active node only. An attempt to install HPOM DMA on a non-active node is rejected by the installer.

HPOM DMA must be individually installed on each node participating in the cluster. For each node in the cluster, make it the active node and install HPOM DMA on that node, following the instructions given in this chapter. Proceed with the next node in the cluster until HPOM DMA is installed on all cluster nodes.

To install HP Operations Manager Dependency Mapping Automation, follow these steps:

1 Start the application installer:

- *HP-UX and Solaris*

  ```
  <dvd-mountpoint>/hpdma_setup.sh
  ```

  For installation on PA-RISC systems, see Installing HPOM DMA for HPOM for UNIX on PA-RISC Systems.

- *Windows*

  a Close all open applications.

  b Insert the product media disk into the DVD drive of the system where HPOM for Windows is installed.

  If Autorun is enabled, the installation starts automatically.

  c If Autorun is disabled, do one of the following:

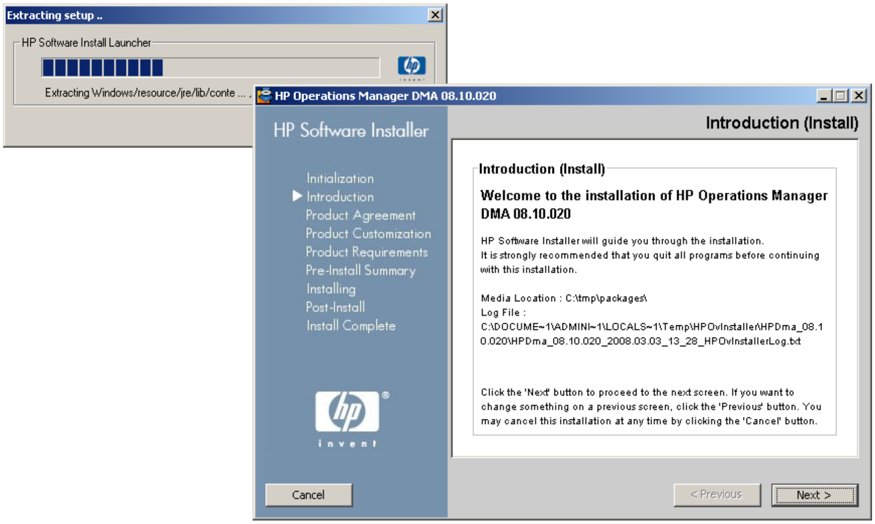
  – Execute the following in a command window:

  ```
  <dvd_drive>:\hpdma_setup.bat
  ```

  – Execute the `hpdma_setup.bat` executable file from an Explorer window.

Follow the on-screen instructions and progress through the installation process using the **Next** and **Install** buttons.

➤ The HPOM DMA installation location is dependent on the HPOM installation location. The HP Software Installer checks for this location. It is not possible to select an alternative for HPOM DMA.



Extracting setup ..

HP Software Install Launcher

Extracting Windows/resource/jre/lib/conte ...

HP Operations Manager DMA 08.10.020

HP Software Installer

Introduction (Install)

Introduction (Install)

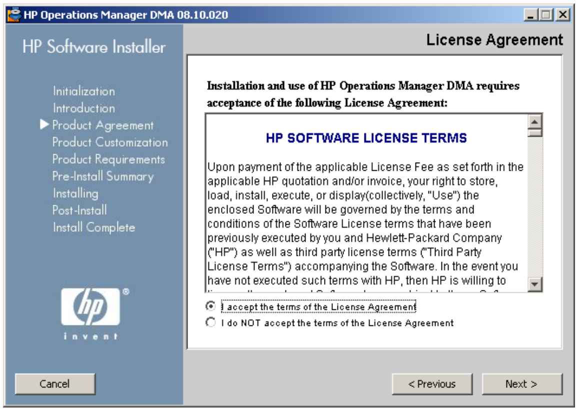
Welcome to the installation of HP Operations Manager DMA 08.10.020

HP Software Installer will guide you through the installation.
It is strongly recommended that you quit all programs before continuing with this installation.

Media Location : C:\tmp\packages\
Log File :
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\HPOvInstaller\HPDma_08.10.020\HPDma_08.10.020_2008.03.03_13_28_HPOvInstallerLog.txt

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button. You may cancel this installation at any time by clicking the 'Cancel' button.

2 Read and accept the Licence agreement and click **Next**.



HP Operations Manager DMA 08.10.020

HP Software Installer

License Agreement

Installation and use of HP Operations Manager DMA requires acceptance of the following License Agreement:

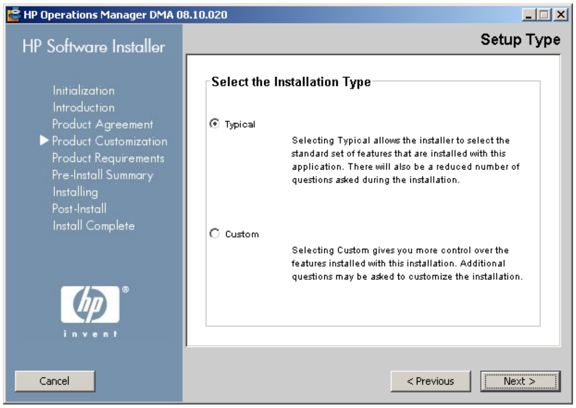
HP SOFTWARE LICENSE TERMS

Upon payment of the applicable License Fee as set forth in the applicable HP quotation and/or invoice, your right to store, load, install, execute, or display(collectively, "Use") the enclosed Software will be governed by the terms and conditions of the Software License terms that have been previously executed by you and Hewlett-Packard Company ("HP") as well as third party license terms ("Third Party License Terms") accompanying the Software. In the event you have not executed such terms with HP, then HP is willing to

● I accept the terms of the License Agreement
○ I do NOT accept the terms of the License Agreement

3 Select the **Typical** installation type and click **Next**.

The pre-install checks, including available disk space, are executed.



Select the Installation Type

● Typical

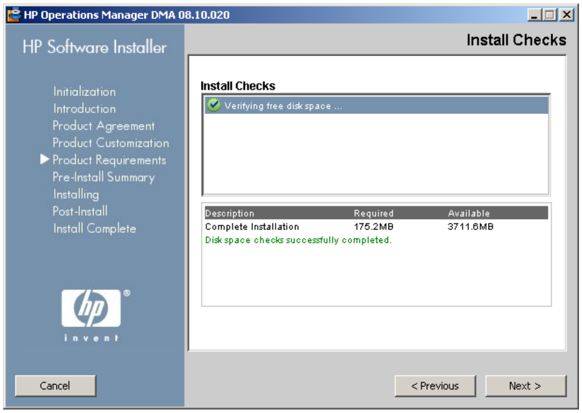
Selecting Typical allows the installer to select the standard set of features that are installed with this application. There will also be a reduced number of questions asked during the installation.

○ Custom

Selecting Custom gives you more control over the features installed with this installation. Additional questions may be asked to customize the installation.

4 If they complete successfully, click **Next**.

The pre-install summary lists the components to be installed or updated.



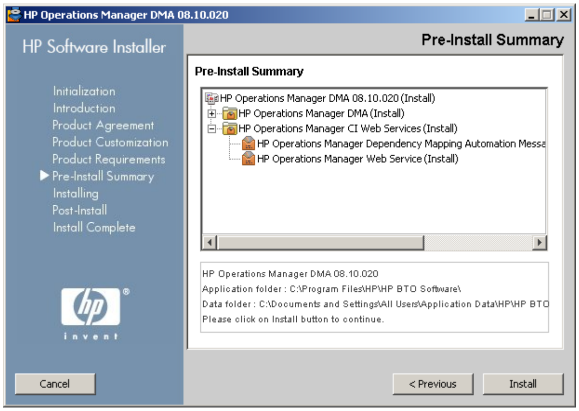
Install Checks

✓ Verifying free disk space ...

Description	Required	Available
Complete Installation	175.2MB	3711.6MB

Disk space checks successfully completed.

5 Click **Next**.



Pre-Install Summary

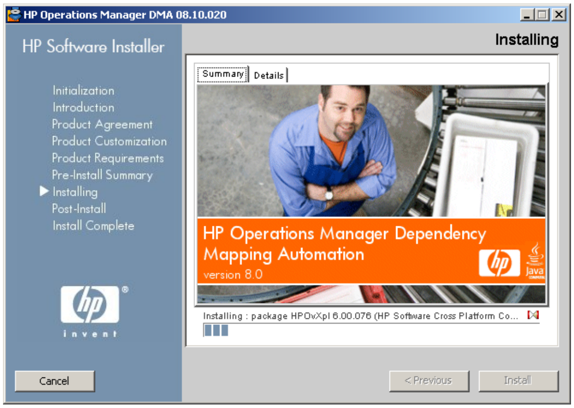
Pre-Install Summary

- HP Operations Manager DMA 08.10.020 (Install)
  - HP Operations Manager DMA (Install)
  - HP Operations Manager CI Web Services (Install)
    - HP Operations Manager Dependency Mapping Automation Messa
    - HP Operations Manager Web Service (Install)

```
HP Operations Manager DMA 08.10.020
Application folder : C:\Program Files\HP\HP BTO Software\
Data folder : C:\Documents and Settings\All Users\Application Data\HP\HP BTO
Please click on Install button to continue.
```

The HPOM DMA installation starts installing files onto the host system. Overall progress is displayed along with the name of the package being currently installed.

The last stage in the installation creates the HPOM DMA uninstaller.



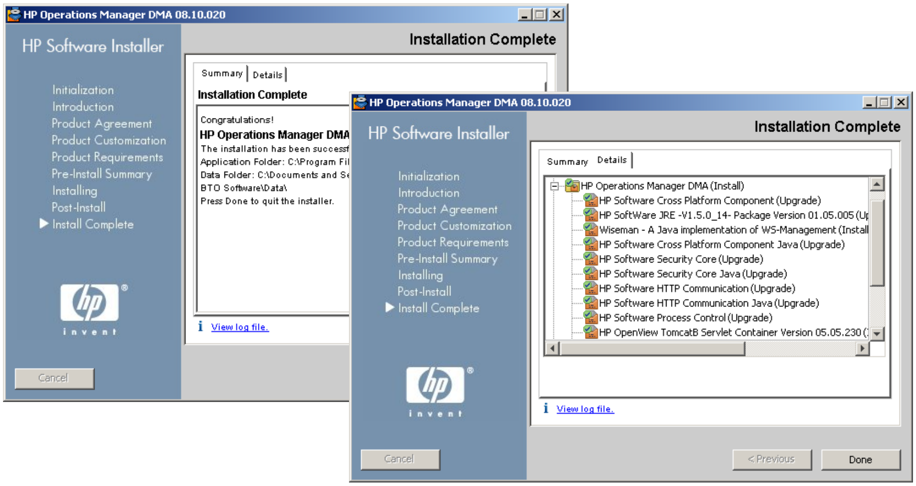
```
Installing : package HPOvXpl 6.00.076 (HP Software Cross Platform Co...
```

After the installation process is finished, the Installation Complete window opens showing a summary of the installation paths used.

You can also access the installation log file from the link in this window and open it in a web browser.

The installed packages can be seen from the Details tab.

6 Click **Done** to close the installation program.



Installation Complete

Congratulations!

HP Operations Manager DMA

The installation has been successf

Application Folder: C:\Program Fil

Data Folder: C:\Documents and Se

BTO Software\Data\

Press Done to quit the installer.

- HP Operations Manager DMA (Install)
  - HP Software Cross Platform Component (Upgrade)
  - HP SoftWare JRE -V1.5.0_14- Package Version 01.05.005 (Up
  - Wiseman - A Java implementation of WS-Management (Install
  - HP Software Cross Platform Component Java (Upgrade)
  - HP Software Security Core (Upgrade)
  - HP Software Security Core Java (Upgrade)
  - HP Software HTTP Communication (Upgrade)
  - HP Software HTTP Communication Java (Upgrade)
  - HP Software Process Control (Upgrade)
  - HP OpenView TomcatB Servlet Container Version 05.05.230 (

Configuring Smart Message Mapping in Cluster Environments

If you want to use Smart Message Mapping in cluster environments, you must make some configuration changes in the `ov-server.cntl` file.

To configure a cluster node for Smart Message Mapping, follow these steps:

1. Open the `ov-server.cntl` file for editing on the selected cluster node:

   ```
   /etc/cmcluster/ov-server/ov-server.cntl
   ```

2. Add the following function after the existing `start_services` function:

   ```
   function restart_dmamsg
   {
           /opt/OV/bin/ovc -stop dmamsg
           /opt/OV/bin/ovc -start dmamsg
           print "dmamsg restarted" >> $0.log }
   ```

3. Search for the following code section

   ```
   if [[ $1 = "start" ]]
   then
           print "\n\t########### Node \"$(hostname)\": Starting
   package at $(date) ###########"
           activate_volume_group
           check_and_mount
           add_ip_address
           get_ownership_dtc
           customer_defined_run_cmds
           start_services
   Check exit value
           if (( $exit_value == 1 ))
   ```

4. Add the **`restart_dmamsg`** entry as shown in the following extract:

   ```
   if [[ $1 = "start" ]]
   then
           print "\n\t########### Node \"$(hostname)\": Starting
   package at $(date) ###########"
           activate_volume_group
           check_and_mount
           add_ip_address
           get_ownership_dtc
           customer_defined_run_cmds
           start_services
           restart_dmamsg
   Check exit value
           if (( $exit_value == 1 ))
   ```

5. Save and close the file.
6. Repeat step 1 to step 5 for all nodes in the cluster.
7. Restart the cluster application.

To run Smart Message Mapping, you must:

- Enable Server-based Message Stream Interface (Server MSI).
- Start the Smart Message Mapping component.

For information on how to run Smart Message Mapping, see Configuring Smart Message Mapping on page 129.

Starting the HPOM DMA Console

To start the HPOM DMA console, do one of the following:

- *On Windows installations:* Double-click the desktop icon.
- In a web browser, enter the following location:

  http://<*Remote_HPOM_DMA_System*>:8081/hpdma

Further Essential Installation and Configuration Steps

To complete the HPOM DMA installation and configuration on the HPOM and UCMDB or BAC host systems, continue with the instructions described in Configuring HPOM DMA on page 83.

6 Installing HPOM DMA for HPOM for UNIX on PA-RISC Systems

HPOM DMA is not supported on HPOM host systems that run on a PA-RISC system. If you have such an HPOM installation, it is possible to install and configure HPOM DMA on an additional Windows system and remotely connect to your HPOM host system.

You must complete the following tasks:

- Install the web services and the Smart Message Mapper on the PA-RISC HPOM host system.
- Complete post-installation steps on the PA-RISC HPOM host system.
- Install the HPOM DMA product software without the web services on the remote HPOM DMA Windows host system.
- Complete post-installation steps on the remote HPOM DMA Windows host system.

This chapter guides you through all the required steps. These steps should take approximately 90 minutes to complete.

➤ Before you start the installation wizard, read the rest of this guide to plan your decisions and gather the information that you need.

Installing on Clusters

HPOM DMA is cluster aware. It has the capability to switch over automatically to an alternative cluster system (failover) under the same conditions as HPOM. HPOM DMA belongs to the same XPL High Availability (HA) resource group as HPOM.

➤ Applications running in a cluster environment are configured as HA Resource Groups. HA Resource Group is a generic term for cluster objects representing HA Applications. For further details on HPOM running in cluster environments, see the HPOM documentation.

For cluster-related information, for example, how to switch a system move from passive to active mode, see your clustering software documentation.

Applications Stopped and Restarted During Installation

HPOM DMA stops and restarts the following applications:

- Cluster monitoring on cluster systems
- Local HPOM agent
- HPOM for UNIX
- All `ovc` applications including the OV Control Daemon (`ovcd`)

The restarts are performed for install, uninstall and repair.

Repairing an HPOM DMA Installation

If your HPOM DMA installation is damaged, execute the installation procedure again and select the **Repair** option. The damaged files are replaced and HPOM DMA should be operational again. Your configuration files are not affected by the repair.

Loading the Installation Media

To prepare for the HPOM DMA software installation from the product media, follow the steps:

1. Insert the product media into an appropriate DVD-ROM drive.
2. Create a directory to mount the drive:

   ```
   mkdir /<mount_point>
   ```

   Example:

   ```
   mkdir /dvdrom
   ```

3. Mount the DVD-ROM drive:

   ```
   mount -r -F cdfs /dev/<dvdrom_drive_name> /<mount_point>
   ```

   Example:

   For a local DVD-ROM, you can execute:

   ```
   mount -r -F cdfs /dev/dsk/c0t2d0 /dvdrom
   ```

   You can also run SAM and mount the CD-ROM to a specific path in the Disks and File Systems window.

Installing on the PA-RISC HPOM Host System

To install the HPOM DMA web services and Smart Message Mapper components on the PA-RISC HPOM for UNIX host system, follow these steps:

1. Enter the following command to start the installation:

   ```
   <dvd-mountpoint>/hpdma_setup.sh
   ```

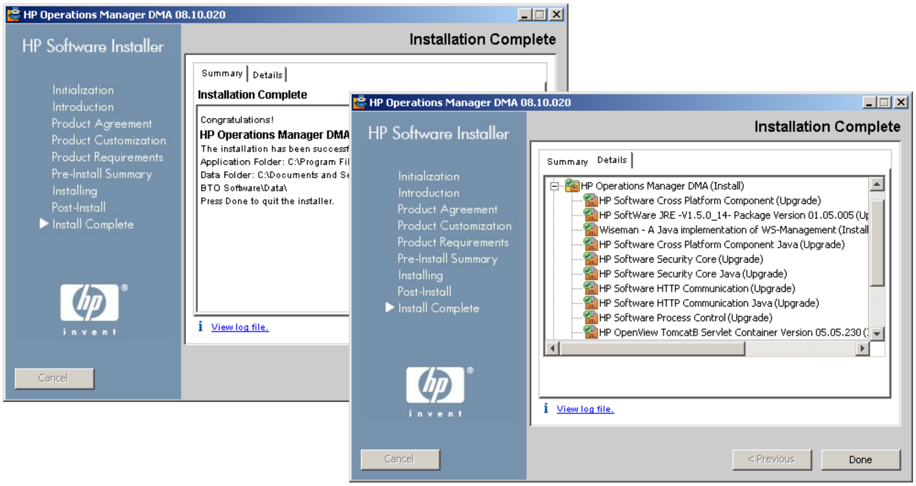
2. Follow the on-screen instructions and progress through the installation process using the **Next** and **Install** buttons.

   After the installation process is finished, the Installation Complete window opens showing a summary of the installation paths used.

   You can also access the installation log file from the link in this window and open it in a web browser.

The installed packages can be seen from the Details tab.

3 Click **Done** to close the installation program.



Installation Complete

Congratulations!

HP Operations Manager DMA

The installation has been successf

Application Folder: C:\Program Fil

Data Folder: C:\Documents and S

BTO Software\Data\

Press Done to quit the installer.

- HP Operations Manager DMA (Install)
  - HP Software Cross Platform Component (Upgrade)
  - HP SoftWare JRE -V1.5.0_14- Package Version 01.05.005 (U
  - Wiseman - A Java implementation of WS-Management (Install
  - HP Software Cross Platform Component Java (Upgrade)
  - HP Software Security Core (Upgrade)
  - HP Software Security Core Java (Upgrade)
  - HP Software HTTP Communication (Upgrade)
  - HP Software HTTP Communication Java (Upgrade)
  - HP Software Process Control (Upgrade)
  - HP OpenView TomcatB Servlet Container Version 05.05.230 (

➤ PA-RISC HPOM for UNIX host systems do not need an HPOM DMA licence. The HPOM DMA installation on the selected Windows host system requires a valid licence. For further details, see Chapter 10, Licensing.

Installing on the HPOM DMA Windows Host System

➤ The system selected to be the proxy system to host HPOM DMA must not be a system where HPOM for Windows is installed.

To install HP Operations Manager Dependency Mapping Automation on the remote HPOM DMA Windows host system, follow these steps:

➤ The HPOM DMA installation on the selected remote HPOM DMA Windows host system requires a valid licence. For further details, see Chapter 10, Licensing.

PA-RISC HPOM host systems do not need HPOM DMA licences.

1 Start the application installer as follows:

   a Close all open applications.

   b Insert the product media disk into the DVD drive of the HPOM DMA Windows host system.

      If Autorun is enabled, the installation starts automatically.

   c If Autorun is disabled, do one of the following:

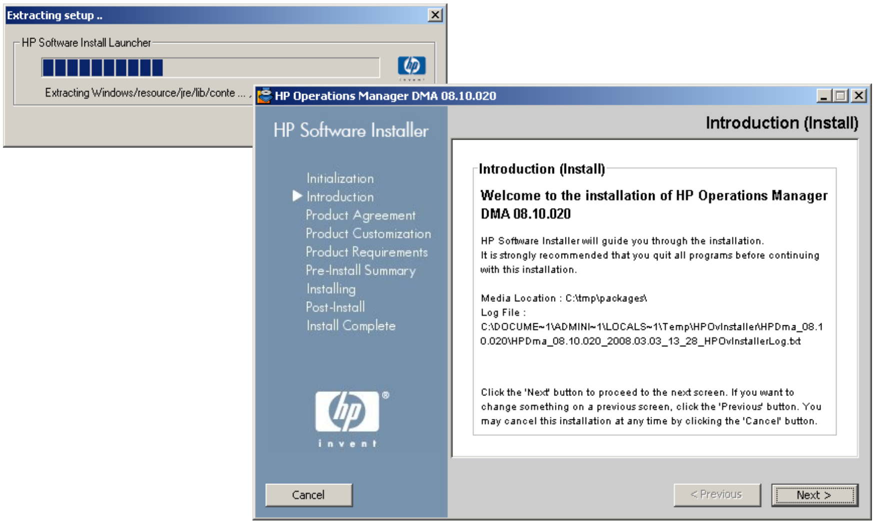
      — Execute the following in a command window:

```
<dvd_drive>:\hpdma_setup.bat
```

      — Execute the `hpdma_setup.bat` executable file from an Explorer window.

   Follow the on-screen instructions and progress through the installation process using the **Next** and **Install** buttons.

   ➤ The HPOM DMA installation location is dependent on the HPOM installation location. The HP Software Installer checks for this location and it is not possible to select an alternative for HPOM DMA.



Introduction (Install)

Introduction (Install)

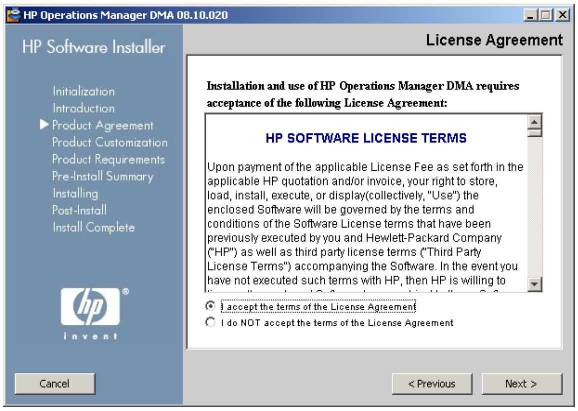
Welcome to the installation of HP Operations Manager DMA 08.10.020

HP Software Installer will guide you through the installation.
It is strongly recommended that you quit all programs before continuing with this installation.

Media Location : C:\tmp\packages\
Log File :
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\HPOvInstaller\HPDma_08.10.020\HPDma_08.10.020_2008.03.03_13_28_HPOvInstallerLog.txt

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button. You may cancel this installation at any time by clicking the 'Cancel' button.

2 Read and accept the Licence agreement and click **Next**.



License Agreement

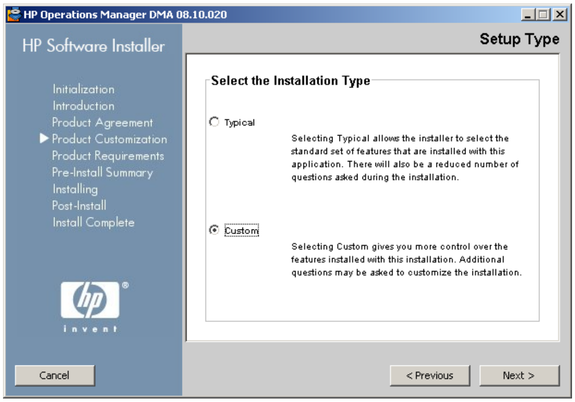
Installation and use of HP Operations Manager DMA requires acceptance of the following License Agreement:

HP SOFTWARE LICENSE TERMS

Upon payment of the applicable License Fee as set forth in the applicable HP quotation and/or invoice, your right to store, load, install, execute, or display(collectively, "Use") the enclosed Software will be governed by the terms and conditions of the Software License terms that have been previously executed by you and Hewlett-Packard Company ("HP") as well as third party license terms ("Third Party License Terms") accompanying the Software. In the event you have not executed such terms with HP, then HP is willing to

● I accept the terms of the License Agreement
○ I do NOT accept the terms of the License Agreement

3 Select the **Custom** installation type and click **Next**.



Setup Type

Select the Installation Type

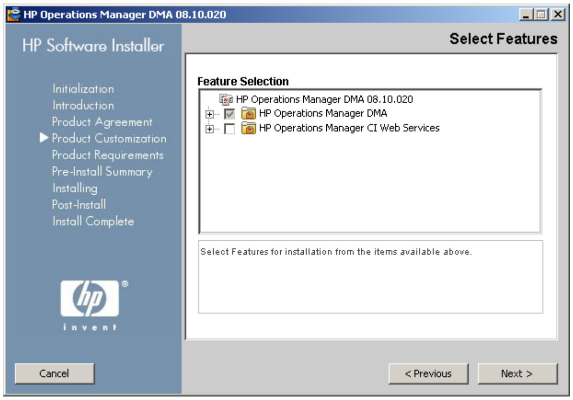
○ Typical

Selecting Typical allows the installer to select the standard set of features that are installed with this application. There will also be a reduced number of questions asked during the installation.

● Custom

Selecting Custom gives you more control over the features installed with this installation. Additional questions may be asked to customize the installation.

4 Clear the HP Operations Manager CI Web Services option and click **Next**.



Select Features

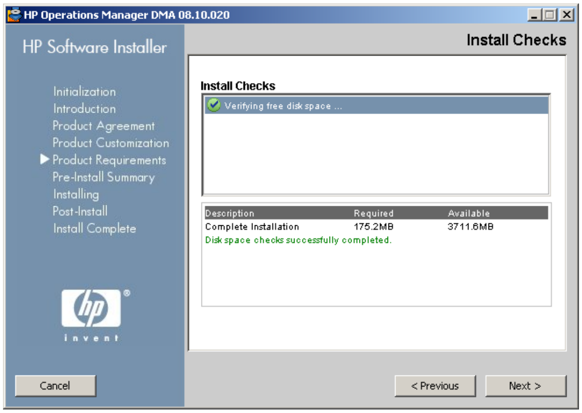
Feature Selection

HP Operations Manager DMA 08.10.020
☑ HP Operations Manager DMA
□ HP Operations Manager CI Web Services

Select Features for installation from the items available above.

The pre-install checks, including available disk space, are executed.

5 If they complete successfully, click **Next**.



Install Checks

Install Checks

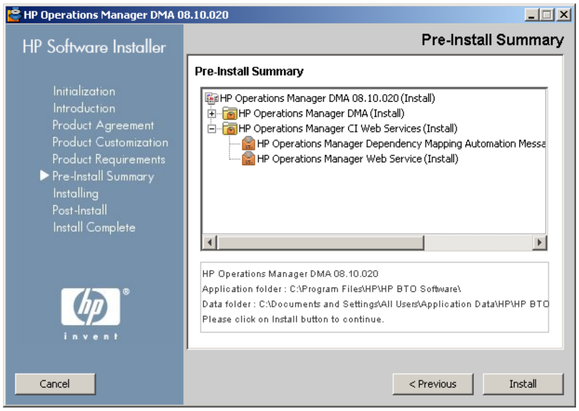
Verifying free disk space ...

Description	Required	Available
Complete Installation	175.2MB	3711.6MB

Disk space checks successfully completed.

The pre-install summary lists the components to be installed or updated.

6 Click **Next**.



Pre-Install Summary

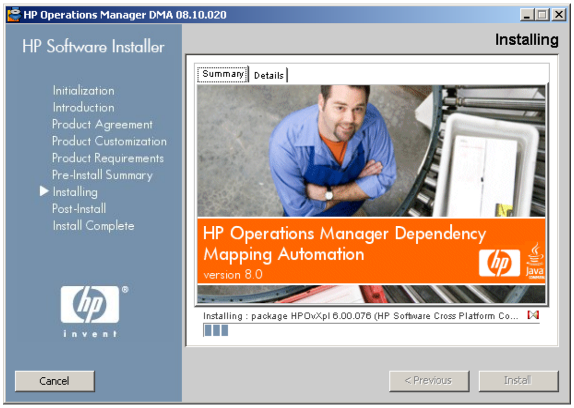
Pre-Install Summary

```
HP Operations Manager DMA 08.10.020 (Install)
  HP Operations Manager DMA (Install)
  HP Operations Manager CI Web Services (Install)
    HP Operations Manager Dependency Mapping Automation Messa
    HP Operations Manager Web Service (Install)
```

HP Operations Manager DMA 08.10.020
Application folder : C:\Program Files\HP\HP BTO Software\
Data folder : C:\Documents and Settings\All Users\Application Data\HP\HP BTO
Please click on Install button to continue.

The HPOM DMA installation starts installing files onto the host system. Overall progress is displayed along with the name of the package being currently installed.

The last stage in the installation creates the HPOM DMA uninstaller.



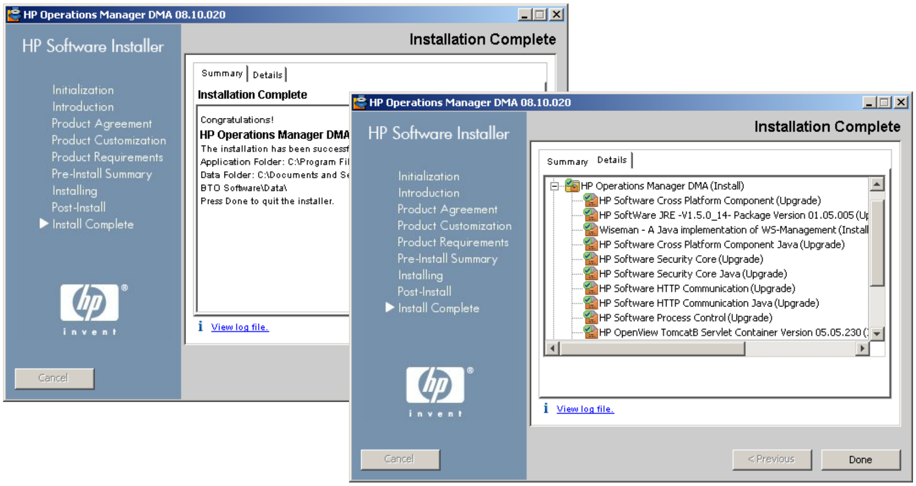
Installing : package HPOvXpl 6.00.076 (HP Software Cross Platform Co...

After the installation process is finished, the Installation Complete window opens showing a summary of the installation paths used.

You can also access the installation log file from the link in this window and open it in a web browser.

The installed packages can be seen from the Details tab.

7 Click **Done** to close the installation program.



Installation Complete

Congratulations!

HP Operations Manager DMA

The installation has been successf

Application Folder: C:\Program Fil

Data Folder: C:\Documents and Se

BTO Software\Data\

Press Done to quit the installer.

- HP Operations Manager DMA (Install)
  - HP Software Cross Platform Component (Upgrade)
  - HP SoftWare JRE -V1.5.0_14- Package Version 01.05.005 (Up
  - Wiseman - A Java implementation of WS-Management (Install
  - HP Software Cross Platform Component Java (Upgrade)
  - HP Software Security Core (Upgrade)
  - HP Software Security Core Java (Upgrade)
  - HP Software HTTP Communication (Upgrade)
  - HP Software HTTP Communication Java (Upgrade)
  - HP Software Process Control (Upgrade)
  - HP OpenView TomcatB Servlet Container Version 05.05.230 (

Post-Installation Steps on the PA-RISC Host System

To complete the post-installation steps on the PA-RISC HPOM for UNIX host system, execute the following steps:

1. Untar the `DmaUploadsOmU.tar` file which you copied from the HPOM DMA Windows host system. See step 5 on page 80.

   ➤ `/opt/OV/misc/dma/ReadMe.txt` contains sample commands for the following tasks.

   If you make the `/opt/OV/misc/dma/ReadMe.txt` file executable and run it, the post-installation steps are done for you automatically:

   ```
   chmod 750 /opt/OV/misc/dma/ReadMe.txt
   sh /opt/OV/misc/dma/ReadMe.txt
   ```

2. Load the default root-service, calculation and propagation rules for HPOM DMA into HPOM for UNIX with the command:

   ```
   /bin/opcservice -add /opt/OV/misc/dma/
   default_calcprop.xml
   ```

3. Load the service type definitions into HPOM for UNIX with the commands:

   ```
   /opt/OV/bin/ServiceTypeDefinitionCLI -o -a /opt/OV/misc/
   dma/default_std.xml
   ```

   ```
   /opt/OV/bin/ServiceTypeDefinitionCLI -o -a /opt/OV/misc/
   dma/eum_std.xml
   ```

4. Load the default node group and templates into HPOM for UNIX:

   - **Node Groups**

     a. Go to the `/tmp` directory:

     ```
     cd /tmp
     ```

     b. Untar the `defaultNodeGroup.tar` package:

     ```
     /usr/bin/tar xf /opt/OV/misc/dma/
     defaultNodeGroup.tar
     ```

     c. Upload the default node group:

     ```
     /opt/OV/bin/OpC/opccfgupld -add -ascii /tmp/Sonata
     ```

d. Clean up the temporary files:

```
rm -r /tmp/Sonata
```

- **Templates**

  a. Go to the `/tmp` directory:

  ```
  cd /tmp
  ```

  b. Untar the `OmDmaTemplates.tar` package:

  ```
  /usr/bin/tar xf /opt/OV/misc/dma/OmDmaTemplates.tar
  ```

  c. Upload the default templates:

  ```
  /opt/OV/bin/OpC/opccfgupld -add -ascii /tmp/
  OmDmaTemplates
  ```

  d. Clean up the temporary files:

  ```
  rm -r /tmp/OmDmaTemplates
  ```

5. HPOM DMA delivers templates for self monitoring. To find out how to assign and deploy the OM DMA template group, see Assigning the OM DMA Template Group on page 99 and Deploying the OM DMA Template Group on page 100. However, the HPOM DMA synchronization log does not run on the HPOM management server, but on the HPOM DMA Windows host system, and specific deployment is needed for this template

   To deploy the `HPOM DMA Synchronization Log` template.

   a. Change specified log file in the `HPOM DMA Synchronization Log` template:

   – From:

   ```
   /var/opt/OV/shared/server/log/dma/sync.*.en
   ```

   – To:

   ```
   C:\Documents and Settings\All Users\Application
   Data\HP\HP BTO Software\shared\server\log\dma\
   sync.*.en
   ```

   b. Install an HPOM agent on the HPOM DMA Windows host system.

   c. Assign and deploy the `HPOM DMA Synchronization Log` template to this new managed node.

Post-Installation Steps on the Windows Host System

After installing HPOM DMA on a Windows host system, follow these steps.

➤ For details of the directories used by HPOM DMA, see Installation Locations on page 221.

1 Remove the contents of the directory:

   `<SharedDir>\conf\dma\sync-packages`

2 Copy the contents of the directory:

   `<InstallDir>\newconfig\DataDir\conf\dma\sync-packages\unix`

   To the directory:

   `<SharedDir>\conf\dma\sync-packages`

   This is the directory from which you deleted the original files in step 1.

3 Start the HPOM DMA console by double-clicking the desktop icon or by entering the following address into a web browser:

   http://<*Remote_HPOM_DMA_System*>:8081/hpdma

4 In the Connection page of the HPOM DMA console, specify the connection for the HPOM management server:

   `http://<PA-RISC_Mgmt_Server>:8081/ConfigurationItem/`

5 Copy the `<InstallDir>\misc\dma\DmaUploadsOmU.tar` file to a temporary location, for example, `/tmp`, on the PA-RISC HPOM system.

   The `DmaUploadsOmU.tar` file contains the default root-service, calculation and propagation rules, service type definitions, and the node group and templates for HPOM DMA.

6 Copy the `DefaultSyncTask.settings` file to the equivalent location on the PA-RISC HPOM system:

   — From:

   `<SharedDir>\conf\dma\DefaultSyncTask.settings`

   — To:

   `/var/opt/OV/shared/server/conf/dma/`

   d Overwrite the default version on the PA-RISC HPOM system.

Starting the HPOM DMA Console

To start the HPOM DMA console, do one of the following:

- Double-click the desktop icon.
- In a web browser, enter the following location:

  http://<*Remote_HPOM_DMA_System*>:8081/hpdma

Further Essential Installation and Configuration Steps

To complete the HPOM DMA installation and configuration on the HPOM and UCMDB or BAC host systems, continue with the instructions described in Configuring HPOM DMA on page 83.

7 Configuring HPOM DMA

To configure your installation, you need to make the following changes on the UCMDB or BAC system, the HPOM system and in the HPOM DMA console:

- **Change the HPOM DMA Console Default Password**

  It is recommended that you immediately add at least one user with password and delete the default user to aid security.

  For detailed instructions, see Managing Users and Passwords on page 85.

- **Update Your UCMDB or BAC Installation**

  — Upload and deploy the HPOM DMA packages to the UCMDB or BAC system.

  — Review the TQL queries in UCMDB or BAC, adapt them to your environment, and apply the enrichment rules.

  For detailed instructions, see Configuring UCMDB or BAC on page 88.

- **Complete Assignments in HPOM**

  — Assign the CMDB Service and Groups to an HPOM user.

  — Assign and deploy the OM DMA policy or template group to the HPOM management server (optional).

  For detailed instructions, see Configuring HPOM for UNIX on page 98.

- **Specify Configurations in HPOM DMA**

  Specify the web service endpoint connections between the UCMDB and the HPOM systems. Also specify the content for HPOM DMA synchronization.

  For detailed instructions, see Configuring HPOM DMA on page 110.

Customizing synchronization using scripting (see the *HPOM DMA Extensibility Guide*) requires the HPOM DMA installation to be on the same system as the HPOM management server because synchronization package `Script: Trigger Policy Distribution` is expected to run locally on the HPOM management server.

The remote HPOM DMA installation required to support HPOM on PA-RISC systems does not allow the script to be run as expected. If you want to use this feature for PA-RISC installations, you must run the script remotely on the HPOM management server system, for example, by using ssh.

Managing Users and Passwords

The HPOM DMA console installation includes a default user:

- User: `admin`
- Password: `admin`

It is recommended that you immediately add at least one user with password and delete the default user to aid security.

Users are managed using the `dmauser` command-line tool available in the following location:

- *UNIX*

  `<InstallDir>/bin/dmauser.sh`

- *Windows*

  `<InstallDir>\bin\dmauser.bat`

Adding a User

The `dmauser` command adds the specified user and its password to the local users store.

To add a new user, execute the following command:

- *UNIX*

  ```
  <InstallDir>/bin/dmauser.sh -a <user name> <password>
  ```

- *Windows*

  ```
  <InstallDir>/bin/dmauser -a <user name> <password>
  ```

Changing a Password

The `dmauser` command changes the password of an existing user in the local users store.

To change the password of an existing user, execute the following command:

- *UNIX*

```
<InstallDir>/bin/dmauser.sh -a <user name> <password>
```

- *Windows*

```
<InstallDir>/bin/dmauser -a <user name> <password>
```

Deleting a User

To delete an existing user from the local users store, execute the following command with the user name to be deleted:

- *UNIX*

```
<InstallDir>/bin/dmauser.sh -d <user name>
```

- *Windows*

```
<InstallDir>/bin/dmauser -d <user name>
```

Listing Users

To list all existing users in the local users store, execute the following command:

- *UNIX*

```
<InstallDir>/bin/dmauser.sh -l
```

- *Windows*

```
<InstallDir>/bin/dmauser -l
```

dmauser Usage

```
dmauser(.sh) -a <user name> <password> | -d <user name> |
 -h | -l | -version
```

`-a, -add <user name> <password>`	Adds a user to the local users store. If the user already exists, its password is replaced.
`-d, -delete <user name>`	Deletes the specified user from the local users store.

`-l, -list`	Displays all users stored in the local users store.
`-h, -help`	Displays usage information.
`-version`	Displays the version number of the dmauser tool.

Configuring UCMDB or BAC

HPOM DMA delivers basic synchronization for operating systems and databases.

To use synchronization tools, follow these steps:

- **HPOM DMA Packages**

  Upload and deploy the HPOM DMA packages to the UCMDB or BAC system.

  For detailed instructions, see Deploying HPOM DMA Packages to UCMDB or BAC on page 89 or see the HPOM DMA online help.

- **TQL Queries**

  Review the TQL queries in UCMDB or BAC and adapt them to your environment.

  For detailed instructions, see Reviewing the HPOM DMA Packages on page 90 and Adapting HPOM DMA TQL Queries on page 93.

  If you want to restrict service synchronization to nodes managed by a selected HPOM management server, you must configure the TQL queries to match your HPOM management server. For detailed instructions, see Restricting Service Synchronization to Managed Nodes on page 141.

- **Enrichment Rules**

  Apply the enrichment rules.

  For detailed instructions, see Apply Enrichment Rules on page 96.

Deploying HPOM DMA Packages to UCMDB or BAC

To upload and deploy HPOM DMA packages to your UCMDB or BAC installation, follow these steps:

1 Open the Package Manager:

- *UCMDB*

  Select **Admin** → **Settings** → **Package Manager.**

- *BAC*

  Select **Admin** → **Universal CMDB** → **Settings** → **Package Manager.**

2 Add packages to the server packages directory:

Version 7.00

Click **Upload package to server packages directory**.

Version 7.50

Click **Deploy** → **Add**.

The selected package is uploaded and for version 7.50, deployed.

3 Browse to the following directory on the HPOM DMA host system:

`<InstallDir>/misc/dma/`

4 Select the `hpdmacore.zip` file and click **Save/OK**.

This package must be uploaded and, for version 7.00, deployed before any of the other HPOM DMA packages.

5 *Version 7.00 only:* Select the `hpdmacore.zip` file from the Package list and click **Deploy**.

6 Upload any of the following packages that you want to use:

- `hpdmaos.zip`

  Used for operating systems.

- `hpdmadb.zip`

  Used for databases.

- `hpdmasamples.zip`

  Used for the My Company Sample synchronization package.

- `hpdmaEUM.zip`

  HP BAC only: Used for End User Monitors

For the required package:

BAC and UCMDB version 7.00: repeat step 2 *to* step 5.

BAC and UCMDB version 7.50: repeat step 2 to step 4.

Reviewing the HPOM DMA Packages

HPOM DMA uses TQL queries to extract node and service information from UCMDB. This information is then used to populate HPOM nodes and services.

For operating systems, the following TQL queries and corresponding views included in the `hpdmaos.zip` are delivered:

- `UNIX Operating System (Operations)`
- `Windows Operating System (Operations)`

For databases, the `hpdmadb.zip` package includes the following TQL queries and corresponding views:

- `Oracle (Operations)`
- `MS SQL Server (Operations)`
- `Informix (Operations)`
- `Sybase (Operations)`

An example of how to customize Service Navigator views in HPOM is available in the `hpdmasamples.zip` package. The TQL queries and corresponding views included are:

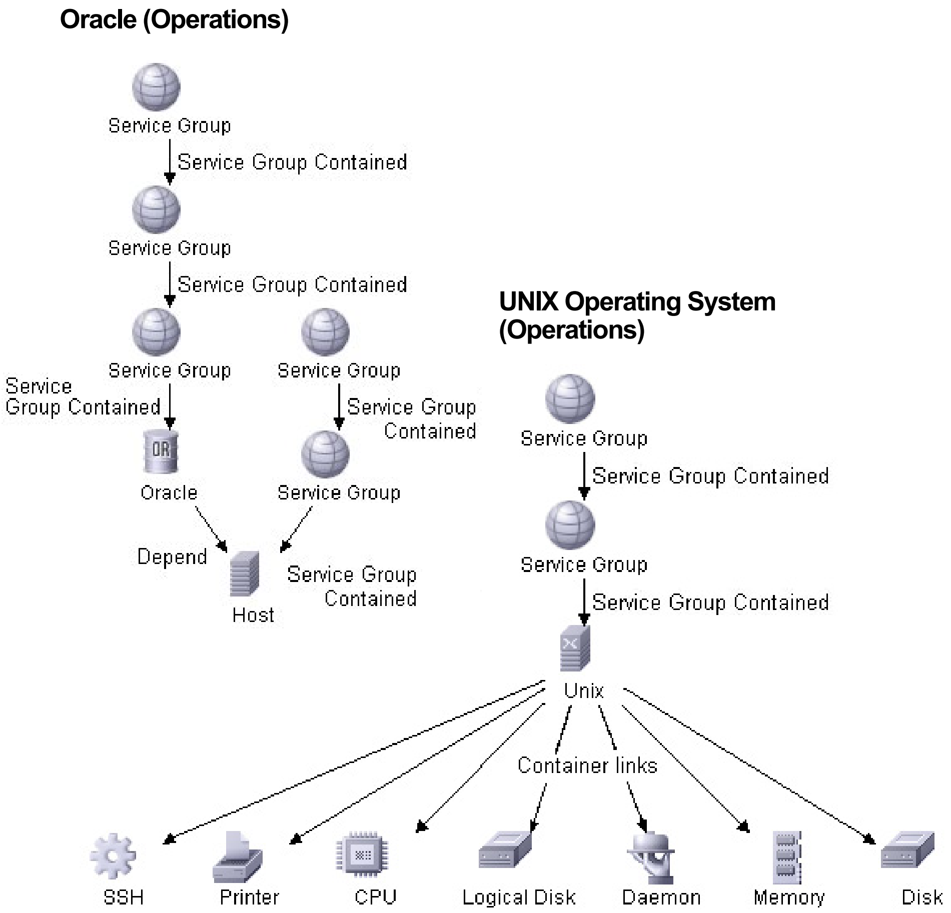
- `My Company US (Operations)`
- `My Company EMEA (Operations)`
- `My Company ASIAPAC (Operations)`

For displaying of End User Management views from BAC in HPOM, the TQL queries and corresponding views included in the `hpdmaEUM.zip` package are:

- `End User Monitors (Operations)`

Some examples of TQL queries are shown in Figure 14.

Figure 14 Examples of TQL Queries



The predefined TQL queries are created to support HPOM service views. The relationships and the relationship types are important for correct status propagation within HPOM.

The correct status propagation within HPOM is achieved by the following:

- HPOM DMA introduces a new CI Type `Service Group` that is used as the top-level service above the discovered CIs. CIs are arranged under these service groups and linked using the `Service Group Contained` relationship.

The predefined package delivers the following service groups:

- Applications
  - Databases
    - Databases on UNIX
    - Databases on Windows
- End User Monitors
- Organizations
  - My Company
    - My Company ASIAPAC
    - My Company EMEA
    - My Company US
- Systems Infrastructure
  - UNIX
  - Windows

- HPOM DMA then enriches the UCDMB or BAC system to assign the discovered CIs to the appropriate server groups. For that the following enrichment rules are used:
  - DatabaseDependency
  - EUM
  - My Company ASIAPAC Databases
  - My Company ASIAPAC Unix Nodes
  - My Company ASIAPAC Windows Nodes
  - My Company EMEA Databases
  - My Company EMEA Unix Nodes
  - My Company EMEA Windows Nodes
  - My Company US Databases
  - My Company US Unix Nodes
  - My Company US Windows Nodes
  - NodeServerType

- `Unix Databases`
- `Windows Databases`
- `Unix Nodes`
- `Windows Nodes`

- UCMDB by default, includes a `host contains databases` relationship. For proper status propagation, HPOM DMA introduces a `database depends on host` relationship. This is done by the enrichment rule `Database Dependency`.
- UCMDB includes the following relationships:
  - `depends on` relationship between Business Process Group and Business Process Step
  - `monitored by` relationship between Business Process Step and BPM Transaction from location

  With HPOM DMA, the `EUM` enrichment rule adds an EUM contained relation for proper status propagation.

  Additionally, the `End User Monitors` service group is added as the top level for End User Monitors CIs.
- HPOM DMA introduces an enrichment rule `Node Server Type`. With that rule, the host server type is set to the installed database type, for example, `oracle`. This is used for mapping hosts to node groups in HPOM.
- All other enrichment rules are used to assign the required CIs to appropriate service groups.

Adapting HPOM DMA TQL Queries

As HPOM DMA populates your HPOM node banks and service tree, it is necessary that you adapt the TQL queries to suit to your specific environment.

To adapt HPOM DMA TQL queries, follow these steps:

1. Open the View Manager:
   - *UCMDB*

     Admin → Modeling → View Manager

- *BAC*

  Admin → **Universal CMDB** → **Modeling** → **View Manager**

2 Expand the **hpdma** view from the Views list.

  The TQL queries in the `Database` and `Operating System` groups include filters in the node types that you must adapt to your environment.

3 For each TQL query in the `Database` and `Operating System` groups, select the node type (Host, UNIX, or Windows).

4 From the shortcut menu, open **Node Condition**.

5 Change the filter to your environment.

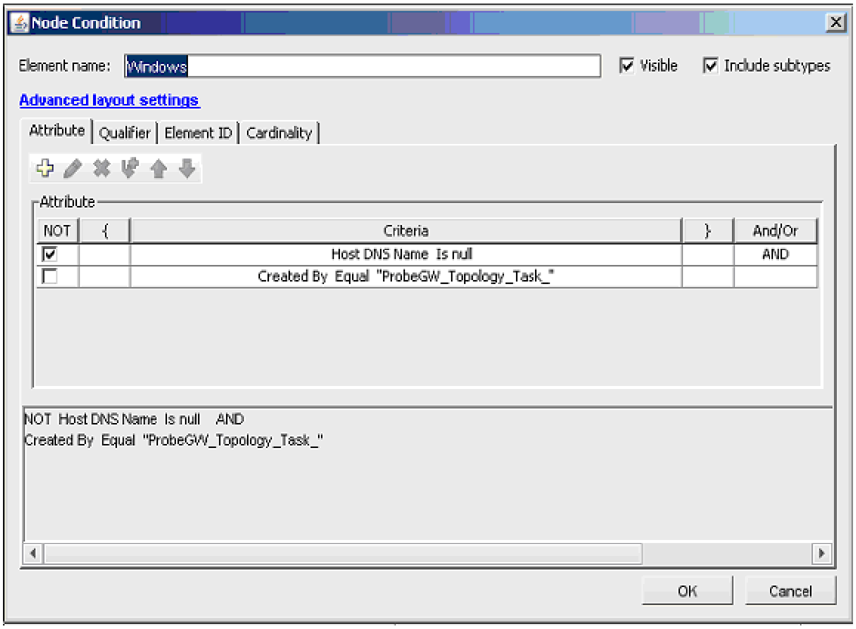
  By default, only nodes that include running UCMDB probes are selected. This is specified with the following node condition:

  ```
  Created By Equal "ProbeGW_Topology_Task_"
  ```

  You can delete this condition and add new ones to match your environment. For example, `restrict on domain names` and specify domains to limit your search.

  Setting filters for TQL queries in the Node Condition window is shown in Figure 15.

Figure 15 Setting Node Condition Filters for TQL Queries



Element name: Windows
☑ Visible ☑ Include subtypes

NOT	{	Criteria	}	And/Or
☑		Host DNS Name Is null		AND
□		Created By Equal "ProbeGW_Topology_Task_"		

```
NOT Host DNS Name Is null   AND
Created By Equal "ProbeGW_Topology_Task_"
```

Do not remove the `HOST DNS Name is null` filter, as this is required for HPOM DMA.

For adapting My Company synchronization package TQL queries, see the *HPOM DMA Extensibility Guide*.

Apply Enrichment Rules

Apply each enrichment rule in the `hpdma` group.

> ➤ UCMDB enrichment rules only add the selected CI and relations to UCMDB. If you change the enrichment rule, for example, change the list of nodes that should be added to a service group, then the already existing CIs in the group are not automatically removed.
>
> Before you change an enrichment rule, you should remove the already existing CIs.
>
> If you want to remove all currently existing assignment, select the enrichment rule in the CMDB Enrichment Manager and click **Remove Enrichment Results**.
>
> This might also remove CIs and relations that have been added by other enrichment rules.

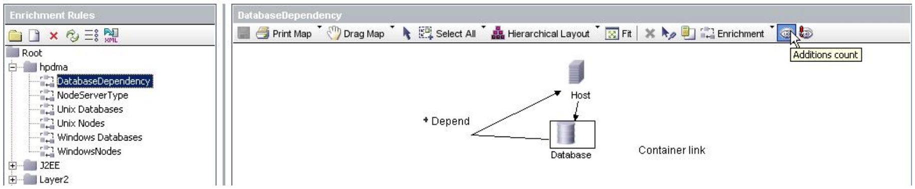
To apply enrichment rules, follow these steps:

1. Open the Enrichment Manager:
   - *UCMDB*

     Admin → **Modeling** → **Enrichment Manager**
   - *BAC*

     Admin → **Universal CMDB** → **Modeling** → **Enrichment Manager**
2. Expand the **hpdma** group from the Enrichment Rules list.
3. Apply each enrichment rule by pressing the icon picturing an eye as shown in Figure 16.

Figure 16 Applying Enrichment Rules



You must execute each enrichment rule whenever you discover new instances.

To make executing enrichment rules easier, you can add a schedule to regularly apply enrichment rules.

- *UCMDB*

  Select **Admin** → **Settings** → **Scheduler.**

- *BAC*

  Select **Admin** → **Universal CMDB** → **Settings** → **Scheduler**.

Configuring HPOM for UNIX

This section contains the instructions how to do the following essential assignments on the HPOM for UNIX management server:

- Assigning the CMDB Service Group to an HPOM User on page 98.
- Assigning the CMDB Node Groups to an HPOM User **on page 98.**

This section also contains the instructions how to do the following optional assignments on the HPOM for UNIX management server:

- Assigning the OM DMA Template Group on page 99.
- Creating Service Type Definitions Automatically on page 100.
- Assigning User Profiles for Services on HPOM for UNIX on page 101.
- Automating Policy Distribution on page 103.
- Configuring HPOM Agent Types on page 103.

Assigning the CMDB Service Group to an HPOM User

To assign the CMDB service group to an HPOM user, execute the following command:

```
opcservice -assign <HPOM_User_Name> CMDB
```

Example:

```
opcservice -assign opc_adm CMDB
```

User profile mapping enables you to map a service to an HPOM user profile. After synchronization, the service is assigned to all operators that are included in any specified HPOM user profile. If you use the User Profile Mapping feature, assigning the CMDB service group to a user may not be appropriate. See the *HPOM DMA Extensibility Guide* for further details.

Assigning the CMDB Node Groups to an HPOM User

To assign the CMDB node groups to an HPOM user, follow these steps:

1 Open the HPOM GUI (opc).

2 Go to the User Bank by selecting:

Window → User Bank

3 Right-click the required user and select **Modify** from the shortcut menu.

The Modify User window opens.

4 Click **Responsibilities.**

5 Select the CMDB node groups:

- `CMDB`
- `CMDB_removed`

6 Click **Close**.

7 In the Modify User window, click **OK**.

Assigning the OM DMA Template Group

Assign the `OM DMA` template group to the agent on the HPOM management server. For details about the available templates, see Objects Installed on HPOM on page 227.

To assign the `OM DMA` template group, from HPOM UI, follow these steps:

1 In the Node Bank window, select the HPOM management server node.

2 Open the Define Configuration window:

Actions → Agents → Assign Templates

3 Select HPOM management server system and click **Add**.

The Add Configuration window opens.

4 Click **Open Template Window.**

The Message Source Templates window opens.

5 Select the **Group OM DMA** template.

6 In the Add Configuration window, click **Get Template Selections.**

7 Click **OK.**

8 In the Define Configuration window, click **OK.**

Deploying the OM DMA Template Group

Deploy the `OM DMA` template group to the agent on the HPOM management server. For details about the available templates, see Objects Installed on HPOM on page 227.

> When monitoring HPOM DMA in cluster installations, policies or templates should be enabled on the active node and disabled on all inactive nodes.
>
> For information about policy or template deployment in cluster installations, see the appropriate HPOM documentation.
>
> For HPOM for UNIX installed on a cluster, template assignments must be done on Virtual Nodes. For details, see the chapter entitled “Working with Virtual Nodes” in the *HTTPS Agent Concepts and Configuration Guide*.

To deploy the `OM DMA` template to the agent on the HPOM management server node, from HPOM UI, follow these steps:

1. In the Node Bank window, select the HPOM management server node.
2. Open the Install & Update Software and Configuration window:

   Actions → **Agents** → **Install & Update Software and Config**
3. Make sure that the HPOM management server node appears in the Target Nodes list.
4. Check **Templates** in the Components pane.
5. Click **OK** to deploy the OM DMA template to the HPOM management server node.

Creating Service Type Definitions Automatically

Service type definitions (STDs) are used to identify how CIs from UCMDB are to be handled when building services in HPOM on synchronization. If an STD for an imported CI is not available in HPOM, it cannot be displayed in the

Service Navigator and an error message is displayed explaining that STDs are missing. HPOM DMA can automatically create STDs to suit non-matching CIs as they are imported into HPOM.

Automatic service type definition creation is disabled by default.

To enable automatic service type definition creation, follow these steps:

1 Enable automatic service type definition creation in the HPOM web service:

```
ovconfchg -ovrg server -ns
opc.WebService.ConfigurationItem -set StdCreationEnabled
true
```

2 Restart the Tomcat server:

```
ovc -restart ovtomcatB
```

Assigning User Profiles for Services on HPOM for UNIX

User Profile Assignment enables you to map a service to an HPOM user profile. After synchronization, the service is assigned to all operators that are included in the specified HPOM user profile.

Profile Prerequisites

Make sure that at least one user profile already exists in HPOM.

If the profile is missing or cannot be assigned to the service, the Service CI is created and a warning is logged in HPOM DMA. Additionally, an HPOM event message should be sent to the HPOM server. No error is returned by the web service when the HPOM DMA monitoring templates are deployed.

It is recommended that you do not assign user profiles to every service. Instead, assign them to a selected set of services at the top of a tree to be managed by the specified profile. Assigning a profile to every service usually results in poor performance.

Mapping User Profiles

It is necessary to create user profile mapping (`usermapping.xml`) files for the services that you want to assign to a user. One user profile mapping file is required for each synchronization package that references services that you want to assign. To find out how to specify User Profile mapping, see the online help and the *HPOM DMA Extensibility Guide*.

Enabling User Profile Assignment

User profile assignment for services is disabled by default. It can be enabled as follows:

1 Configure the HPOM for UNIX service engine to include user profiles by entering the following commands:

```
ovconfchg -ovrg server -ns opc -set
OPCSVC_CONSIDER_PROFILES TRUE
```

2 Restart the service engine:

```
opcsv -stop
opcsv -start
```

3 Create user profiles and assign operators to the profiles (see HPOM for UNIX documentation).

4 Create the user profiles in the service engine repository:

```
opcservice -operator <UserProfile>
```

5 Assign and deassign the user profiles to and from an existing service:

```
opcservice -assign <UserProfile> <ServiceName>
opcservice -deassign <UserProfile> <ServiceName>
```

For example:

```
opcservice -assign UserProfile1 CMDB
opcservice -deassign UserProfile1 CMDB
```

6 Enable user profile assignment in the HPOM web service:

```
ovconfchg -ovrg server -ns
opc.WebService.ConfigurationItem -set
UserProfileAssignmentEnabled true
```

7 Restart the Tomcat server:

```
ovc -restart ovtomcatB
```

8 Restart Smart Message Mapping, if required:

```
ovc -start dmamsg
```

Automating Policy Distribution

The HPOM DMA `Script: Trigger Policy Distribution` synchronization package is deployed as part of the standard installation. It contains a post-upload script that triggers policy distribution.

If you want to configure automatic policy distribution, activate the `Script: Trigger Policy Distribution` synchronization package from the Content page.

Configuring HPOM Agent Types

Attribute mapping defines the properties of a UCMDB CI, which in turn determines the node type on HPOM. It maps them to HPOM-specific values for the following properties:

- `ovo_osType`
- `ovo_osVersion`
- `ovo_SystemType`
- `ovo_CommType`

After a CI is identified as a node of a known type, it is ready for agent deployment and management using HPOM.

When nodes whose agents are not installed or available in HPOM are synchronized, warnings are written to the log files found in the following directory:

```
<SharedDir>/log/
```

The warnings take the following form:

```
WARNING; Machine Type for systemType: x86/x64 Compatible, osType:
Windows_32, osVersion: Server 2003 (5.2), commType: HTTPS could
not be evaluated and is set to OPC_MACHINE_OTHER (0)
```

In HPOM, not all agent packages must be installed. It is often the case that users have installed only the agent software to match the systems that they currently want to manage. When you want to manage additional agent types, you must install the appropriate HPOM agent packages.

After installing additional agent packages, it is necessary for you to execute the `ConfigureMachineTypes` script. This script uses the list of installed agent types from the HPOM database to select the required machine types from the `MachineTypes_template.xml` template file. The script stores this information for use at run time.

When you execute the `ConfigureMachineTypes` script, you might also see an error message of the following form, which describes the missing machine type and creates an example that can be used to update the `MachineTypes_template.xml` template:

```
No entry for Machine Type: 8(Machine Type: SNI RM400/600 Network
Type:
IP Network OS Name: SINIX) found in the template (/var/opt/OV/
shared/server/conf/dma/MachineTypes.xml).
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<MachineType xmlns="http://schemas.hp.com/operations/1/
      MachineTypes" MachTypeId="8">
   <Description>Machine Type: SNI RM400/600 Network Type:
      IP Network OS Name: SINIX</Description>
   <Representations>
      <Default CommType="TO_BE_FILLED" SystemType=
         "TO_BE_FILLED" OsVersion="TO_BE_FILLED"
         OsType="TO_BE_FILLED"/>
   </Representations>
</MachineType>

Repository not updated, update the template and start again!
```

Update HPOM DMA After Adding a New Agent Type

To update HPOM DMA after adding a new agent type to HPOM, follow these steps:

1. Open the template files for editing:

   <DataDir>`/shared/server/conf/dma/MachineTypes_template.xml`

2. Add an entry in the template file to describe the machine type.

The following example shows how the entry for the missing `SNI RM400/600` machine type should be specified:

```
<tns:MachineType MachTypeId="8">
   <tns:Description>Machine Type: SNI RM400/600 Network Type:
      IP Network OS Name: SINIX</tns:Description>
   <tns:Representations>
      <tns:Default CommType="DCE"
         SystemType="RM400/600" OsVersion="" OsType="SINIX"/>
   </tns:Representations>
</tns:MachineType>
```

3. Save and close the `MachineTypes_template.xml` file.

4. Update the attribute mapping to set correct values for this machine type.

   In HPOM DMA:

   - `osType` is mapped to `ovo_osType`
   - `osVersion` is mapped to `ovo_osVersion`
   - `SystemType` is mapped to `ovo_SystemType`
   - `CommType` is mapped to `ovo_CommType`

   In the example, the attribute mapping must be updated with these values:

   - `ovo_osType="SINIX"`
   - `ovo_osVersion=""`
   - `ovo_SystemType="SINIX"`
   - `ovo_CommType="DCE"`

   For further information about attribute mapping, see the *HPOM DMA Extensibility Guide*.

5. Execute the `ConfigureMachineTypes` script:

   ***<InstallDir>*/bin/ConfigureMachineTypes**

   The following message should be displayed if the updates have been correctly completed:

   ```
   Repository successfully updated
   ```

Configuring HPOM for Windows

This section explains how to do the following:

- Creating Service Type Definitions Automatically on page 106.
- Assigning User Roles for Services on HPOM for Windows on page 107.
- Assigning and Deploying the OM DMA Policy Group on page 109.

Creating Service Type Definitions Automatically

Service type definitions (STDs) are used to identify how CIs from UCMDB are to be handled when building services in HPOM on synchronization. If an STD for an imported CI is not available in HPOM, it cannot be displayed in the Service Navigator, and an error message is displayed explaining that STDs are missing. HPOM DMA can automatically create STDs to suit non-matching CIs as they are imported into HPOM.

Automatic service type definition creation is disabled by default.

To enable automatic service type definition creation, follow these steps:

1. Enable automatic service type definition creation in the HPOM web service:

   ```
   ovconfchg -ovrg server -ns
   opc.WebService.ConfigurationItem -set StdCreationEnabled
   true
   ```

2. Restart the Tomcat server:

   ```
   ovc -restart ovtomcatB
   ```

When you create your own STDs and you use the UI launch feature, you must assign the `BAC Service UI Launch` or `UCMDB Service UI Launch` tool groups to those STDs.

This is done in the HPOM for Windows console under **Tools** → **Configure** → **Service Types**.

Assigning User Roles for Services on HPOM for Windows

User Role Assignment enables you to map a service to an HPOM user role. After synchronization, the service is assigned to all operators that are included in the specified HPOM user role.

User Role Prerequisites

Make sure that at least one user role already exists in HPOM.

If the role is missing or cannot be assigned to the service, the Service CI is created and a warning is logged in HPOM DMA. Additionally, an HPOM event message should be sent to the HPOM server. No error is returned by the web service when the HPOM DMA monitoring templates are deployed.

➤ It is recommended that you do not assign a user role to every service, but to a selected set of services at the top of a tree to be managed by the specified role.

Mapping User Roles

It is necessary to create user profile mapping (`usermapping.xml`) files for the services that you want to assign to a user. One user profile mapping file is required for each synchronization package that references services that you want to assign. See the online help and the *HPOM DMA Extensibility Guide* for details on specifying User Profile mapping.

Enabling User Role Assignment

User role assignment for services is disabled by default. It can be enabled as follows:

1. Create user roles and assign operators to the roles.

   For instructions, see the HPOM for Windows documentation.

2. Enable user role assignment in the HPOM web service:

   ```
   ovconfchg -ovrg server -ns
   opc.WebService.ConfigurationItem -set
   UserProfileAssignmentEnabled true
   ```

3. Restart the IIS Admin Service:

   a. Select **Start** → **Administrative Tools** → **Services**.

   b. Right-click `IIS Admin Service`.

   c. Click **Restart**.

4. Restart Smart Message Mapping, if required:

   ```
   ovc -start dmamsg
   ```

Assigning and Deploying the OM DMA Policy Group

Assign and deploy the `OM DMA` policy group on the HPOM management server.

For details about the available templates, see Objects Installed on HPOM on page 227.

➤ When monitoring HPOM DMA in cluster installations, policies or templates should be enabled on the active node and disabled on all inactive nodes.

For information about policy or template deployment in cluster installations, see the appropriate HPOM documentation.

For HPOM for Windows installed on a cluster, policies must be controlled by the agent Application Package Manager (APM). For details, see the HPOM for Windows online help.

To assign and deploy the `OM DMA` policy group, from HPOM UI, follow these steps:

1 In the HPOM console browse to:

Policy management → **Policy groups** → **OM DMA**

2 From the shortcut menu, select:

All Tasks → **Deploy on**

The Deploy policies on window opens.

3 Select the management server.

4 Click **OK**.

Configuring HPOM DMA

To configure HPOM DMA, complete the following tasks:

- Specifying Web Service Endpoints on page 110
- Specifying Synchronization Content on page 110
- Specifying Synchronization Content on page 110

Specifying Web Service Endpoints

The web service endpoints for UCMDB and HPOM must be specified for correct connectivity. This is set from the Connections page in the HPOM DMA console. For detailed instructions, see the HPOM DMA online help.

➤ The user to be specified in the Connection page of the HPOM DMA console must have sufficient rights on the HPOM for Windows management server.

To find out which users are HPOM for Windows administrators, check the `HP-OVE-Administrators` group on the system where the HPOM for Windows management server is installed:

My Computer → **Manage** → **Local Users and Groups** → **Groups** → **HP-OVE-ADMINS** → **Properties**

Use one of these user to synchronize HPOM for Windows using HPOM DMA.

In HPOM for Windows version 8.10, the local administrator account is no longer automatically added to the `HP-OVE-Administrators` group.

Specifying Synchronization Content

Before attempting to import node and service information from UCMDB or BAC into HPOM, you must specify some basic settings:

- HPOM root service for services imported from UCMDB or BAC
- Services and nodes CIs to be synchronized
- Synchronization packages that you wish to activate

For detailed instructions, see the HPOM DMA online help.

Synchronizing Nodes and Services

After specifying the content of the HPOM DMA synchronization, you can do the following:

- Manually synchronize nodes or services in HPOM with their associated values in UCMDB.
- Set up a schedule to automatically trigger synchronizations.For detailed instructions, see the HPOM DMA online help.

8 Upgrading HPOM DMA

The HPOM DMA upgrade installs the HPOM DMA version 8.10 software onto the HPOM host system. This chapter guides you through all the required steps. This process should take approximately 60 minutes to complete.

➤ If you have HPOM DMA 8.00 installed with HPOM for Windows 8.00, you must first upgrade to HPOM for Windows 8.00 and then upgrade to HPOM DMA 8.10.

➤ Read the rest of this guide before you start the installation wizard to plan your decisions and gather the information that you need.

➤ **Upgrading on Cluster Nodes**

Upgrading HPOM DMA on a system participating in a cluster is supported on the active node only. An attempt to upgrade HPOM DMA on a non-active node is rejected by the installer.

HPOM DMA must be individually upgraded on each node participating in the cluster. For each node in the cluster, make it the active node and upgrade HPOM DMA on that node, following the instructions given in this chapter. Proceed with the next node in the cluster until HPOM DMA is upgraded on all cluster nodes.

To upgrade HP Operations Manager Dependency Mapping Automation, you must follow these steps:

1. Install HPOM DMA using the DMA Application Installer. Follow the instructions in Chapter 5, Installing HPOM DMA. The existing installation is updated.
2. If you have modified the HPOM DMA 8.00 TQL queries, back them up to a safe location. For details, see Backing Up TQL Queries on page 114.
3. Undeploy and remove the HPOM DMA 8.00 TQL queries from the UCMDB or BAC system. For details, see Removing HPOM DMA 8.00 from UCMDB or BAC on page 115.

4 Upload and deploy the HPOM DMA 8.10 TQL queries to the UCMDB or BAC system. For details, see Deploying HPOM DMA 8.10 to UCMDB or BAC on page 117.

5 If you have modified the HPOM DMA 8.00 TQL queries, open both versions of the TQL queries and merge the original modifications into the new HPOM DMA 8.10 TQL queries. For details, see Restoring TQL Query Modifications on page 118.

Backing Up TQL Queries

Backing up TQL Queries requires you to create a new package and add all TQL queries, enrichments, and views to the package.

To create a new package and add all custom and modified TQLs queries, enrichments, and views, follow these steps:

1 Open the Package Manager:

- *UCMDB*

  Admin → **Settings** → **Package Manager**

- *BAC*

  Admin → **Universal CMDB** → **Settings** → **Package Manager**

2 Click **Add**.

The Package Builder dialog box opens.

3 Enter a name and description for the new package and click **Next**.

4 Expand the Query list.

5 Select all custom and modified enrichments from the TQLs pane and add them to the right pane.

6 Select all custom and modified views from the left TQLs pane and add them to the right pane.

7 Select all custom and modified enrichments from the left Enrichments pane and add them to the right pane.

8 Select all custom and modified views from the left Views pane and add them to the right pane.

Removing HPOM DMA 8.00 from UCMDB or BAC

Removing HPOM DMA 8.00 from UCMDB or BAC requires you to undeploy and remove the HPOM DMA 8.00 package from the UCMDB or BAC system.

To undeploy and remove the HPOM DMA 8.00 package from the UCMDB or BAC system, follow these steps:

1 Remove all instances of the CI type `Service Group` from UCMDB.

The `hpdma.zip` package can only be undeployed if all references in the TQL queries are removed.

➤ You must select **Entire CMDB** in the `Search in` feature.

a Open the IT Universe Manager:

- *UCMDB*

  Admin → **Settings** → **IT Universe Manager**

- *BAC*

  Admin → **Universal CMDB** → **IT Universe Manager**

b Search for **CI type: `Service Group`**.

Service Group is found under `Business`.

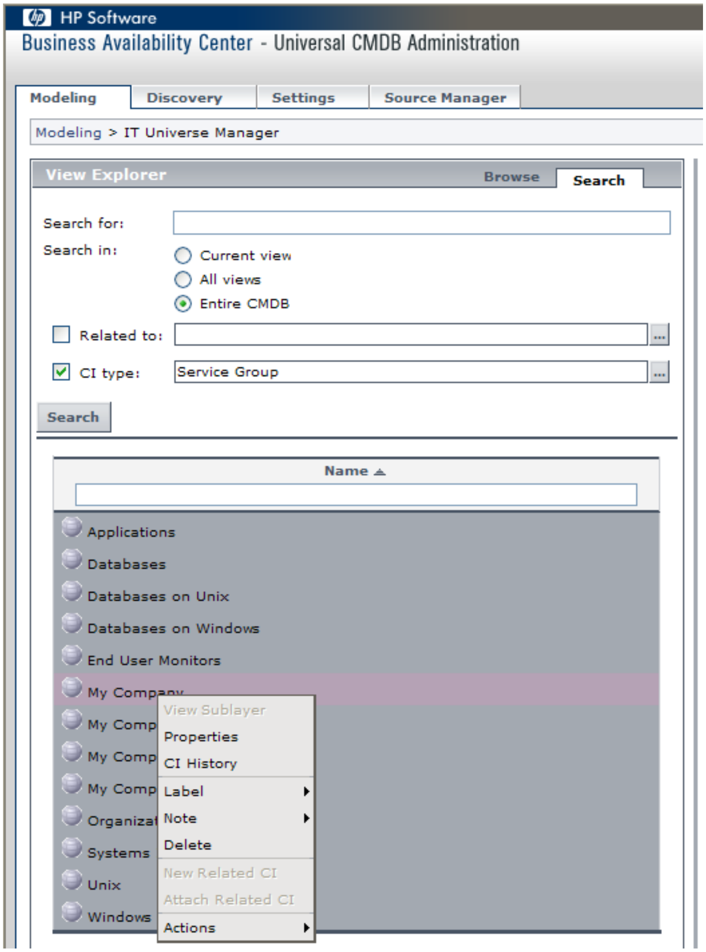
c Select all returned items.

d Right-click to open the shortcut menu.

e Select **Delete**.

An example is shown in Figure 17.

Figure 17 Removing CI Type Instances



Search for:

Search in: ○ Current view ○ All views ● Entire CMDB

☐ Related to:

☑ CI type: Service Group

2 Open the Package Manager:

- *UCMDB*

  Admin → Settings → Package Manager

- *BAC*

  Admin → Universal CMDB → Settings → Package Manager

3 Undeploy the `hpdma.zip` package and the `hpom.zip` package, if deployed.

4 Delete the `hpdma.zip` package and the `hpom.zip` package, if deployed, by selecting the package from the list and clicking **Delete**.

Deploying HPOM DMA 8.10 to UCMDB or BAC

Deploying HPOM DMA 8.10 to UCMDB or BAC requires you to upload and deploy the HPOM DMA 8.10 package to the UCMDB or BAC system.

To upload and deploy the HPOM DMA package to your UCMDB or BAC installation, follow these steps:

1 Open the Package Manager:

- *UCMDB*

  Admin → **Settings** → **Package Manager**

- *BAC*

  Admin → **Universal CMDB** → **Settings** → **Package Manager**

2 *Version 7.00*

Click **Upload package to server packages directory.**

Version 7.50

Click **Deploy** → **Add**.

3 Browse to the following directory on the HPOM DMA host system:

`<`*`InstallDir`*`>/misc/dma/`

4 Select the `hpdmacore.zip` file.

5 Click **Save/OK**.

6 For version 7.00, select the `hpdmacore.zip` file from the Package list and click **Deploy**.

7 Repeat steps step 4 to step 6 for all other required synchronization packages. For example:

- `hpdmadb.zip` for databases
- `hpdmaEUM.zip` for HP BAC End User Monitors
- `hpdmaos.zip` for operating system

- `hpdmasamples.zip` for the My Company Sample synchronization package
- `hpom.zip` for the Discovery Pattern for HPOM

Restoring TQL Query Modifications

If you have modified the HPOM DMA 8.00 TQL queries, enrichments, and views, and want to update the HPOM DMA 8.10 TQL queries with these original modifications, you have two options:

- Open both versions and manually merge the original modifications into the new HPOM DMA 8.10 TQL queries.
- Deploy the backup discovery package as created in Backing Up TQL Queries on page 114. Deploying this package overwrites the 8.10 TQLs queries, enrichments, and views with the original ones.

To select the most appropriate option, view the new HPOM DMA 8.10 TQL queries, enrichments, and views. Decide whether you can replace them or whether you need to merge the original changes into them.

9 Additional Features for HPOM DMA

HPOM DMA incorporates some additional features that make working with HPOM DMA, HPOM, UCMDB or BAC much more effective. It is not essential that you install and configure them. If you decide to use any or all of them, you may choose to set them up independently, and at any time.

The following lists HPOM DMA additional features:

- **Install and Configure the UI Launch**

  When operators receive status change messages, they can open BAC or UCMDB from the HPOM console and drill down directly to the problem area using one of the following UI Launch tools:

  - Show Correlated CI Map
  - Show Change Report
  - Show Neighborhood Map
  - Show Triage Report (BAC only)
  - Show End User Monitors (BAC only)
  - Show Service Impact (BAC only)

  To set up UI Launch for HPOM operators, you must complete some integration steps to set up the required tools and applications.

  For detailed instructions, see Installing and Configuring the UI Launch on page 121.

- **Activate and Configure Smart Message Mapping**

  To run Smart Message Mapping, you must first enable the Server-based Message Stream Interface and configure policies or templates.

  For detailed instructions, see Configuring Smart Message Mapping on page 129.

- **Select the Discovery Source**

  You can choose how to discover your services in Service Navigator. The two types of discovery sources are:

  - SPI discovery
  - UCMDB discovery

  If you want to use the UCMDB-based discovery, you must disable the service upload of the SPI discovery to avoid displaying two instances of the same service. It is recommended that you do not switch off the SPI discovery as some SPIs still need it for monitoring. Service upload is disabled by adding a filter entry corresponding to the SPI discovery that needs to be switched off.

  For detailed instructions, see Selecting the Discovery Source on page 137.

- **Restrict Service Synchronization to Nodes Managed by a Selected HPOM Management Server**

  HPOM DMA synchronizes services in UCMDB with the services monitored by HPOM. UCMDB typically maintains information about many more services than is actually managed by HPOM. HPOM DMA enables you to limit the synchronized information to those services that are of interest to a particular HPOM management server.

  For detailed instructions, see Restricting Service Synchronization to Managed Nodes on page 141.

- **Business Process Monitoring Integration**

  HPOM users can retrieve status alerts of business processes being monitored by BAC using Business Process Monitoring (BPM). To do this, you must complete the associated integration steps to set up BPM alert forwarding. You can also synchronize End User Management (EUM) views from BAC into HPOM by installing the BAC package for EUM Synchronization with HPOM DMA.

  For detailed instructions, see Integrating Business Process Monitoring on page 149.

Installing and Configuring the UI Launch

If you want to install and configure UI Launch, follow these steps:

- *For Show Change Report UI Launch:* Create and configure a Profile Database (Microsoft SQL Server) or a User Schema (Oracle). For detailed instructions, see Configure a Profile Database or User Schema on page 121.
- Upload the Applications or Tools into HPOM. For detailed instructions, see the section appropriate for the operating system of your HPOM host system: Uploading Applications into HPOM for UNIX on page 123 or Uploading Tools into HPOM for Windows on page 125.
- Install the UI Launch Web Application on the BAC or UCMDB web server. For detailed instructions, see Installing the UI Launch Web Application on page 127.

Configure a Profile Database or User Schema

To launch the Show Change Report, a Profile Database (Microsoft SQL Server) or a User Schema (Oracle) must be configured.

This task describes how to configure one or more Profile Databases on a Microsoft SQL Server or Profile User Schemas on your Oracle Server.

Prerequisites

Before you begin, make sure that you have the following connection parameters to the database server:

1. **Server Name**

   Name of the machine on which the database application is installed.

2. **Database User Name and Password**

   User name and password of a user with administrative rights on the database server.

3. **Server Port**:

   - Microsoft SQL Server's TCP/IP port (default: 1433)
   - Oracle listener port (default: 1521)

Additional prerequisite information for Oracle installations:

1 **SID**

   Oracle instance name that uniquely identifies the instance of the Oracle database being used, if different from the default value, `orcl`.

2 **Default Tablespace**

   Name of the dedicated default tablespace you created for profile user schemas. If you do not require a dedicated default tablespace, specify an alternative tablespace. The default Oracle tablespace is called `users`.

3 **Temporary Tablespace**

   Name of the dedicated temporary tablespace you created for profile user schemas. If you do not require a dedicated temporary tablespace, specify an alternate tablespace. The default Oracle temporary tablespace is called `temp`.

If required, consult with your organization's database administrator to obtain this information.

Add a Database

1 Access the Database Management page, located at:

   Admin → Platform → Setup and Maintenance → Manage Profile Databases

2 Select **MS SQL** or **Oracle**, as appropriate, from the shortcut menu, and click **Add**.

3 In the Profile Database Properties page, enter the parameters of your database. For details, see the BAC or UCMDB documentation.

Uploading Applications into HPOM for UNIX

The UCMDB or BAC UI Launch tools must be uploaded by running the `dmadrilldown-toolgen.sh` command located in the `<InstallDir>/bin` directory.

dmadrilldown-toolgen.sh Command Parameters

```
dmadrilldown-toolgen.sh <tools_tar_file> <input_file>
<output_file> <customer_id> <system_type> <URL> <user_name>
<user_password>
```

`tools_tar_file` Path to the UCMDB or BAC launch tools tar file. Specify the file appropriate for your product installation:

`dma-BACTools`

`dma-UCMDBTools`

`input_file` Path to the UCMDB or BAC launch tools files. Select the file appropriate for your product installation:

`/opt/OV/misc/dma/drilldown/dma-BACapplications.dat.src`

`/opt/OV/misc/dma/drilldown/dma-UCMDBapplications.dat.src`

`output_file` A temporary file used to upload the UCMDB or BAC launch tools. The following files are used in examples in this section:

`/opt/OV/misc/dma/drilldown/dma-BACapplications.dat`

`/opt/OV/misc/dma/drilldown/dma-UCMDBapplications.dat`

`customer_id` Typically `1`.

`system_type` `BAC` or `UCMDB`, depending on your product installation.

`URL` The URL of the BAC or UCMDB system:

`http://`*`<BAC_UCMDB_hostname>`*`:8080`

`user_name` User name used to log on to the BAC or UCMDB system (optional).

`user_password` Password used to log on to the BAC or UCMDB system (in conjunction with `user_name`).

Uploading the UCMDB or BAC launch tools requires you to execute the appropriate command for your product, specifying the host name and, if desired, the user name and password. If the user name and password are not specified, UI launches are accompanied by a log-on page where the appropriate credentials must be entered before the UI launch is allowed.

To upload the UCMDB or BAC launch tools, execute the appropriate command for your product:

- *UCMDB*

  ```
  dmadrilldown-toolgen.sh dma-UCMDBTools /opt/OV/misc/dma/
  drilldown/dma-UCMDBapplications.dat.src /opt/OV/misc/dma/
  drilldown/dma-UCMDBapplications.dat 1 UCMDB http://
  <UCMDB_hostname>:8080 <user_name> <user_password>
  ```

  Example:

  ```
  dmadrilldown-toolgen.sh dma-UCMDBTools /opt/OV/misc/dma/
  drilldown/dma-UCMDBapplications.dat.src /opt/OV/misc/dma/
  drilldown/dma-UCMDBapplications.dat 1 UCMDB http://
  myUCMDBsystem.example.com:8080 UCMDBuser MyPassWord
  ```

- *BAC*

  ```
  dmadrilldown-toolgen.sh dma-BACTools /opt/OV/misc/dma/
  drilldown/dma-BACapplications.dat.src /opt/OV/misc/dma/
  drilldown/dma-BACapplications.dat 1 BAC http://
  <BAC_hostname>:8080 <user_name> <user_password>
  ```

  Example:

  ```
  dmadrilldown-toolgen.sh dma-BACTools /opt/OV/misc/dma/
  drilldown/dma-BACapplications.dat.src /opt/OV/misc/dma/
  drilldown/dma-BACapplications.dat 1 BAC http//
  myBACsystem.example.com:8080 BACuser MyPassWord
  ```

Activating Application Groups

To be able to cross launch into BAC or UCMDB, you must activate an appropriate application group for the operator.

To activate an application group for the operator, follow these steps:

1. Open the HPOM for UNIX Application Bank.
2. Select the appropriate Application Group:
   - **Universal CMDB**
   - **Business Availability Center**
3. Open the HPOM for UNIX User Bank.
4. Modify the user as follows:
   a. In the Modify User window, click **Applications.**
   b. In the Applications of User: window, select:

      Actions → **Applications** → **Add to this Group**
5. In the Modify User: window, click **OK**.

Uploading Tools into HPOM for Windows

The UCMDB or BAC UI launch tools must be uploaded by running the `dmadrilldown-toolgen.bat` command located in the `<*InstallDir*>\bin` directory.

dmadrilldown-toolgen.bat Command Parameters

```
dmadrilldown-toolgen.bat <input_file> <output_file>
<customer_id> <system_type> <URL> <user_name>
<user_password>
```

➤ The following examples assume that you are entering the commands from the `<*InstallDir*>\bin` directory.

`input_file` Relative path to the UCMDB or BAC launch tools files. Select the file appropriate for your product installation:

`..\misc\dma\moffiles\en\dma-BACTools.mof.src`

`..\misc\dma\moffiles\en\dma-UCMDBTools.mof.src`

`output_file`	A temporary file used to upload the UCMDB or BAC launch tools. The following files are used in this section:
	`..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof`
	`..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof`

`customer_id`	Typically `1.`
`system_type`	`BAC` or `UCMDB`, depending on your product installation.
`URL`	URL of the BAC or UCMDB system: `http://<BAC_UCMDB_hostname>:8080`
`user_name`	User name used to log on to the BAC or UCMDB system (optional).
`user_password`	Password used to log on to the BAC or UCMDB system (in conjunction with `user_name`).

Uploading the UCMDB or BAC launch tools requires you to execute the appropriate command for your product, specifying the host name and, if desired, the user name and password. If the user name and password are not specified, UI launches are accompanied by a log-on page where the appropriate credentials must be entered before the UI launch is allowed.

To upload the UCMDB or BAC launch tools, execute the appropriate command for your product:

- *UCMDB*

  ```
  dmadrilldown-toolgen.bat
  "..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof.src"
  "..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof" "1"
  "UCMDB" "http://<UCMDB_hostname>:8080" <user_name>
  <user_password>
  ```

  Example:

  ```
  dmadrilldown-toolgen.bat
  "..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof.src"
  "..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof" "1"
  "UCMDB" "http://myUCMDBsystem.example.com:8080" UCMDBuser
  MyPassWord
  ```

- *BAC*

```
dmadrilldown-toolgen.bat
"..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof.src"
"..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof" "1"
"BAC" "http://<BAC_hostname>:8080" <user_name>
<user_password>
```

Example:

```
dmadrilldown-toolgen.bat
"..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof.src"
"..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof" "1"
"BAC" "http://myBACsystem.example.com:8080" BACuser
MyPassWord
```

Installing the UI Launch Web Application

The HPOM tools and applications execute a web application. This web application must be manually installed on the BAC or UCMDB web server.

To install the UI launch web application, follow these steps:

1. Create the following directory:

   `hpdma-uilaunch.war`

2. Extract the `hpdma-uilaunch.zip` file:

   a. locate the file in this directory:

      `<InstallDir>/misc/dma/`

   b. Extract the file into the directory that you created in step 1:

      `hpdma-uilaunch.war`

3. Move or copy the `hpdma-uilaunch.war` directory with all its contents to the following location:

   - *UCMDB*

     `<UCMDB-install-dir>\j2f\AppServer\webapps\`

     The default UCMDB install directory is:

     `C:\HP\UCMDB\`

   - *BAC*

     `<BAC-install-dir>\AppServer\webapps\`

The default BAC install directory is:

```
C:\HPBAC\
```

➤ The scripts should be deployed automatically. If UI Launch is not available, restart the BAC or UCMDB server process.

4 Open the following file for editing:

```
hpdma-uilaunch.war\WEB-INF\ucmdbWebService.properties
```

5 Make sure that the default URL is the URL of the UCMDB web service interface on the local machine.

The default URL takes the following form:

```
url=http://localhost:8080/axis2/services/UcmdbService
```

6 Change the user name and password for the UCMDB web service.

7 Test the availability of the script by launching the following URL from a web browser:

http://<*BAC_or_UCMDB_hostname*>:8080/hpdma-uilaunch

The deployment is successful if this URL shows a page with the message `UI Launch is available`.

Configuring Smart Message Mapping

To run Smart Message Mapping, you must:

- Enable Server-based Message Stream Interface (Server MSI).
- Start the Smart Message Mapping component.

➤ If you want to use Smart Message Mapping in cluster environments, you must make some configuration changes in the `ov-server.cntl` file. For further details, see Configuring Smart Message Mapping in Cluster Environments on page 65.

Enabling Server MSI on UNIX

To enable Server MSI, follow these steps:

1. From the Node Bank, open the **Server Configuration** dialog box.

   Actions → Server → Configure

2. In the Configure Server dialog box, select the following options:
   - **Enable Output**
   - **Send all messages to server MSI**
   - **Divert Messages**
3. Click **OK**.

Enabling Server MSI on Windows

To enable Server MSI, follow these steps:

1. In the HPOM shortcut menu, select **Configure → Server**.
2. In the Configure Server dialog box, open the **Namespace** drop-down menu and select **Server-based Message Stream Interface**.
3. Set `Enable server-based MSI` to **True**.
4. Set `Global Streaming Mode` for the server-based MSI to **Divert**.

Starting and Stoping Smart Message Mapping

To start Smart Message Mapping, execute the command:

```
ovc -start dmamsg
```

To stop Smart Message Mapping, execute the command:

```
ovc -stop dmamsg
```

Setting Smart Message Mapping Sleep Time

The Smart Message Mapping sleep delay stops the Smart Message Mapper from updating too often when there are multiple changes in Service Navigator within a short period of time.

➤ Any changes that appear in Service Navigator during the sleep time are not recognized by the Smart Message Mapper.

Set the Smart Message Mapping sleep time in the Contents page of the HPOM DMA console. For detailed instructions, see the HPOM DMA online help.

Customizing Smart Message Mapping

You can configure which separators the Smart Message Mapper uses to extract keywords and hostnames from an incoming message, and also specify whether case sensitivity is required when matching CI attributes against fields in a message ID.

These configurations are set using an ovconfchg command of the following format:

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
<parameter> <value>
```

Configuring the Keyword Separator

The keyword separator is used as the indicator for the Smart Message Mapper to divide an incoming message into the required keywords. The default keyword separator is a colon (`:`).

A typical message takes the following form:

```
service_id="OSSPI:os:filesystem:/home@@testsystem.example.com"
```

It contains the following data used by the Smart Message Mapper to identify the service:

- `OSSPI`
- `os`
- `filesystem`
- `/home`

It is possible that messages from different sources are configured to use different separators. One source may use a colon (`:`) and another source uses a number sign (#). Multiple separators can also be specified.

Setting One Keyword Separator

Do not select the same character to be used for keyword separation and hostname separation.

To set one symbol to be recognized as the keyword separator:

1 Enter the following command:

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
ServiceSeparator “<symbol>”
```

In this command, *<symbol>* is the separator used in your messages. For example, use the following command if your separator is a number sign (#):

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
ServiceSeparator “#”
```

The following message can be handled by the Smart Message Mapper:

```
service_id="OSSPI#os#filesystem#/
home@@testsystem.example.com"
```

2 Restart Smart Message Mapping:

```
ovc -restart dmamsg
```

Setting Multiple Keyword Separators:

➤ Do not select the same character to be used for keyword separation and hostname separation.

To set multiple symbols to be recognized as keyword separators:

1 Enter the following command:

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
ServiceSeparator "[<symbol1><symbol2><symbol3>...]"
```

In this command, *<symbolx>* is a separator used in your messages. For example, use the following command if your separators are a number sign (#), a dollar sign ($), and the percent sign (%):

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
ServiceSeparator "[#$%]"
```

2 Restart Smart Message Mapping:

```
ovc -restart dmamsg
```

Configuring the Hostname Separator

The hostname separator is used as the indicator for the Smart Message Mapper to identify the start of the hostname in an incoming message. The default hostname separator is two at signs (@@).

A typical message takes the following form:

```
service_id="OSSPI:os:filesystem:/home@@testsystem.example.com"
```

It is possible that messages from different sources are configured to use different separators. One source may use two at signs (@@) and another source uses a number sign (#).

➤ Do not select the same character to be used for keyword separation and hostname separation.

To set one character sequence to be recognized as the hostname separator:

1 Enter the following command:

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
HostnameSeparator "<symbols>"
```

In this command, *<symbols>* is the separator used in your messages. For example, use the following command if your separator is a number sign (#):

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
HostnameSeparator "#"
```

The following message can be handled by the Smart Message Mapper:

```
service_id="OSSPI:os:filesystem:/home#testsystem.example.com"
```

2 Restart Smart Message Mapping:

```
ovc -restart dmamsg
```

Configuring Case Sensitivity

The Smart Message Mapper is by default, configured to consider the case of the text in incoming messages. However, this is not always an advantage. For example, DNS servers are not case sensitive, and CI attributes input using a mixture of cases may be referring to the same attribute.

`MyWindowsHost.Example.COM` is viewed by the network as the same system as `mywindowshost.example.com`.

To configure case sensitivity:

1 Set the appropriate flag using the following command:

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
IgnoreCase <flag>
```

In this command, *<flag>* is one of the following:

- **true** for case insensitive
- **false** for case sensitive

For example, use the following command to set case insensitivity (ignore case):

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set
IgnoreCase true
```

2 Restart Smart Message Mapping:

```
ovc -restart dmamsg
```

Changing the Order of MSI Processes

The Message Stream Interface (MSI) API is used to register applications to receive messages on HPOM management servers. Messages are intercepted before they are added to the HPOM database and before they are displayed in the HPOM message browsers.

It might be necessary to change the order of MSI processes. For example, if an MSI process requires the original service IDs, you must assign a later order number to the Smart Message Mapping process.

For further information on changing the order of MSI processes, see the HP Operations Manager documentation.

Setting the Order in HPOM for UNIX

To set the order for the Smart Message Mapper process in MSI:

1. Open the following file in an editor:

   ```
   /etc/opt/OV/share/conf/OpC/mgmt_sv/msiconf
   ```

   ➤ If this file does not exist, create it. Add all processes that you need to order.

2. Add the following line to the file:

   ```
   DmaSMM <your order number>
   ```

   In this entry, the number is an integer and signifies where in the list of processes the `DmaSSM` process is placed.

3. Save and close the file.

Setting the Order in HPOM for Windows

To set the order for the Smart Message Mapper process in MSI:

1. Open the Operations Manager console and select the Server-based MSI policy group:

   Policy Management → **Server policies grouped by type** → **Server-based MSI**

2. Add a new policy:

   Right-click **Server-based MSI** → **New** → **Policy**

The Server-based MSI policy editor opens.

3 Select **New**.

The MSI Instance dialog box opens.

4 In the Instance Name field, specify **DmaSMM**.

5 Enter the required order number.

The number is an integer and signifies where in the list of processes the DmaSSM process is placed.

6 Select the Application type **Legacy UNIX API**.

7 Click **OK**.

8 Click **Save and Close**.

9 Add a name and description for this new policy.

10 Click **OK**.

Smart Message Mapping Simulation

The dmasmmsim command-line tool can be used to simulate and verify the behavior of the Smart Message Mapper without sending an OpC message. In the same way as the actual Smart Message Mapper, the dmasmmsim simulation tool evaluates how a message would be mapped. It responds with the selected service, where possible, without actually sending a message or updating any services in the Service Navigator. It also shows if there is no suitable service.

The dmasmmsim tool is located in *<InstallDir>*/support.

The dmasmmsim tool is executed in a similar way to the opcmsg command. It requires the following mandatory parameters:

- application name: a
- object name: o
- target node: node

The following parameter is optional:

service identifier: service_id

For example, enter the following command:

```
dmasmmsim a=oracle o=tablespace node=dbhost.example.com
service_id="openview@@dbhost.example.com"
```

The result takes the following form:

```
Found CIs: 3634
Matching CI is: openview ( ucmdb:d3bb0fc4562258ba33a43d329efe017
@@dbhost.example.com )
```

Sending Messages to Virtual Services

There are two basic types of services:

- Hosted services — mainly representing CIs
- Virtual services — representing a service such as a mail service, provided by an organization for use by users.

There are two ways to send a message to a virtual service:

- Using a service ID:

  ```
  opcmsg a=oracle o=tablespace node=dbhost.example.com
  service_id="mailservice" sev=warning msg_text="service slow"
  ```

- Using application and object, and forcing the Smart Message Mapper to search only for a virtual service by providing a dummy node. A dummy node is a node without associated services.

  It is recommended that you create such a dummy node with the sole purpose of triggering the Smart Message Mapper to look for a virtual service when this node is specified in a message.

  If you need to send a message to a virtual service, the following format is required:

  ```
  opcmsg a=virtual_service o=object1:object2 node=dummynode
  ```

Selecting the Discovery Source

You can choose how to discover your services in Service Navigator.

The two types of discovery sources are:

- SPI discovery
- UCMDB discovery

You may want to use the UCMDB-based discovery as the source for displaying services in Service Navigator, but continue to use SPIs for monitoring. If both the UCMDB-based discoveries and the SPI-based discoveries are activated, you see two service trees in Service Navigator. SPI-generated messages are used to identify status in the SPI-based discovery service tree.

When you are satisfied that the service tree derived from the UCMDB discovery is being correctly displayed, you can disable the service upload of the SPI discovery and delete the service tree generated from the SPI discovery. This avoids displaying two instances of the same service.

It is recommended that you do not switch off the SPI discovery as some SPIs still need it for monitoring. You can disable the service upload only. See Disabling SPI Discovery Service Upload for HPOM for UNIX on page 137 and Disabling SPI Discovery Service Upload for HPOM for Windows on page 138 for details.

To continue to identify status in the UCMDB-based discovery service tree, activate Smart Message Mapping. For detailed instructions, see Configuring Smart Message Mapping on page 129.

Service upload for a particular SPI discovery is disabled by adding a filter entry corresponding to the SPI discovery that needs to be switched off.

Disabling SPI Discovery Service Upload for HPOM for UNIX

On HPOM for UNIX, to disable a discovery service upload to Service Navigator, an option must be added to the associated application to stop the service upload.

To disable discovery from a SPI, follow these steps:

1. Open the required Application Bank:

Application Bank → ***<A_Group>*** → ***<A_Discovery_Group>*** → ***<A_Discovery_Application>***

Example:

Application Bank → **UNIX OS SPI Group** → **OS SPI Discovery Group** → **OS SPI Discovery Application**

2 Right-click the application and select **Modify**.

3 In the Application Call statement, replace the command with the following:

```
/opt/OV/SPISvcDisc/bin/SPI_DiscServOprInt.sh -v -f /opt/
OV/lib/osspi/UnixOSSPI_Disc.conf -n "$OPC_NODES"
```

4 In the Additional Parameters field, enter the parameter:

```
-u false
```

5 Click **OK**.

6 Delete the service tree generated from the SPI discovery. For details, see the HPOM for UNIX documentation.

Disabling SPI Discovery Service Upload for HPOM for Windows

On HPOM for Windows, any discovery source that must be disabled is added to the XPL configuration under the namespace `DiscoveryServiceFilter`. This namespace contains a list of service ID patterns used to filter out any service that should not be uploaded into Service Navigator. The patterns are matched against the text at the beginning of every service ID. For example, if discovery from the OSSPI is to be disabled, messages from the OSSPI must be ignored. This is done by filtering out any messages starting with the string:

```
OSSPI:
```

The XPL configuration has the following format, where a comma separated value list of patterns specifies the services that are filtered out:

```
[DiscoveryServiceFilter]
Excludes=OSSPI:,DBSPI:,MySPI,MyService
```

Disabling Discovery from a SPI from the HPOM for Windows UI

To disable discovery from a SPI with messages that start with the `OSSPI:` strings, follow these steps:

1 From the HPOM for Windows UI, start the Disable SPI Discovery tool:

Go to **Tools** → **HP Operations Manager Tools** → **Disable SPI Discovery** and double-click the tool.

The Tool Status window and the Disable SPI Discovery windows are opened.

2 In the Disable SPI Discovery window, add the required statements. In the example, this is:

```
OSSPI:
```

➤ If you are adding statements, make sure that you add commas between the existing statements and the new ones.

3 Click **OK**.

➤ If you select **Cancel**, a confirmation window opens with two portions:

- **OK** - All filter statements are deleted.
- **No** - Original filter statements are retained.

4 Delete the OSSPI service tree generated from the SPI discovery.

Disabling Discovery from a SPI using XPL Configuration

The XPL configuration can also be modified with the XPL configuration tools. Use the `ovconfchg` command to add the discovery filters to the configuration, as described in the following procedure.

To add the discovery filters to the configuration, follow these steps:

1 Execute the following command:

```
ovconfchg -edit
```

The configuration file opens in a text editor (for example, Notepad).

2 In the editor window, add the following statements:

```
[DiscoveryServiceFilter]
Excludes=OSSPI:
```

3 Save the changes.

4 Delete the OSSPI service tree generated from the SPI discovery.

Restricting Service Synchronization to Managed Nodes

HPOM DMA synchronizes services in UCMDB with the services monitored by HPOM. UCMDB typically maintains information about many more services than are actually managed by HPOM. HPOM DMA enables you to limit the synchronized information to those services that are of interest to a particular HPOM management server.

To help you do this, Discovery Pattern package is included. To install it, follow these steps:

1. Installing the Discovery Probe Patch (Version 7.00 Only) on page 141 for BAC and UCMDB version 7.00.
2. Modifying the UCMDB or BAC Classloader on page 142.
3. Instal l the Discovery Pattern on the BAC or UCMDB system. For detailed instructions, see Installing the BAC or UCMDB Discovery Pattern for HPOM on page 142.

To restrict service synchronizations you must configure the TQL queries to match your selected HPOM management server. For detailed instructions, see Modifying the TQL Queries to Specify the HPOM Management Server on page 144.

Installing the Discovery Probe Patch (Version 7.00 Only)

The UCMDB or BAC discovery probe in BAC and UCMDB version 7.00 has a problem where custom Java code is not recognized.

To correct this behavior:

1. Go to the following web site

   http://support.openview.hp.com/selfsolve/patches

2. From the `Universal CMDB (Application Mapping)` section, select **All Versions** and click **Search**.
3. Go to the page entitled:

   Patch 06.HP Operations Manager (Sonata) discovery

4. Download the `AM_00368.zip` patch package.
5. Extract the files from the package file to a temporary location.

6. Install the patch by following the instructions included with the patch.
7. Restart the discovery probe.

Modifying the UCMDB or BAC Classloader

To modify the UCMDB or BAC classloader, follow these steps:

1. Open the following configuration file for editing:

   ```
   <Discovery_Probe_InstallDir>\scripts\install\conf\
   WrapperEnv.conf
   ```

2. Find the `set COLLECTORS_PROBE_CLASSPATH` entry:

   ```
   set COLLECTORS_PROBE_CLASSPATH=%MAM_JARS%;%lib%/
   collectors;%JDBC_CLASSES% ...
   ```

3. Add the following paths to the start of the statement:

   ```
   %lib%/collectors/probeManager/discoveryResources/
   saaj-api.jar;;%lib%/collectors/probeManager/
   discoveryResources/jaxb-api.jar;
   ```

   The statement should now be as follows:

   ```
   set COLLECTORS_PROBE_CLASSPATH=%lib%/collectors/probeManager/
   discoveryResources/saaj-api.jar;;%lib%/collectors/
   probeManager/discoveryResources/
   jaxb-api.jar;%MAM_JARS%;%lib%/collectors;%JDBC_CLASSES% ...
   ```

4. Save and close the configuration file.
5. Restart the Probe.

Installing the BAC or UCMDB Discovery Pattern for HPOM

To install the Discovery Pattern for HPOM on the BAC or UCMDB system, follow these steps:

1. Open the Package Manager:

   - *UCMDB*

     Admin → Settings → Package Manager

   - *BAC*

Admin → **Universal CMDB** → **Settings** → **Package Manager**

2 *Version 7.00*

Click **Upload package to server packages directory.**

Version 7.50

Click **Deploy** → **Add**.

3 Browse to the following directory on the HPOM DMA host system:

`<InstallDir>/misc/dma/`

4 Select the `hpom.zip` file.

5 Click **Save**.

6 Select the `hpom.zip` file from the Package list and click **Deploy.**

7 From the Discovery tab, select **Domain Configuration**.

8 Go to **Credentials** → **OM WS Protocol**

9 Click **Add new connection details for selected protocol type**.

The Add Protocol Parameter dialog box opens.

10 Specify the credential required by the HPOM management server. The required fields are:

- Port Number
- User Label
- User Name
- User Password
- HTTP protocol (http/https)

  If you are using the https protocol for secured connection, you must create a keystore for the web service client. This keystore must be located at:

  ```
  <Discovery_Probe_InstallDir>\root\lib\collectors\
  probeManager\discoveryScripts
  ```

Multiple credentials may be specified.

11 Open the Job Configuration page:

- *UCMDB*

Admin → **Discovery** → **Job Configuration**

- *BAC*

  Admin → **Universal CMDB** → **Discovery** → **Job Configuration**

12 Select **Application HPOM Topology** → **HPOM by WS**

13 Right-click **HPOM by WS**, and from the shortcut menu, select **Activate**.

14 Right-click **HPOM by WS**, and from the shortcut menu, select **Run Now**.

The discovered topology is now configured.

Modifying the TQL Queries to Specify the HPOM Management Server

To modify a TQL query to restrict synchronization to data that relates to nodes and services managed by a particular HPOM management server, follow these steps:

1 Open the View Manager:

- *UCMDB*

  Admin → **Modeling** → **View Manager**

- *BAC*

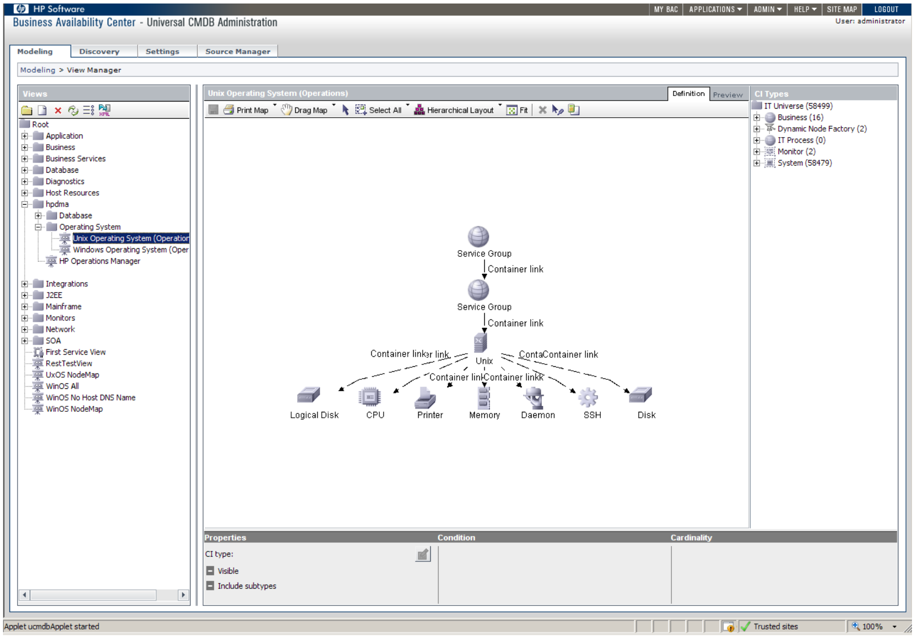
  Admin → **Universal CMDB** → **Modeling** → **View Manager**

2 Expand the **hpdma** view from the Views list.

An example is shown in Figure .

The TQL queries are divided into the following groups:

- `Database`
- `EUM`
- `Operating System`
- `Organization`



3 Select a TQL query.

4 Add HPOM Agent and Relationship:

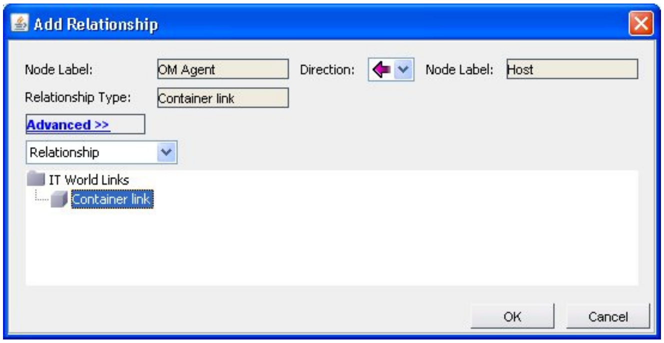
a From the CI Types list, navigate to `OM Agent`:

IT Universe → System → Software Element → Agent → OM Agent

b Drag the **OM Agent** onto the TQL Query pane.

c Create a `Container link` relationship from the `Host` to the `HPOM Agent`.

In the TQL Query pane, right-click the **HPOM Agent** and the **Host**. From the shortcut menu, select **Add Relationship**.



Add Relationship

Node Label: OM Agent

Direction: ←

Node Label: Host

Relationship Type: Container link

5 Add HPOM Server and Relationship:

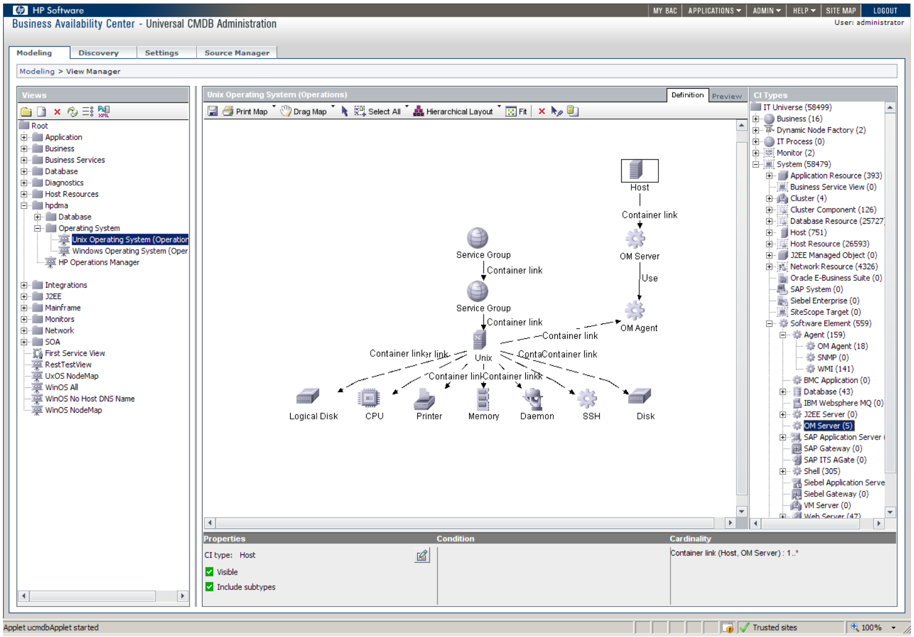
a From the CI Types list, navigate to `OM Server`:

IT Universe → **System** → **Software Element** → **OM Server**

b Drag the **OM Server** onto the TQL Query pane.

c Create a `Use` relationship from the `HPOM Server` to the `HPOM Agent`.

An example is shown in Figure .



CI type: Host

☑ Visible

☑ Include subtypes

Container link (Host, OM Server) : 1..*

6 Add Host and Relationship:

a From the CI Types list, navigate to `Host`:

IT Universe → System → Host

b Drag the **Host** onto the TQL Query pane.

c Create a `Container link` relationship from the `Host` to the `HPOM Server`.

7 Right-click the newly added host that represents the HPOM management server and select **Node Condition**.

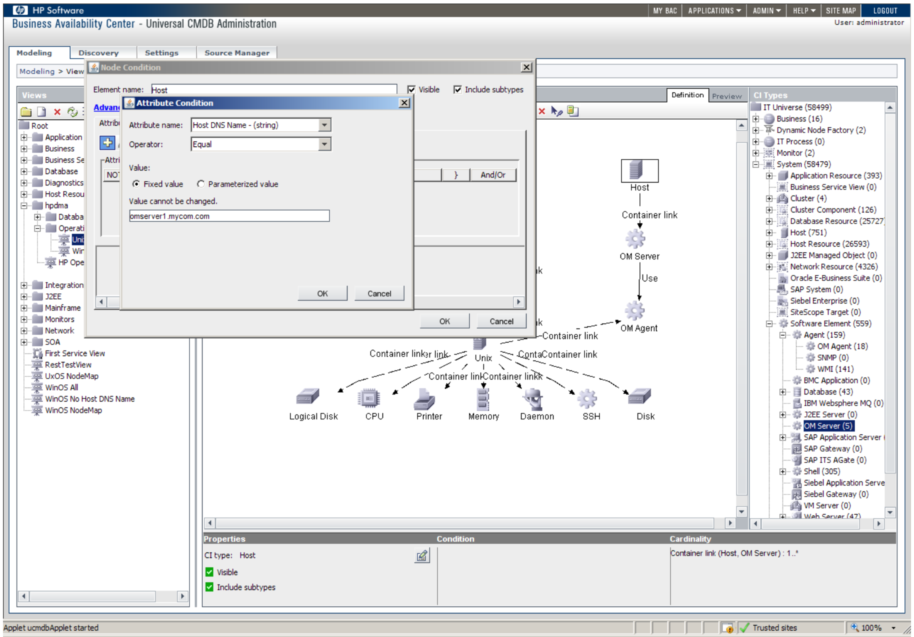
The Node Condition dialog box opens.

8 Click **Add** to open the Attribute Condition dialog box.

9 Select the following:

- Attribute name: **Host DNS Name - (string)**
- Operator: **Equal**
- Value: **Fixed Value** (Value cannot be changed.)

Enter the fully qualified host name of the HPOM management server system in the Value field, as shown in Figure .



Node Condition

Element name: Host ☑ Visible ☑ Include subtypes

Attribute Condition

Attribute name: Host DNS Name - (string)

Operator: Equal

Value: ● Fixed value ○ Parameterized value

Value cannot be changed.

omserver1.mycom.com

Properties: CI type: Host ☑ Visible ☑ Include subtypes

Cardinality: Container link (Host, OM Server) : 1..*

10 Click **OK**.

11 Verify using the **Preview** tab.

12 If the preview displays the required results, for each newly added CI Type and relationship in the TQL query:

a Select **Node Condition**.

b Clear the `Visible` check box and click **OK**.

In the example, the Host and the OM Agent are added CI types that must not be visible. The two Container links and the Use relationship connecting the Host and the OM Agent to the system CI must also not be visible.

The TQL query is now modified to synchronize only the services being managed by the specified HPOM management server.

Integrating Business Process Monitoring

HPOM operators can retrieve status alerts of business processes being monitored by BAC using Business Process Monitoring (BPM). When HPOM operators receive status change messages, they can open the BAC End User Monitors view from the HPOM console and drill down directly to the problem area.

To set up Business Process Monitoring for HPOM operators, complete these tasks:

- Task 1: Forwarding BPM Alerts to HPOM on page 149
- Task 2: Setting Up CI Status Alerts on page 149
- Task 3: Setting Up Performance Limit Alerts on page 151

Forwarding BPM Alerts to HPOM

To enable operators to forward BPM alerts to HPOM, follow these steps:

- Make sure the HPOM agent is installed on the BAC server system.
- Make sure an `opcmsg` policy or template is created and deployed for the BAC alerts.
- Log on to the BAC UI at the following location:

  http://<*hostname*>/topaz

Alerts can be set up to trigger on exceeding performance limits or when there is a change in the status of a CI. The CI Status Alerts are recommended because they can capture all status changes within the monitored business process.

Setting Up CI Status Alerts

To set up CI Status Alerts, follow these steps in the BAC UI:

1 Open the CI Status Alerts tab:

  Admin → Alerts → CI Status Alerts

2 Select the End User Monitors view.

3 Click **New Alert**.

The Create New Alert dialog box opens.

4 Click **Next** and set up a new alert as follows.

5 Specify a name and description and use the condition **Send alert if status worsens**.

6 Click **Next** and select the required CIs.

7 Click **Next** and go to **Actions** and click **New Executable File**.

8 In the Create New Executable File dialog box, enter an `opcmsg` command.

Example:

```
opcmsg service="BPM" a="<<Alert Name>>" o="<<CI Name>>"
msg_t="<<Current Status>>: <<KPI Name>> = <<KPI Value>>"
-option KPIName="<<KPI Name>>" -option KPIValue="<<KPI
Value>>" -option PreviousStatus="<<Previous Status>>"
-option CurrentStatus="<<Current Status>>" -option
TriggerTime="<<Trigger Time>>"
```

➤ The example assumes that there is a service with the name BPM in the service tree. This is a manually added service. If you plan to synchronize the End User Monitors view, you should change the service parameter to *<CI_name>*.

9 Click **OK**.

10 Click **Finish**.

The alert summary page opens.

11 Click **OK** to apply the CI status alert. It is then available in the alert list.

BPM alerts are now available in the HPOM console.

12 To see a report of generated alerts, open the CI Status Alert Reports tab:

Applications → **Alerts** → **CI Status Alert Reports**

For further information about CI Status Alerts in Business Process Monitoring, see the BAC online help from the Help menu.

Setting Up Performance Limit Alerts

To set up alerts on performance limits, follow these steps in the BAC UI:

1 Open the Event Based Alerts Configuration page:

Admin → Alerts → Event Based Alerts → Event Based Alerts Configuration

2 Select a business process profile from the **Profile:** drop-down list.

3 Click **New Alert**.

The Create Alert Wizard opens.

4 Select a trigger type from the Trigger Criteria tab. For example, `Transaction response time` or `Average transaction response time`.

5 Select the **Filters** tab and specify any required restrictions.

6 Select the **Actions** tab and click **Run executable file**.

The Run Executable File dialog box opens.

7 In the Run Executable File dialog box, select **User defined** from the drop-down menu and enter the name of the file you want to execute.

The file should contain an `opcmsg` command.

Example:

```
opcmsg service="BPM" a="<<Profile Name>>"
o="<<Transaction Name>>" msg_text="<<Severity>>: <<Actual
Details>>, BPM location: <<Location Name>>" -option
AlertName="<<Alert Name>>" -option
AlertPurpose="<<AlertPurpose>>" -option ID="<<ID>>"
-option LocationName="<<Location Name>>" -option
Severity="<<Severity>>" -option TriggerCause="<<Trigger
Cause>>" -option UserMessage="<<User Message>>"
```

➤ The example assumes that there is a service with the name BPM in the service tree. This is a manually added service. If you plan to synchronize the End User Monitors view, you should change the service parameter to *<CI_name>*.

8 Click **OK** to close the Run Executable File dialog box.

9. Select the **Settings** tab and set severity and notification frequency.
10. Click **Finish**.
11. To see a report of generated alerts, open the Event-Based Alerts Reports tab:

    Applications → **Alerts** → **Event-Based Alerts Reports**

BPM alerts are now available in the Performance Limit Alerts in Business Process Monitoring, see the BAC online help from the Help menu.

Synchronizing EUM Views

You can also synchronize End User Management (EUM) views from BAC into HPOM.

To synchronize EUM views, complete these tasks:

- Task 1: Installing the BAC Package for EUM Synchronization with HPOM DMA on page 152
- Task 2: Activating the End User Monitors Synchronization Package on page 154

The following are automatically installed:

- An additional Synchronization Package for HPOM DMA
- Additional Service Type Definitions and Compositions for the EUM CI types are automatically uploaded into HPOM during the HPOM DMA installation

➤ End User Monitors are only available in BAC and not in the standalone UCMDB product. Do not deploy to a UCMDB installation.

Installing the BAC Package for EUM Synchronization with HPOM DMA

The BAC package is a ZIP file installed to the following location during installation:

`<Install_Dir>\misc\dma\hpdmaEUM.zip`

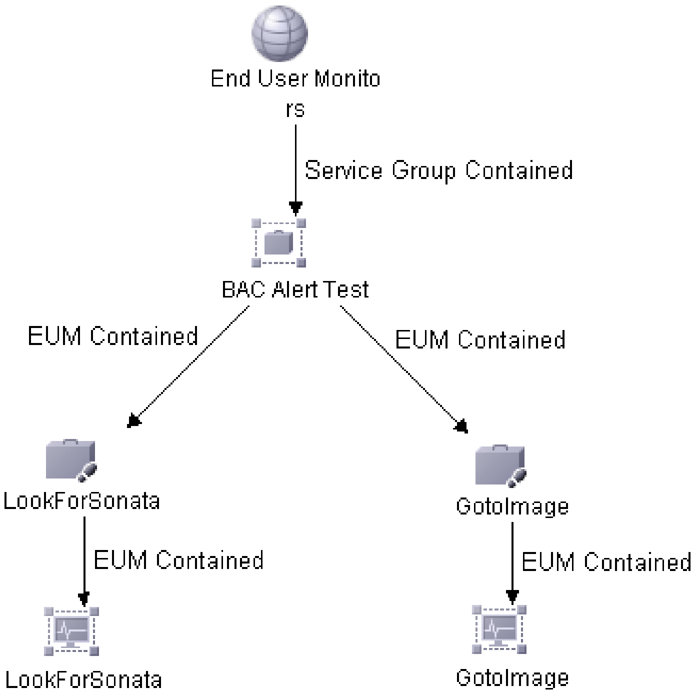
The `hpdmaEUM.zip` package contains:

- `EUM contained` UCMDB containment relationship type

- UCMDB enrichment rule used to prepare the EUM tree for synchronization
- `End User Monitors (Operations)` view TQL, which can be queried by HPOM DMA using the UCMDB web service interface

Figure 18 shows an example of an EUM View in BAC selected by the `End User Monitors (Operations)` view TQL.

Figure 18 EUM View in BAC Selected by End User Monitors (Operations) View TQL



To upload and deploy the BAC package to your BAC installation, follow these steps:

1. Open the Package Manager in BAC:

   Admin → Settings → Package Manager

2. *Version 7.00*

Click **Upload package to server packages directory**.

Version 7.50

Click **Deploy** → **Add**.

3 Browse to the following directory on the HPOM DMA host system:

`<InstallDir>/misc/dma/`

4 Select the `hpdmaEUM.zip` file.

5 Click **Save**.

6 Select the `hpdmaEUM.zip` file from the Package list and click **Deploy**.

Activating the End User Monitors Synchronization Package

The synchronization package for the EUM synchronization is automatically installed during HPOM DMA installation as a standard synchronization package.

To activate the End User Monitors Synchronization Package:

1 Open the Synchronization configuration page and check the **End User Monitors (BAC only): Out of the box synchronization package for BAC End User Monitors**.

2 Click **Save**.

3 Start a new synchronization form the Synchronization page.

On completion, the EUM view is synchronized into HPOM.

10 Licensing

This chapter describes how to install and configure OVkey licenses for HPOM DMA.

OVkey Licenses

HPOM DMA uses the HP AutoPass licensing security technology for the management of OVkey licenses. All OVkey license passwords are stored in a license file, maintained by AutoPass.

Because the OVkey licensing technology does not require a license server, the product may be used behind firewalls and in clustered environments.

When installing and setting up OVKey licenses in your HPOM DMA environment, keep the following points in mind:

- Licenses are linked to the IP address of the HPOM DMA host system and not its target ID.
- Each HPOM DMA installation has one central location for license administration.

➤ The HPOM DMA installation on the selected Windows host system requires a valid licence. PA-RISC HPOM for UNIX host systems do not need an HPOM DMA licence.

Types of Licenses

You can obtain the following types of licenses:

- **Instant-On License**

  This license is install with HPOM DMA and enables you to use HPOM DMA for evaluation purposes. You can use HPOM DMA for a period of 60 days. You can extend its validity once for a further 60 days by submitting a request to the HP Password Delivery Service.

- **Permanent License**

  A permanent license allows you unlimited use of HPOM DMA for the associated installation.

  See Requesting a Product License on page 160 for more details about requesting licenses.

- **Evaluation License**

  An extended temporary license allows you an extra 60 days evaluation period for HPOM DMA.

  If the permanent license key is not yet available, or if more evaluation time is needed, an evaluation extension license key can be requested at no cost through the local password center. These requests should be made by Telephone, although email and fax requests are also accepted. Evaluation extension license keys may be requested once only, and they are valid only for the system specified in the request. Some products do not have extension keys available. Hewlett-Packard reserves the right to restrict the availability of extension license keys at any time.

  ➤ Evaluation extension requests cannot be made through the web. If the request is urgent and the local regional password center is closed, the password center that is open in another region can be contacted.

  Have the following information available before requesting an Evaluation Extension:

  - Software product number
  - IP address or host name of the system where the evaluation software is installed.
  - Contact information (company, name, address, phone, and email).

Evaluation extension keys are sent out through email and are valid for 60 days. See the product documentation for information on license key installation.

Checking Licenses

HPOM DMA checks licenses during startup and when scheduled, once every 24 hours.

If your Instant-On license has not expired, you are informed of the days remaining before the license expires.

If your Instant-On license has expired, you receive a message in a message browser once every 24 hours.

Setting Up OVkey Licenses

To set up and activate an HPOM DMA product license, follow these steps:

1. Obtain the required information from your host system.

   See Getting the Required Information on page 158 for details.

2. Complete the HP Software License Request Form by doing one of the following:

   - Edit the request-form file for a licence, then email, fax, or mail the file to HP.
   - Fill out an online form at the HP Internet License Request Center.

   See Requesting a Product License on page 160 for details.

3. Receive a license from the HP Password Delivery Center.

   See Receiving License Passwords on page 162 for details.

4. Install and verify the HPOM DMA Product License.

   See Installing Product Licenses on page 162, and Verifying Product Licenses on page 163 for details.

Getting the Required Information

You can get the information specified in Table 1 on page 159 from documents included with your product.

Table 1 Information Required to Get Licenses

Information Required	Where to Find It
HP Order Number (permanent passwords only)	License-to-Use Entitlement Certificate Local system administrator or HP Sales Representative.
IP address of the HPOM DMA[a] host system	On the HPOM DMA host system, execute the following command in a Command Prompt window: • *UNIX* **`/usr/bin/nslookup <hostname>`** • *Windows* **`ipconfig /all`**
Hostname[b]	On the HPOM DMA host system, execute the following command in a Command Prompt window: **`hostname`**
Operating System Version	On the HPOM DMA host system: • *UNIX* Execute the following command in a Command Prompt window: **`uname -a`** • *Windows* Go to **Start** → **Control Panel** → **System** → **General**
Number of Licenses (permanent passwords only)	HP Purchase Order

[a] If you are operating in a clustered environment, the IP address of the HPOM DMA cluster package and all local IP addresses of the participating nodes are required.

[b] If you are operating in a clustered environment, the fully qualified host name of the HPOM DMA cluster package and all fully qualified host names of the participating nodes are required.

Requesting a Product License

You may request a license in one of two ways:

- **Internet**

  If you have access to the Internet, you can use the HP Internet Password Delivery Service.

- **Mail, Phone or Fax**

  If you do not have access to the Internet, you can complete and submit a license request form.

AutoPass stores the passwords at a location that is typically not shared in HA environments, and it also uses the local IP address and not the virtual IP address, make sure that you request license passwords for all cluster nodes in an HA environment with its physical IP address and install these passwords on the according cluster nodes.

Requesting by Internet

If you can access the Internet, you can get license passwords by visiting the home page of the HP Password Delivery Service at the following location:

http://www.webware.hp.com/

You can use this site to do the following:

- **Generate Passwords**

  Generate new product passwords, assuming you have already purchased a product and have an HP order number.

- **Move Licenses**

  Move licenses from one machine to another.

- **Migrate Licenses**

  Migrate licenses from an older version of a product to a new version using a migration password.

- **Contact a Password Delivery Center**

  Locations, contact details, and availability of the HP Password Delivery Centers.

- **Passwording FAQs**

  Information about licensing and passwords.

Requestting by Mail, Phone or Fax

If you do not have access to the Internet, you can request a license by mail or fax using the licence request template on the back of the entitlement certificate. Enter the requested information, and mail or fax it to the nearest HP Password Delivery Center using the information in Table 2.

Table 2 HP Password Delivery Centers

Your Location	Password Center Location	Email Address	Phone/*Fax* Number	Service Hours (Mon-Fri Local Time)
North/South America	USA	americas_password@cnd.hp.com	+1 (801) 431-1597 +1 (800) 326-0411 *+1 (801) 431-3654*	06:00-18:00 (MST)[a]
Asia/Pacific	Japan	asia_password@cnd.hp.com	Japanese: +81 (3) 3227-5264 English: +81-(3)-3227-5672 *+81 (3) 3227-5238*	09:00-17:00 (JST)[b]
Europe and Africa	Netherlands	europe_password@cnd.hp.com	+31 (55) 543 4642 *+31 (55) 543 4645*	09:00-18:00 (CET)[c]

[a] Mountain Standard Time (U.S.A.)

[b] Japanese Standard Time

[c] Central European Time

For further information, see the HP License Key Delivery Service web site:

https://webware.hp.com/

Receiving License Passwords

You should receive your license password in one of two time frames:

- **Immediately (Internet)**

  If you order a password on the HP License Center Internet site, you receive a license password immediately.

- **Within 48 hours (mail, fax)**

  If you order a password by mail, fax, or phone, you receive a license password within 48 hours of receipt from one of the Password Delivery Centers listed in Table 2 on page 161.

You receive your password in one of three ways:

- **Email**

  If you provide an email address on your request form, you receive your password by email.

- **Fax**

  If you do not specify an email address, you receive your password by fax.

- **Phone**

  If you do not specify either a fax number or an email address, you receive your password by phone.

Installing Product Licenses

The HPOM DMA installation on the selected Windows host system requires a valid licence. Remote HPOM host systems do not need an HPOM DMA licence.

To install the HPOM DMA product license using AutoPass, follow these steps:

1. Start AutoPass using the script or batch file appropriate for your operating system:

   - *UNIX*

     ```
     <InstallDir>/bin/startDmaLicenseUI.sh
     ```

- *Windows*

  ***<InstallDir>*\bin\startDmaLicenseUI.bat**

2 From the AutoPass menu, select **Install/Restore Licences**.

3 In the File path dialog box, click **Browse**.

4 In the Browse dialog box, select **All Files** and browse to the license file to be installed and click **Install**.

Verifying Product Licenses

You can verify licenses using the AutoPass License Report tool. It provides information on the installed passwords.

To verify the HPOM DMA product license, follow these steps:

1 Start AutoPass using the script or batch file appropriate for your operating system:

- *UNIX*

  ***<InstallDir>*/bin/startDmaLicenseUI.sh**

- *Windows*

  ***<InstallDir>*\bin\startDmaLicenseUI.bat**

2 From the AutoPass menu, select **Licences Report**.

3 Verify that the license you have installed is listed.

11 Securing

The following features for making working with HPOM DMA more secure are available:

- Secure the web service communication between HPOM DMA and HPOM with SSL Configuration.
- Restrict IIS access to a single port by linking Tomcat and IIS using the JK Connector.
- Grant access to users' LDAP authentication.

Configuring SSL on UNIX

To configure SSL on UNIX systems, complete the following procedures:

1. Configuring Tomcat for SSL HTTP/1.1
2. Exporting Certificates for HPOM DMA Clients on page 166
3. Configuring HPOM DMA to Use SSL on page 173

Configuring Tomcat for SSL HTTP/1.1

To configure Tomcat to run an SSL HTTP/1.1 connector, follow these steps:

1. Open the following file for editing:

   ```
   <InstallDir>/nonOV/tomcat/b/conf/server.xml.ovtemplate
   ```

2. Uncomment the connector port specification from the following section:

```
<!-- Define an SSL HTTP/1.1 Connector on port 8444 -->
<!--@ENABLESTANDALONEHTTPS@
<Connector port="@STANDALONESERVERPORTFORHTTPS@" maxHttpHeaderSize="8192"
              maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
              enableLookups="false" disableUploadTimeout="true"
              acceptCount="100" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS"
              keystoreFile="@TOMCAT_KEYSTORE_FILE@" />

@END_ENABLESTANDALONEHTTPS@-->
```

It should appear as follows:

```
<!-- Define an SSL HTTP/1.1 Connector on port 8444 -->
<Connector port="@STANDALONESERVERPORTFORHTTPS@" maxHttpHeaderSize="8192"
              maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
              enableLookups="false" disableUploadTimeout="true"
              acceptCount="100" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS"
              keystoreFile="@TOMCAT_KEYSTORE_FILE@" />
```

3 Save and close the file.

4 Upload the changes to the template with the command:

```
<InstallDir>/nonOV/tomcat/b/bin/ovtomcatbctl -configure
```

5 Restart the Tomcat server using the commands:

```
ovc -stop ovtomcatB
ovc -start ovtomcatB
```

Exporting Certificates for HPOM DMA Clients

To export server certificates for use by clients, follow these steps:

1 Go to the directory containing the Tomcat keystore file:

```
cd <DataDir>/certificates/tomcat/b
```

2 List the certificates contained in the keystore using the Java keystore tool (keytool):

```
<InstallDir>/nonOV/jre/b/bin/keytool -list -keystore
tomcat.keystore
```

3 Enter the keystore password. If the password is not known just press return when prompted.

The following output is displayed:

```
*****************  WARNING WARNING WARNING  *****************
* The integrity of the information stored in your keystore  *
* has NOT been verified!  In order to verify its integrity, *
* you must provide your keystore password.                  *
*****************  WARNING WARNING WARNING  *****************

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

ovtomcatb, Jun 25, 2007, keyEntry,
Certificate fingerprint (MD5):
96:C6:07:A8:11:02:9E:D4:99:CB:BF:07:39:22:00:69
```

4 Export the Tomcat server certificate using `keytool`, and specify the alias name obtained from the listing, for example, `ovtomcatb`:

```
<InstallDir>/nonOV/jre/b/bin/keytool -keystore
tomcat.keystore -export -alias ovtomcatb -file /tmp/
server.cer
```

5 Enter the keystore password. If the password is not known just press return when prompted.

The following output is displayed:

```
Certificate stored in file <server.cer>
```

The certificate is saved to the specified file in a format that can be imported into a Java keystore file for use by the HPOM DMA Gateway and Smart Mapper client applications.

6 Specify the location of the keystore file in the HPOM configuration settings:

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore
"location of <client.keystore> file"
```

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore
/var/opt/OV/shared/server/certificates/dma/
client.keystore
```

7 Restart the Tomcat server using the commands:

```
ovc -stop ovtomcatB
ovc -start ovtomcatB
```

To configure the client to use SSL, see Configuring HPOM DMA to Use SSL on page 173.

Securing Clustered Systems with SSL

To provide SSL communication through the virtual IP address of a cluster, you must use an SSL certificate for Tomcat that is issued for the virtual IP of that cluster. For example, if your cluster consists of the hosts `hostA` and `hostB`, and is accessible externally using a virtual IP `hostV`, a certificate must be issued for `hostV`.

Also make sure, that the URL of the HPOM management server web service uses the virtual IP of the cluster (for example, **http://hostV:80/...**) and not `localhost`.

Configuring SSL on Windows

To configure SSL on Windows systems, complete the following procedures:

1. Switching HPOM to Use SSL
2. Exporting Certificates for HPOM DMA Clients on page 171
3. Configuring HPOM DMA to Use SSL on page 173

Switching HPOM to Use SSL

To switch HPOM to use an SSL connection, create a server certificate and configure the web services to use SSL:

1. Open the Internet Information Services (IIS) Manager control panel:

   Start → **Control Panel** → **Administrative Tools** → **Internet Information Services (IIS) Manager**

2. Navigate to the Default Web Site:

   <hostname> → **Web Sites** → **Default Web Site**

3. Open the Directory Security tab in the Properties dialog box:

   Right-click **Default Web Site**, select **Properties**, and open the **Directory Security** tab.

4. Install a server certificate (or select an existing certificate):

   a. From the Secure Communications section, click **Server Certificate.**

   b. Follow the steps of the `Web Server Certificate Wizard`.

   Alternatively, you can use tools like `SelfSSL` from the IIS Resource kit to install a self-signed server certificate.

5. Open the file for editing from the following location:

   `<InstallDir>\www\webapps\omws\web.config`

6. In the bindings section, change each instance of the XML element name `httpTransport` to **`httpsTransport`**.

7. Save the file.

8 Restart the Default Web Site in IIS:

Right-click ***<hostname>*** → **All Tasks** → **Restart IIS**

Checking the SSL Configuration

To check that the SSL connection is correctly configured, from the Internet Information Services (IIS) Manager control panel:

1 Navigate to the `omws` entry in the Default Web Site folder:

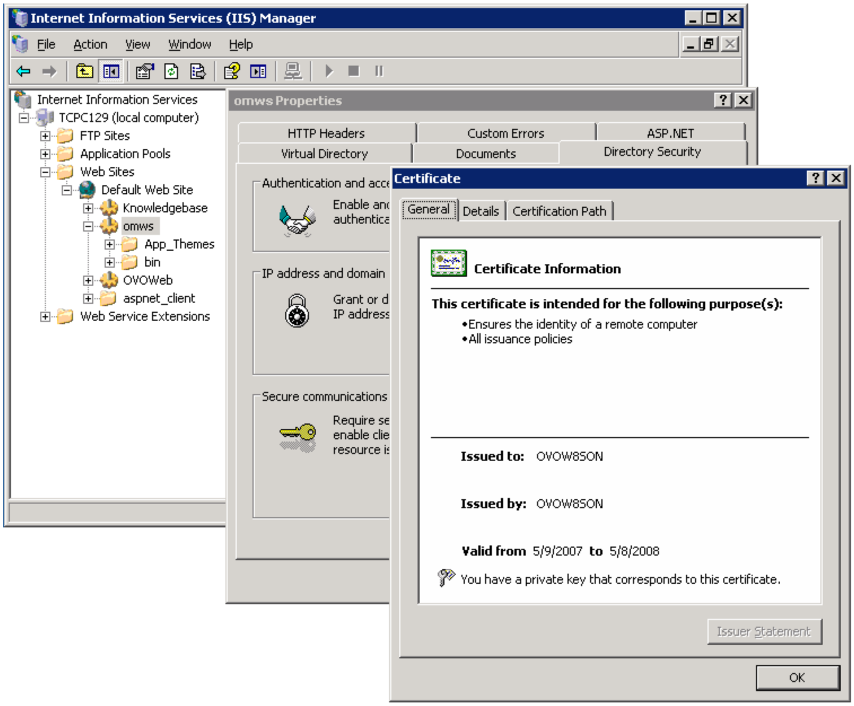
<hostname> → **Web Sites** → **Default Web Site** → **omws**

2 Open the Directory Security tab in the Properties dialog box:

Right-click **Default Web Site**, select **Properties**, and open the **Directory Security** tab.

3 From the Secure Communications section, click **Server Certificate.**

The certificate that you installed is displayed.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- All issuance policies

Issued to: OVOW8SON

Issued by: OVOW8SON

Valid from 5/9/2007 **to** 5/8/2008

You have a private key that corresponds to this certificate.

Exporting Certificates for HPOM DMA Clients

To export server certificates for use by web service clients, follow these steps from the Internet Information Services (IIS) Manager control panel:

1. Navigate to the `omws` entry in the Default Web Site folder:

   <hostname> → **Web Sites** → **Default Web Site** → **omws**

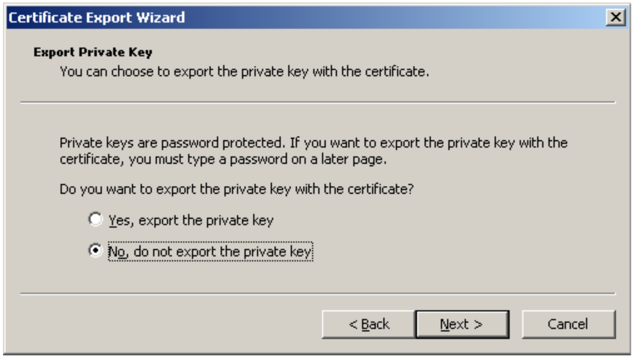
2. Open the Directory Security tab in the Properties dialog box:

   Right-click **Default Web Site**, select **Properties**, and open the **Directory Security** tab.

3. From the Secure Communications section, click **View Certificate.**

   The Certificate dialog box opens.

4. Select the **Details** tab.
5. Click **Copy to File**.
6. Click **Next**.
7. Select **No, do not export the private key** and click **Next**.



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

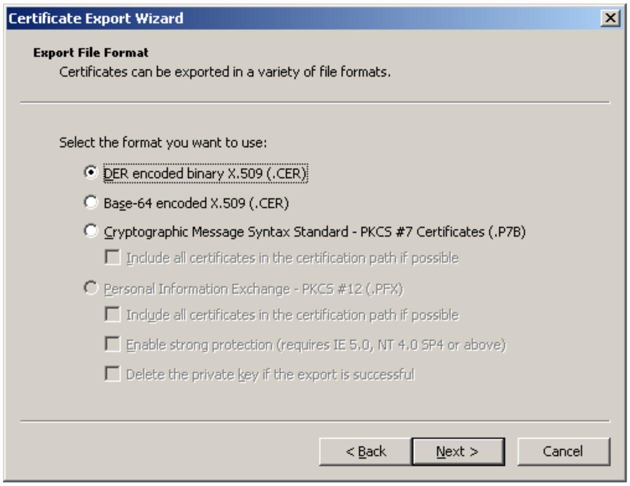
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

8 Select the format **DER encoded binary X.509 (.CER)** and click **Next**.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

9 Enter a file name to hold the certificate:

Example:

`C:\OMWServerCertificate.cer` and click **Next**.

10 Click **Finish** and then **OK**.

The certificate is saved to the specified file in a format that can be imported into a Java keystore file for use by the HPOM DMA gateway and Smart Message Mapper client applications.

To configure the client to use SSL, see Configuring HPOM DMA to Use SSL on page 173.

Configuring HPOM DMA to Use SSL

To configure HPOM DMA to use SSL:

1 From the Connection page in the HPOM DMA console or in the `DefaultSyncTask.settings` file, change the URL to use the HTTPS protocol and the SSL port of the server as follows:

- *UNIX*

  ```
  hpOmWsEpr=https://<Hostname>:8444/ConfigurationItem/
  ```

- *Windows*

  ```
  hpOmWsEpr=https://<Hostname>:443/omws/
  ConfigurationItem.svc
  ```

In this command, hostname is the name of the system to which the certificate is issued.

2 Check if the client keystore already exists:

```
<InstallDir>/nonOV/jre/b/bin/keytool -list -keystore
<SharedDir>/certificates/dma/client.keystore
```

3 Get a copy of the server certificate exported on the HPOM server. See Exporting Certificates for HPOM DMA Clients on page 166 or Exporting Certificates for HPOM DMA Clients on page 171 for details.

4 Copy the server certificate file `ServerCert.cer` to the directory:

```
<SharedDir>/certificates/dma
```

If this directory does not exist, create it.

5 Create the Java keystore file for the client and import the server certificate into it:

```
<InstallDir>/nonOV/jre/b/bin/keytool -import -file
<SharedDir>/certificates/dma/serverCert.cer -keystore
<SharedDir>/certificates/dma/client.keystore
```

6 Select and enter a password for the keystore.

7 When asked to trust this keystore, enter **`yes`**.

8 Specify the location of the keystore file in the HPOM configuration settings:

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore
"location of <client.keystore> file"
```

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore
"C:/ProgramData/HP/HP BTO Software/shared/server/
certificates/dma/client.keystore"
```

9 Stop and restart the Tomcat server and all other processes dependent on the Tomcat server using the commands:

```
ovc -stop ovtomcatB
ovc -start
```

➤ If you want to use an SSL connection to LDAP or UCMDB, you also need to import their respective certificates into the client keystore. In this case, follow the import instructions in step 5 on page 173, using the certificates of your LDAP server or UCMDB server as appropriate.

10 Test the connection from the Connections page of the HPOM DMA console. If the connection test is successful, the configuration is complete and correct.

Restricting IIS Access to a Single Port

The JK Connector can be used to provide a single port of entry for IIS and Tomcat services using port redirection for HPOM DMA Configuration web pages.

Setting Up a Distributed System

To set up a distributed system consisting of an outward facing IIS web server and an internal HPOM DMA installation hosted on Tomcat, complete the following procedure:

1 Download the `isapi_redirect.msi` connector installer package from:

http://archive.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/jk-1.2.15/

➤ You must use the JK Connector. The JK2 Connector is obsolete.

2 Extract the package and execute the installer. Further information can be found at:

http://tomcat.apache.org/connectors-doc/miscellaneous/faq.html

The installer creates a folder structure containing a few files, sets some registry entries, creates an IIS virtual directory, and adds the `isapi_redirect.dll` to the IIS web site ISAPI filters tab.

3 Add a Web Service Extension as follows. This must be done manually because the installer works for IIS 5 and 6, but Web Service Extension applies only to IIS 6.

a Open the Internet Information Services console:

Start → **Administrative Tools** → **Internet Information Services (IIS) Manager**

b In the tree on the left, expand the web server that is running on the local computer and click **Web Service Extensions**.

In general this tree lead is called `<`*`nodename`*`> (local computer).`

c In the right hand pane, click **Add a new Web Service Extension**.

d For the Extension Name, enter **`Jakarta Tomcat`** and click **Add**.

e Browse and select:

```
<drive>:\Program Files\Apache Software Foundation\Jakarta
Isapi Redirector\bin\isapi_redirect.dll
```

f Click **OK**.

g Select the `Set Extension status to Allowed` check box.

h Click **OK**.

The installer looks for a Tomcat listener on localhost.

4 Add the HPOM DMA context. The following assumes a default HPOM DMA install, with your application in:

http://*<your-host>*:8081/hpdma/

Adding the HPOM DMA Context

To add the `HPOM DMA` context, follow these steps:

1 On the IIS web server, open the following file in an editor:

```
C:\Program Files\Apache Software Foundation\Jakarta Isapi
Redirector\conf\uriworkermap.properties
```

In the `# [URL]=[Worker name]` section, add this line:

`/dma/*=wlb`

2 Save the file.

3 Restart the `IIS Admin` services from:

Start → Administrative Tools → Services

4 Test the connector with HPOM DMA using the following URL:

http://*<your-host>*:8081/hpdma

➤ Omit the port 8081. The default port 80 is then used.

If you want to block remote access to port 8081 on Tomcat completely, complete the procedure described in Restricting Access to Localhost on page 177.

Restricting Access to Localhost

It is often desirable to restrict access to Tomcat's web application to specified host names or IP addresses only. Only clients at those specified sites are then served content. Tomcat incorporates two valves that you can configure and use for this purpose:

- `RemoteHostValve`
- `RemoteAddrValve`

These valves enable you to filter requests by host name or by IP address, and to allow or deny hosts that match. If you run HPOM DMA, you may want to allow access to it only from the localhost. This can be achieved by using the following statement:

```
<Context path="/path/to/secret_files" ... >
  <Valve className="org.apache.catalina.valves.RemoteAddrValve?"
     allow="127.0.0.1" deny=""/>
</Context >
```

If no `allow` attribute pattern is specified, all requests that match the `deny` attribute patterns are rejected, and all others are allowed. Similarly, if no `deny` attribute pattern is specified, requests that match the `allow` attribute patterns are allowed, and all others are denied.

Change the Tomcat Server AJP Port

If the Tomcat server AJP port used for the HPOM DMA installation has been changed, for example, if a port conflict occurs, an alternative port must be specified.

To specify an alternative port, follow these steps:

1 Open the following file for editing:

   `<`*`InstallDir`*`>\nonOV\tomcat\b\server.xml.ovtemplate`

2 Find the section that defines the AJP 1.3 Connector:

```
<!-- Define an AJP 1.3 Connector on port 8010 -->
<!--
<Connector port="8010"
       redirectPort="8444"
       enableLookups="false" debug="0" protocol="AJP/1.3" />
-->
```

3 Remove the comment marks around the port specification lines and make a note of the connector port value:

```
<!-- Define an AJP 1.3 Connector on port 8010 -->

<Connector port="8010"
       redirectPort="8444"
       enableLookups="false" debug="0" protocol="AJP/1.3" />
```

4 Edit the file:

`<drive>:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\conf\workers.properties.minimal`

5 Change the following line:

— From:

```
worker.ajp13w.port=8009
```

— To:

`worker.ajp13w.port=<AJPPort>`

In the example, *<AJPPort>* is the port value (`8010`) you noted in step 3.

6 Save the file.

7 Restart the `IIS Admin` services from:

Start → Administrative Tools → Services

LDAP Authentication

HPOM DMA supports authentication using LDAP. Consult your LDAP administrator to gather the configuration values required by HPOM DMA. The values are:

- **Host name or IP address of the LDAP server**

  ```
  ldap.server.address=<DNS_or_IP_Address_LDAP_Server>
  ```

- **Port on LDAP server**

  ```
  ldap.server.port=<Network_Port_LDAP_Server>
  ```

- **Protocol prefix for LDAP connection**

  ```
  ldap.server.protocol=<Protocol_ldap_or_ldaps>
  ```

- **Root of LDAP schema**

  ```
  ldap.schema.root=o\=<LDAP_root>
  ```

- **Branch containing user entries in the LDAP schema**

  ```
  ldap.schema.people=ou\=<Users_branch>
  ```

- **Branch containing group entries in the LDAP schema**

  ```
  ldap.schema.groups=ou\=<Groups_branch>
  ```

- **Canonical name attribute for groups**

  ```
  ldap.schema.group.cn.identifier=<Common_name_identifier>
  ```

- **Distinguished name attribute for users**

  ```
  ldap.schema.user.dn.identifier=<Distinguished_name_
  identifier>
  ```

- **Allowed groups definition**

  ```
  ldap.allowed.groups=<GROUP_Name1>;<GROUP_Name2>;...
  ```

The LDAP configuration values are stored in the `ldap.properties` file and is located at:

```
<SharedDir>/conf/dma/ldap.properties
```

An example of this file is illustrated in Configuring LDAP Access on page 182.

Figure 19 on page 181 shows a typical LDAP schema.

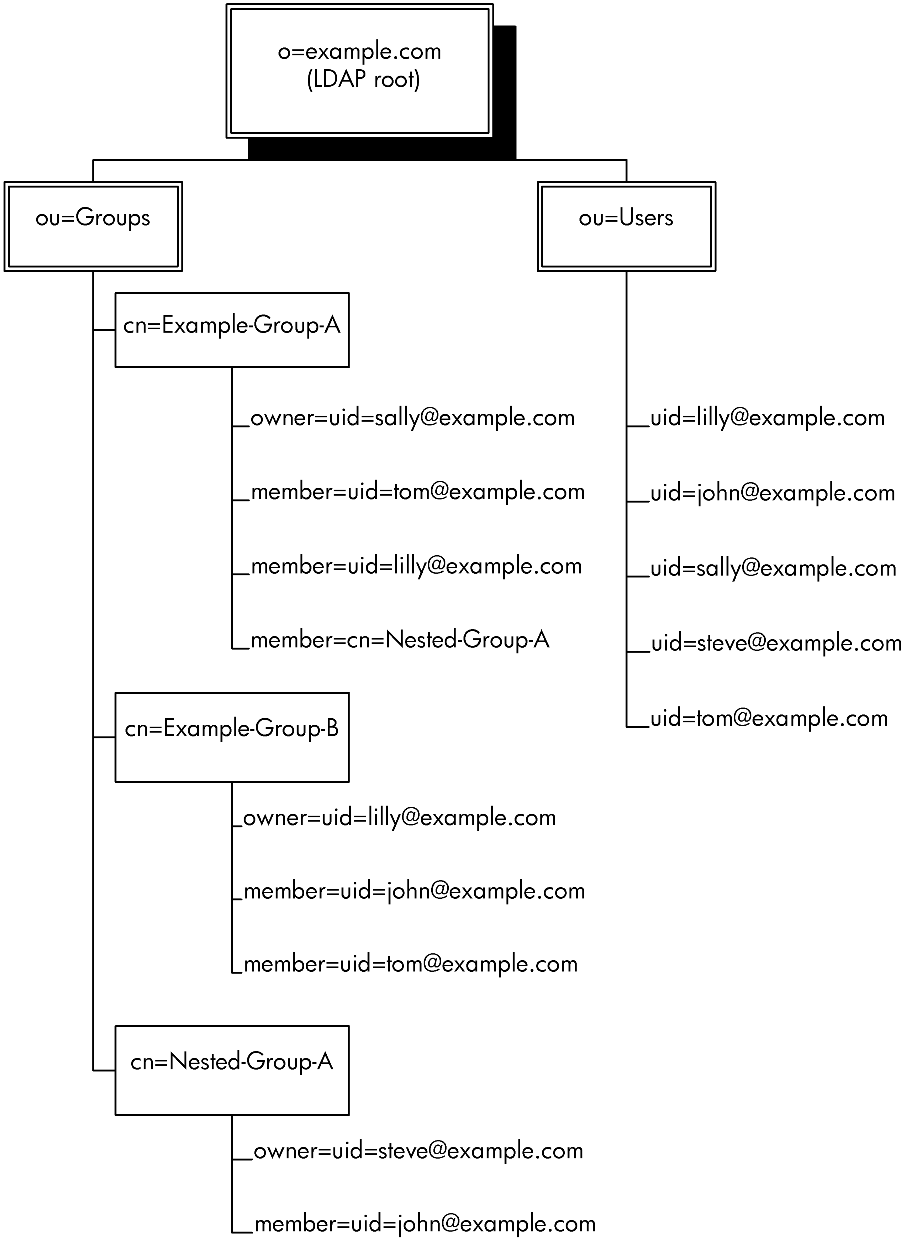
➤ If configuring SSL protected LDAP (`ldaps`), download the LDAP server certificate and import it into the client.keystore and restart the Tomcat server.

To import the LDAP server certificate into the Java keystore file, execute the following command:

```
<InstallDir>/nonOV/jre/b/bin/keytool -import -file
<Downloaded_LDAP_Server_Certificate> -keystore <DataDir>/
certificates/dma/client.keystore
```

If the keystore file does not exist, it is generated.

Figure 19 A Sample LDAP Schema



Configuring LDAP Access

To configure LDAP access, you must modify the `ldap.properties` file as follows:

1 Open the `<SharedDir>/conf/dma/ldap.properties` file for editing:

```
# Defines the host name or IP address of the LDAP server
# example: ldap.example.com
ldap.server.address=192.168.1.1
# Defines the LDAP server's port and protocol prefix
# Defaults are: 389 & ldap for non-SSL
#               636 & ldaps for SSL
ldap.server.port=636
ldap.server.protocol=ldaps
# Defines the LDAP schema's root
# Examples: o\=com
#               o\=example.com
ldap.schema.root=o\=example.com
# Defines the LDAP schema's branch containing user entries
# Examples: ou\=example
#        or dc\=Users
ldap.schema.people=ou\=Users
# Defines the LDAP schema's branch containing group entries
# Examples: ou\=groups
#        or dc\=Groups
ldap.schema.groups=ou\=Groups
# Defines the groups' canonical name attribute
ldap.schema.group.cn.identifier=cn
# Defines the users' distinguished name attribute
# Example: uid\=\{0\}
ldap.schema.user.dn.identifier=uid\=\{0\}
# Defines the allowed LDAP groups
# Multiple groups are separated by semicolons
ldap.allowed.groups=Example-Group-A;Example-Group-B;
Example-Group-E
```

2 Specify the LDAP configurations that are appropriate for your implementation. The example in Figure 19 is reflected in the `ldap.properties` configuration file.

➤ Equal signs (=) and accolades must be escaped with a backslash (\) in the `ldap.properties` file, as shown in the `ldap.properties` file example, because of character encoding in ISO 8859-1.

When specifying allowed groups definitions, do not use spaces before, after, or within group names. In the following example, the first group cannot be recognized, but the second is correctly specified:

```
ldap.allowed.groups= Example Group A;Example-Group-B;
```

3. Save and close the `ldap.properties` file.
4. Specify the location of the keystore file in the HPOM configuration settings:

   ```
   ovconfchg -ovrg server -ns wsman.client -set ssl.keystore
   "location of <client.keystore> file"
   ```

   — *UNIX*

   ```
   ovconfchg -ovrg server -ns wsman.client -set
   ssl.keystore /var/opt/OV/shared/server/certificates/
   dma/client.keystore
   ```

   — *Windows*

   ```
   ovconfchg -ovrg server -ns wsman.client -set
   ssl.keystore "C:/ProgramData/HP/HP BTO Software/
   shared/server/certificates/dma/client.keystore"
   ```

5. Restart the Tomcat server to activate the modified LDAP settings:

   ```
   ovc -stop ovtomcatB
   ovc -start
   ```

➤ Only group members and not group owners can be authenticated with this release.

Logging In Using LDAP Authentication

Using LDAP, you must enter the LDAP Uid (user’s distinguished name identifier), as specified in the `ldap.properties` file, as your user name. In the example, a user logon is `sally@example.com`.

12 Backup, Restore, and Migration

It is possible to make a copy of an existing HPOM DMA setup (tasks, synchronization packages, and connection information) from an existing HPOM DMA installation to another installation. This process can be used for simple copies as well as for backup and restore. It is also applicable to cases where individual synchronization packages need to be migrated.

➤ Before starting a migration, make sure that you have installed HPOM DMA on an alternative HPOM host system running the same operating system as the source system.

Backing up, restoring, and migrating HPOM DMA installations does not manage data synchronized from the UCMDB or BAC. Likewise, it does not back up information available within HPOM.

A separate license is required for the alternative HPOM host system.

Backing Up an HPOM DMA Configuration

To back up the HPOM DMA configuration, copy the following directory and all of its contents from the source system to an alternative, secure location:

```
<SharedDir>/conf/dma
```

Example:

```
C:\Documents and Settings\All Users\Application Data\HP\
HP BTO Software\shared\server\conf\dma
```

Backing Up HPOM DMA TQL Queries

Backing up HPOM DMA TQL queries requires you to create a new package containing the existing UCMDB resources (views and enrichments) being used by HPOM DMA.

To back up your TQL queries and enrichments, follow these steps:

1. Open the Package Manager:

   - *UCMDB*

     Admin → **Settings** → **Package Manager**

   - *BAC*

     Admin → **Universal CMDB** → **Settings** → **Package Manager**

2. Create a backup package:

   — *BAC and UCMDB Version 7.00*

   a. Click **Add**.

      The Package Builder dialog box opens.

   b. Enter a name and description for the new package.

   c. Add the HPOM DMA TQLs from **Root** → **Enrichment** → **hpdma** to the right pane.

   d. Add all the HPOM DMA TQLs from **Root** → **Views** → **hpdma** → ***<subfolders>*** to the right pane.

   e. Add all the HPOM DMA views from **Root** → **hpdma** → ***<subfolders>*** to the right pane.

   f. Add all the HPOM DMA enrichments from **Root** → **hpdma** → ***<subfolders>*** to the right pane.

   g. Click **Save package**.

   — *BAC and UCMDB Version 7.50*

   a. Click **Add**.

      The Create New Package Wizard opens.

   b. Enter a name and description for the new package and click **Next**.

c. Expand **Query** → **TQLs** → **Enrichment** and check `hpdma`.

d. Expand **Query** → **TQLs** → **View** and check `hpdma`.

e. Expand **Query** → **Views** and check `hpdma`.

f. Expand **Query** → **Enrichments** and check `hpdma`.

g. Click **Next**.

   A summary of the selections that you have made is displayed.

h. Click **Finish**.

Restoring the Default HPOM DMA Configuration

To restore the default HPOM DMA configuration:

1. Copy the default data from the storage directory:

   `<`*`InstallDir`*`>/newconfig/DataDir/conf/dma`

   Example:

   ```
   C:\Program Files\HP\HP BTO
   Software\newconfig\DataDir\conf\dma
   ```

2. Place the default data into the configuration directory:

   `<`*`SharedDir`*`>/conf/dma`

   Example:

   ```
   C:\Documents and Settings\All Users\Application Data\HP\
   HP BTO Software\shared\server\conf\dma
   ```

Moving an HPOM DMA Configuration

To move an HPOM DMA configuration, follow these steps:

1 *Optional:* Back up the existing configuration.

Copy the following directory and all of its contents on the source system to an alternative location:

```
<SharedDir>/conf/dma
```

Example:

```
C:\Documents and Settings\All Users\Application Data\HP\
HP BTO Software\shared\server\conf\dma
```

2 Make sure that the following location on the target system is empty:

```
<SharedDir>/conf/dma
```

3 Copy the existing configuration to the following location on the target system:

```
<SharedDir>/conf/dma
```

4 If you do not need the original installation any longer, delete the following directory and all of its contents from the source system:

```
<SharedDir>/conf/dma
```

5 Uninstall HPOM DMA. For further information, see Chapter 13, Uninstalling.

Recreate a Synchronization Package

It is possible to recreate an existing HPOM DMA setup (tasks, synchronization packages, and connection information) from an existing HPOM DMA installation to another installation. This process can be used for simple copies as well as for backup and restore operations. It is also applicable to cases where individual synchronization packages need to be migrated.

➤ Before starting a move, make sure that you have installed HPOM DMA on an alternative HPOM host system running the same operating system as the source system.

You cannot transfer the data from an HPOM DMA installation on an HPOM for Windows system to an HPOM DMA installation on an HPOM for UNIX system.

Make a Copy of a Synchronization Package

To move an HPOM DMA synchronization package configuration, follow these steps:

1 Copy the subdirectory used for the synchronization package configuration, for example, `myspi`, and all of its contents from the source system to the target system:

   ```
   <SharedDir>/conf/dma/sync-packages/
   ```

   Example:

   - *UNIX*

     ```
     /var/opt/OV/shared/server/conf/dma/sync-packages/
     ```

   - *Windows*

     ```
     C:\Documents and Settings\All Users\Application
     Data\HP\HP BTO Software\shared\server\
     conf\dma\sync-packages\
     ```

➤ All subdirectory names must be unique. You may need to rename synchronization packages when copying subdirectories to the directory:

```
<SharedDir>/conf/dma/sync-packages/
```

2 Make sure that the name in the `bundle.xml` file for the relocated synchronization package is unique and preferably matches the name of the synchronization package.

   Example:

   ```
   <Name>My_Application</Name>
   ```

3 Include the relocated synchronization package to be synchronized from the Synchronization page on the target system.

13 Uninstalling

Uninstalling HPOM DMA consists of two procedures:

- Uninstalling HPOM DMA
- Post-Uninstallation Cleanup on page 194

Uninstalling HPOM DMA

➤ Applications are stopped and restarted by the HPOM DMA application installation process during installation, uninstallation, and repair. For detailed instructions, see Applications Stopped and Restarted During Installation on page 58

To delete the installed HPOM DMA components from the system:

1 Start the HP Software Installer:

   - *UNIX*

     Execute the following command:

     ```
     /opt/OV/Uninstall/HPDma/setup.bin
     ```

   - *Windows*

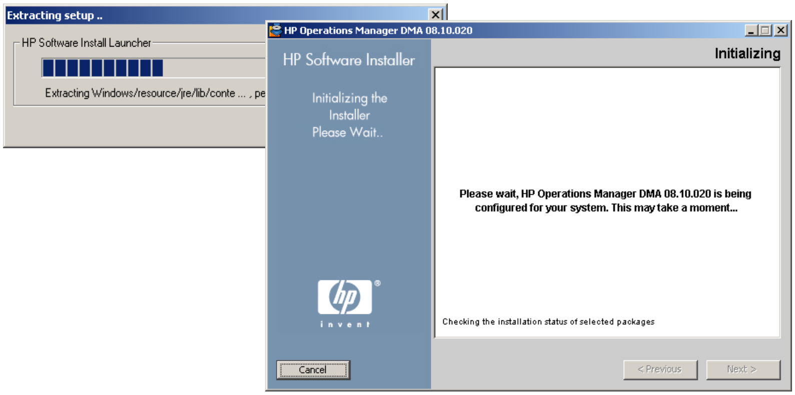
     Select one of the following options:

     – Select the program:

       Control Panel → **Add or Remove Programs** → **HP Operations Manager Dependency Mapping Automation** and click **Change/Remove**.

     – Execute the following command:

       ```
       <InstallDir>/Uninstall/HPDma/setup.exe
       ```



Extracting setup ..

HP Software Install Launcher

Extracting Windows/resource/jre/lib/conte ... , pe

HP Operations Manager DMA 08.10.020

HP Software Installer

Initializing the Installer Please Wait..

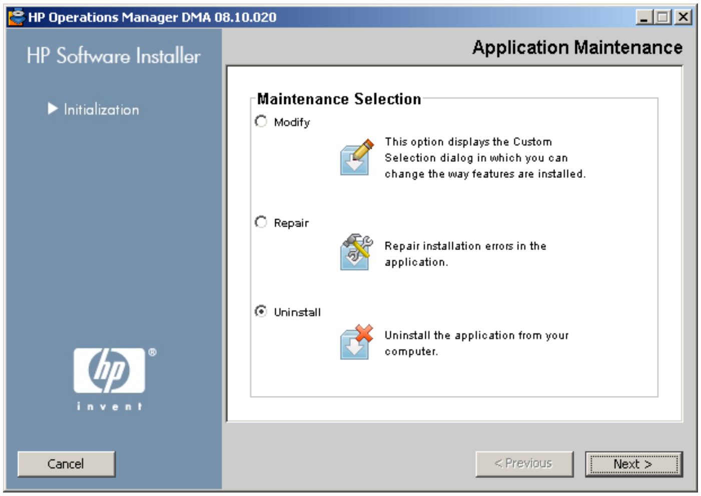
Initializing

Please wait, HP Operations Manager DMA 08.10.020 is being configured for your system. This may take a moment...

Checking the installation status of selected packages

2 Select **Uninstall** and click **Next**.

Follow the on screen instructions and progress through the installation process using the **Next** and **Uninstall** buttons.



HP Operations Manager DMA 08.10.020

HP Software Installer

▶ Initialization

Application Maintenance

Maintenance Selection

○ Modify

This option displays the Custom Selection dialog in which you can change the way features are installed.

○ Repair

Repair installation errors in the application.

● Uninstall

Uninstall the application from your computer.

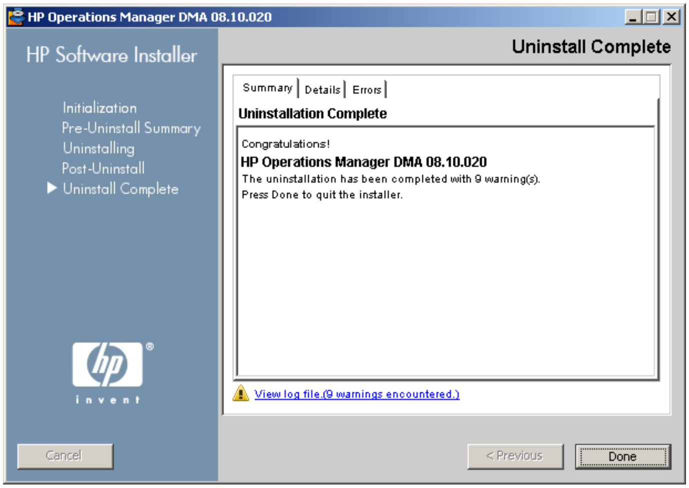
3 After the uninstallation process is finished, the Uninstall Complete window opens showing a summary of the uninstallation paths used.

You can also access the uninstallation log file from the link in this window and open it in a web browser.

The removed packages are listed under the **Details** tab.

If any errors occurred during the Uninstallation, they are summarized under the **Errors** tab.

4 Click **Done** to close the installation program.



Uninstallation Complete

Congratulations!
HP Operations Manager DMA 08.10.020
The uninstallation has been completed with 9 warning(s).
Press Done to quit the installer.

View log file (9 warnings encountered.)

Now go to the Post-Uninstallation Cleanup on page 194 to complete the HPOM DMA uninstallation.

Post-Uninstallation Cleanup

If you want a completely clean system, you must remove a number of files and directories from the HPOM and UCMDB or BAC systems. Follow these instructions to complete your cleanup.

If you are sure that you no longer need any HPOM DMA personalized configurations, delete the HPOM DMA configuration files. After these files are removed, reinstalling HPOM DMA reverts to the default configuration files. If in doubt, retain these files or create a backup copy in a safe location.

Removing the HPOM DMA Configuration Files

Remove the following HPOM DMA configuration files:

- *UNIX*

  ```
  <SharedDir>/shared/server/conf/dma/ldap.properties
  <SharedDir>/shared/server/conf/dma/users.properties
  ```

- *Windows*

  ```
  <SharedDir>\conf\dma\ldap.properties
  <SharedDir>\conf\dma\users.properties
  ```

Removing Log Files

All log files not mentioned in the following sections are shared with other HP products and should not be deleted.

- **HPOM Web Service Log Files**

  Remove the following log files:

  — *UNIX*

  ```
  <SharedDir>/log/om/ciws.<*>.<locale>
  ```

  — *Windows*

  ```
  <SharedDir>\log\om\ws.trace.txt
  ```

- **Synchronization and Smart Message Mapper Log Files**

  Remove the following directory and all of its contents:

  — *UNIX*

  ```
  <SharedDir>/log/dma
  ```

  ```
  rm -rf <SharedDir>/log/dma
  ```

  ```
  <SharedDir>/log/om
  ```

  ```
  rm -rf rm -rf <SharedDir>/log/om
  ```

  — *Windows*

  ```
  <SharedDir>\log\dma
  ```

- **HPOM DMA Web Console (CWC) Log Files**

  ⚠ Remove only if no other application is running in the CWC web UI.

  Remove the following log files:

  — *UNIX*

  ```
  <DataDir>/tmp/cwc.log
  ```

  — *Windows*

  ```
  <drive>:\Windows\system32\cwc.log
  ```

- **Tomcat Server Log Files**

  ⚠ Remove only if no other application is using the Tomcat server.

  Remove the following log files:

  ```
  <DataDir>/log/tomcat/ovtomcatb.out
  ```

- **Installation Log Files**

  Remove the following log files:

  — *UNIX*

  ```
  /var/tmp/HPDma_<version>_HPOvInstaller.txt
  ```

  ```
  /var/tmp/HPOvInstaller/HPDma_<version>/*
  ```

  — *Windows*

  ```
  <drive>:\Documents and Settings\Administrator\
  Local Settings\Temp\HPOvInstaller\HPDma_<version>
  ```

Cleaning Up UCMDB or BAC

To clean up your UCMDB or BAC system, follow these steps:

1 Open the Package Manager:

- *UCMDB*

  Admin → Settings → Package Manager

- *BAC*

  Admin → Universal CMDB → Settings → Package Manager

2 If originally deployed, undeploy the optional synchronization packages:

- `hpdmadb.zip` for databases
- `hpdmaEUM.zip` for HP BAC End User Monitors
- `hpdmaos.zip` for operating system
- `hpdmasamples.zip` for the My Company Sample
- `hpom.zip` for the Discovery Pattern for HPOM

3 Remove all instances of the CI type `Service Group` from UCMDB:

a Open the IT Universe Manager:

- *UCMDB*

  Admin → Settings → IT Universe Manager

- *BAC*

  Admin → Universal CMDB → IT Universe Manager

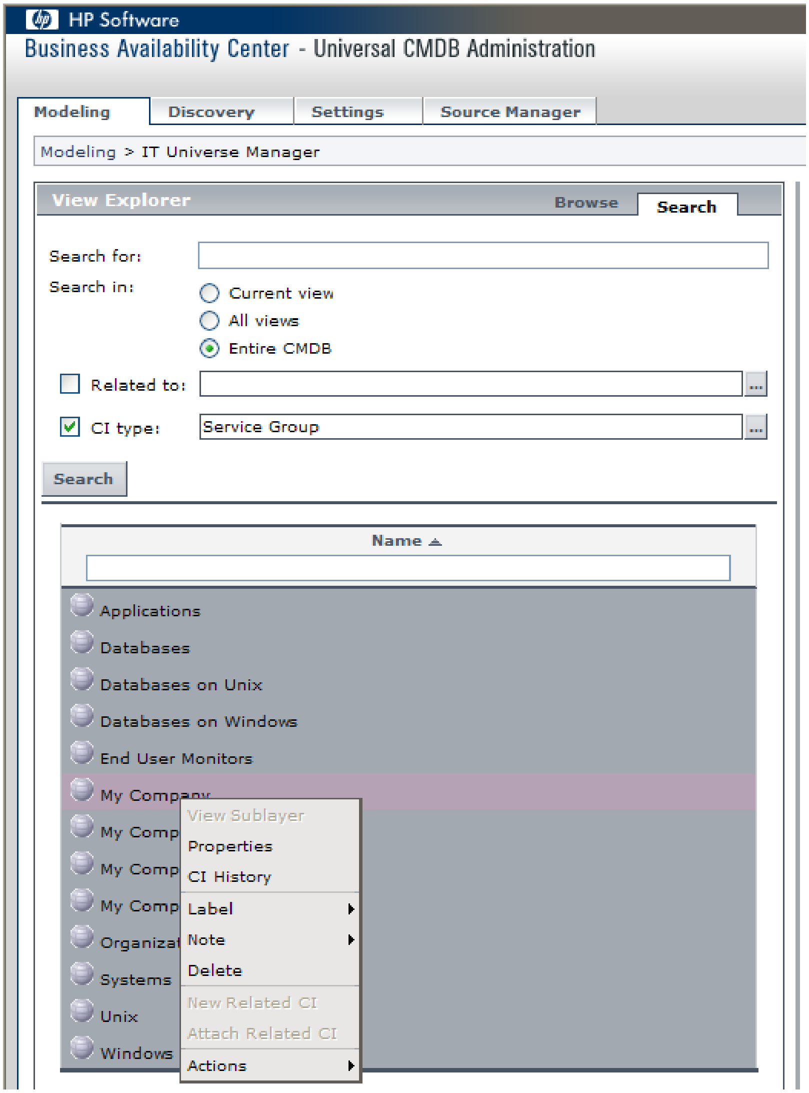
b Search for **CI type:** **`Service Group`**.

Service Group is found under **Business**.

c Select all returned items.

d Right-click to open the shortcut menu.

e Select **Delete**.



HP Software
Business Availability Center - Universal CMDB Administration
Modeling
Discovery
Settings
Source Manager
Modeling > IT Universe Manager
View Explorer
Browse
Search

Search for:

Search in:
○ Current view
○ All views
● Entire CMDB

□ Related to:

☑ CI type: Service Group

4 Delete all TQL queries, views, and enrichments that are related to the CI type `Service Group`. This includes any user-created TQL queries, views, and enrichments.

The `hpdmacore.zip` package can only be undeployed if all references in the TQL queries are removed.

5 Undeploy the `hpdmacore.zip` package.

6 Delete the `hpdmacore.zip` package and, if originally deployed, the any other optional package files.

Cleaning Up HPOM for UNIX

Execute this procedure only if you no longer have HPOM DMA synchronized nodes and services in HPOM or if you have moved required nodes to alternative node groups.

To delete the nodes and services that have been imported by HPOM DMA, follow these steps:

1 Delete the CMDB root service and all its children.

2 Delete all nodes in the `CMDB` node group:

a Open the `CMDB` node group:

Window → Node Group Bank → CMDB

b Select all nodes, right-click the selected collection of nodes, and select **Delete**.

3 Delete all nodes in the CMDB_removed node group:

a Open the CMDB_removed node group:

Window → Node Group Bank → CMDB_removed

b Select all nodes, right-click the selected collection of nodes, and select **Delete**.

4 From the HPOM Node Group Bank, delete the CMDB and CMDB_removed node groups:

Window → Node Group Bank

Right-click the `CMDB` and `CMDB_removed` node groups and select **Delete**.

5 Delete the service type definitions.

6 Unassign templates:

   a In the Node Bank window, select the HPOM management server node.

   b Open the Define Configuration window:

      Actions → **Agents** → **Assign Templates**

   c Select the **Group OM DMA** template and click **Remove selected**.

   d Click **OK**.

7 Undeploy policies or templates.

   To undeploy the `OM DMA` template group from the agent on the HPOM management server node, from HPOM UI, follow these steps:

   a In the Node Bank window, select the HPOM management server node.

   b Open the Install & Update Software and Configuration window:

      Actions → **Agents** → **Install & Update Software and Config**

   c Make sure that the HPOM management server node appears in the Target Nodes list.

   d Check **Templates** in the Components pane.

   e Click **OK** to remove the deployed `OM DMA` template.

Cleaning Up HPOM for Windows

Execute this procedure only if you no longer have HPOM DMA synchronized nodes and services in HPOM or if you have moved required nodes to alternative node groups.

Deleting Imported Services

To delete the services that have been imported by HPOM DMA, follow these steps:

1 Open the Configure Services window:

   a Right-click **Services** to open the shortcut menu.

   b **Configure** → **Services**

2. Delete the CMDB service as follows:

   Right-click the **CMDB** service and select **Delete** and **Yes**.

   Click **OK** in the Configure Services window.

Removing the OM DMA Policy Group

To remove the OM DMA policy group from the agent on the HPOM management server node, from HPOM UI, follow these steps:

1. Go to the OM DMA policy group:

   Policy management → **Policy groups** → **OM DMA**

2. Right-click the **OM DMA** policy group and select **Delete** and **Yes**.

Deleting HPOM DMA Node Groups

If you want to delete the HPOM DMA node groups, follow these steps:

1. Verify that any nodes that have been imported by HPOM DMA and that you want to continue to manage are moved to alternative node groups.
2. Delete the CMDB and CMDB_removed node groups and any nodes that are no longer required.

Uninstalling the UI Launch

To uninstall the UI Launch web application, remove the following directory from your UCMDB or BAC system:

<BAC/UCMDB-install-dir>/AppServer/webapps/uilaunch.war

Removing UI Launch Tools and Applications

If you originally installed and configured UI Launch, you can remove the following tools and applications:

- Show Correlated CI Map
- Show Change Report
- Show Neighborhood Map

- Show Triage Report (BAC only)
- Show End User Monitors (BAC only)
- Show Service Impact (BAC only)

Removing UI Launch Applications from HPOM for UNIX

To remove the UI Launch applications, follow these steps:

1. Open the HPOM for UNIX Application Bank.
2. Select the appropriate Application Group:
   - **Universal CMDB**
   - **Business Availability Center**
3. Click **Delete**.

Removing UI Launch Tools from HPOM for Windows

To remove the UI Launch tools, follow these steps:

1. Open the Configure Tools window:
   a. Right-click **Tools** to open the shortcut menu.

   b. **Configure → Tools**
2. Delete the `Business Availability Center` or `Universal CMDB` tool group as follows:
   a. Right-click the tool group you want to remove and select **Delete,** and **Yes**.

   b. Click **OK** in the Configure Tools window.

Unconfiguring Smart Message Mapping

To unconfigure Smart Message Mapping, disable Server-based Message Stream Interface (Server MSI), if no other product is using MSI, by completing the following steps:

1. From the Node Bank, open the **Server Configuration** dialog box:

   Actions → Server → Configure

2 In the Configure Server dialog box, clear the following options:

- **Divert Messages**
- **Send all messages to server MSI**
- **Enable Output**

3 Click **OK**.

Resetting the Discovery Source to SPI Discovery

Resetting the discovery source requires you to complete one of the following tasks, appropriate for the operating system of the host system:

- Resetting the Discovery on HPOM for UNIX on page 202
- Resetting the Discovery on HPOM for Windows Using the GUI on page 203
- Resetting the Discovery on HPOM for Windows Using XPL on page 203

Resetting the Discovery on HPOM for UNIX

To reset discovery from a SPI, follow these steps:

1 Open the **Application Bank** → ***<A_Group>*** → <***A_Discovery Group>*** → ***<A_Discovery Application>***

Example:

Application Bank → **UNIX OS SPI Group** → **OS SPI Discovery Group** → **OS SPI Discovery Application**

2 Right-click the application and select **Modify** from the drop-down menu.

3 In the Application Call statement, replace the call with the following call:

```
/opt/OV/SPISvcDisc/bin/SPI_DiscServ.sh -v -f /opt/OV/lib/
osspi/UnixOSSPI_Disc.conf -n "$OPC_NODES"
```

4 In the Additional Parameters field, remove the parameter:

```
-u false
```

5 Click **OK**.

6 Delete the service tree generated from the UCMDB discovery.

Resetting the Discovery on HPOM for Windows Using the GUI

To reset discovery from a SPI, for example, with messages that start with the strings `OSSPI:`, follow these steps:

1 From the HPOM for Windows UI, go to:

Tools → HP Operations Tools → Disable SPI Discovery

2 Double-click the **Disable SPI Discovery** tool.

The Tool Status window and the Exclude Service Prefixes windows are opened.

3 In the Exclude Service Prefixes window, add the required statements. In the example, this is: **`OSSPI:`**

> If you are deleting statements, make sure that you delete the comma between the unwanted statements and the next one.

4 Click **OK**.

> If you select **Cancel**, a confirmation window opens with two portions.
>
> - **OK** - All filter statements are deleted.
> - **No** - Original filter statements are retained.

5 Delete the OSSPI service tree generated from the UCMDB discovery.

The XPL configuration can also be modified with the XPL configuration tools. For adding the filters to the configuration, use the `ovconfchg` command as described in Resetting the Discovery on HPOM for Windows Using XPL.

Resetting the Discovery on HPOM for Windows Using XPL

To enable discovery from a SPI with messages that start with the string `OSSPI:`, follow these steps:

1 Execute the following command:

```
ovconfchg -edit
```

The configuration file opens in an editor, for example, Notepad.

2 In the editor window, remove the `OSSPI:` from the following statement:

```
[DiscoveryServiceFilter]
Excludes=OSSPI:
```

3 Save the changes.

4 Delete the OSSPI service tree generated from the UCMDB discovery.

Cleaning Up BPM Integration

Cleaning up the BPM Integration requires you to complete the following tasks:

- Deleting CI Status Alerts on page 204
- Deleting Performance Limit Alerts on page 204

Deleting CI Status Alerts

To delete CI Status Alerts follow these steps in the BAC UI:

1 Open the CI Status Alerts tab:

Admin → **Alerts** → **CI Status Alerts**

2 Select the End User Monitors view.

3 Delete the CI Alerts that you no longer need.

Deleting Performance Limit Alerts

To delete Alerts on performance limits follow these steps in the BAC UI:

1 Open the Event Based Alerts Configuration page:

Admin → **Alerts** → **Event Based Alerts** → **Event Based Alerts Configuration**

2 Select a business process profile from the **Profile:** drop-down list.

3 Delete the Event Based Alerts that you no longer need.

14 Performance and Configuration Tips

When synchronizing CI data from UCMDB or BAC to HPOM using HPOM, the following performance can be expected:

- **UNIX**

  One percent change in 10,000 originally synchronized CIs (100 nodes with 100 services per node) requires approximately 3 minutes.

- **Windows**

  One percent change in 10,000 originally synchronized CIs (100 nodes with 100 services per node) requires approximately 10 minutes.

The time necessary to add a new node depends on the available hardware and operating system information. If the information is provided by UCMDB, or if the node is accessible over the network, only a few seconds are needed. If the information is missing and the node is not reachable for a lookup, it can take 30 seconds depending on the network environment. When adding nodes, make sure that nodes are reachable. If nodes are shut down overnight, and information is not available from within UCMDB, reschedule adding nodes to a time when the majority of nodes are running.

➤ Initial synchronization from UCMDB or BAC may take longer, especially on Windows installations. Initial synchronization of 10,000 CIs on the specified Windows reference system requires approximately 210 minutes.

These values have been achieved using multi-processor server systems. However, HPOM DMA requires only one processor.

- *UNIX:*
  HP ia64 Server rx2600 with 2 x Intel Itanium 2, 1300 MHz CPUs, 2 GB RAM running the HP-UX B.11.23 U operating system.

- *Windows:*
  Intel Xeon Prestonia Server with 2 x 3.2 GHz CPUs, 4 GB RAM, running the Microsoft Windows Server 2003 R2 Enterprise Edition Service Pack 1 operating system.

To help minimize performance issues, you must create efficient mapping rules. See the *Mapping Basics* chapter in the *HPOM DMA Extensibility Guide* for guidance on how to write mapping rules correctly.

Increasing Tomcat Server Memory

Synchronizing bigger hierarchies consumes a lot of memory during synchronization. If the log file contains `OutOfMemoryException` entries, increase the heap size. To prevent memory exceptions and native library errors, increase the maximum heap size of the Tomcat server:

To increase the heap size, follow these steps:

1. Stop the Tomcat server using the command:

   ```
   ovc -stop ovtomcatB
   ```

2. Change the heap size with the following command:

   ```
   ovtomcatbctl -setmaxheapsize <size of heap>
   ```

3. Restart the Tomcat server using the commands:

   ```
   ovc -start ovtomcatB
   ```

If the heap size is already near the maximum (for example, on a system with 4GB RAM, the heap size is set to 3.5GB heap per process), decrease the chunk size. For detailed instructions, see Changing the Chunk Size on page 207.

Changing the Chunk Size

If a web service call returns a very large number of UCMDB objects, the result may be delivered in chunks. Small chunk sizes can lead to timeout problems. Large chunk sizes make higher demands on memory. The maximum number of objects contained in each chunk can be configured in UCMDB or BAC.

Changing the Chunk Size in UCMDB

To change the chunk size used by UCMDB, follow these steps:

1. Edit the file:

   `<UCMDBInstallDir>\UCMDBServer\j2f\conf\settings\ucmdbwsAPI.xml`

2. Set desired chunk size value in the following line:

   ```
   <value type="number"></value>
   ```

   Default: 500

3. Restart UCMDB Server:

   a. In the start menu, select **Stop UCMDB Server**.

   b. Select **Start UCMDB Server**.

Changing the Chunk Size in BAC

To change the chunk size used by the BAC, follow these steps:

1. Open the `<UCMDBInstallDir>\conf\settings\ucmdbwsAPI.xml` file.

2. Set desired chunk size value in the following line:

   ```
   <value type="number"></value>
   ```

   Default: 500

3. Stop and restart the BAC Server:

   a. **Start** → **All Programs** → **HP Business Availability Center** → **Disable Business Availability Center**

   b. **Start** → **All Programs** → **HP Business Availability Center** → **Enable Business Availability Center**

Adding Missing Node Attribute

Make sure that the nodes imported from UCMDB or BAC are fully described using the following attributes:

- System type (for example, Alpha, and Itanium)
- OS type (for example, HP-UX, Solaris, and Windows)
- OS version (for example, B.11.11, and B.11.22)

This ensures that nodes can be brought under management as quickly as possible. If some of this information is missing, HPOM for Windows initiates a discovery to establish the missing values, which takes additional time.

Missing attributes are likely to be a problem of UCMDB or BAC discovery setup. Make sure those attributes are specified to be discovered by UCMDB or BAC and mapped appropriately by HPOM DMA.

Changing XPL Configuration Parameters

Some XPL configuration parameters have an influence on performance and resource consumption. The parameters of interest are stored in the XPL Configuration under the resource group `server` and the name space `dma`.

To view the current settings, execute the command:

```
ovconfget -ovrg server dma
```

Web Service Client

If log files show timeouts, increase the appropriate timeout setting, for example, `operation.timeout` or `enumeration.context.timeout`.

The client implementation uses the following parameters. These parameters can be changed with the command:

```
ovconfchg -ovrg server -ns wsman.client -set <parameter>
<value>
```

operation.timeout

Maximum permitted duration for one Web Service Operation (default is 5 minutes and the value is specified in milliseconds).

enumeration.context.timeout

Maximum permitted duration for a complete enumeration (enumerate, pull, release). This is a suggestion from the client and could be overwritten by the server (default is 10 minutes and the value is specified in milliseconds).

bulkcreate.chunksize

Maximum number of items to be sent in one chunk during a bulk create. Increasing this parameter should lead to better performance, but significantly increases memory consumption (default is 1000).

enumeration.chunksize

Maximum number of items to be retrieved in one chunk during an enumeration. Increasing this parameter should lead to better performance, but significantly increases memory consumption (default is 1000).

ssl.keystore

File name of the keystorage where SSL certificates are stored. Only used for SSL default:

```
${OV_DATA}/shared/certificates/wsman/client.keystore
```

The following are examples of how to change these parameter values:

```
# ovconfchg -ovrg server -ns wsman.client -set
operation.timeout 300000
```

```
# ovconfchg -ovrg server -ns wsman.client -set
enumeration.context.timeout 600000
```

```
# ovconfchg -ovrg server -ns wsman.client -set
bulkcreate.chunksize 1000
```

```
# ovconfchg -ovrg server -ns wsman.client -set
enumeration.chunksize 1000
```

```
# ovconfchg -ovrg server -ns wsman.client -set ssl.keystore
${OV_DATA}/shared/certificates/client.keystore
```

Changing Non-XPL Configuration Parameters

Some non-XPL configuration parameters that have an influence on performance and resource consumption.

HPOM for Windows Web Services

The maximum message size that the HPOM for Windows Web Service Server accepts can be configured in the file:

`<InstallDir>\www\webapps\omws\web.config`

The default maximum size is set to 50MB. If you want to change the maximum message size, in the `MyServiceBinding` binding, change the values of the following parameters as required:

- `maxReceivedMessageSize`
- `maxBufferSize`

➤ The value of `maxBufferSize` must be equal to or greater than the value of `maxReceivedMessageSize`.

Example:

```
<system.serviceModel>
  <bindings>
    <customBinding>
      <binding name="MyServiceBinding">
        <textMessageEncoding messageVersion="Soap12WSAddressingAugust2004" />
         <httpTransport authenticationScheme="Basic"
                maxReceivedMessageSize="52428800" maxBufferSize="52428800" />
      </binding>
```

Tomcat Server

Configurable parameters of the Tomcat server are configured using the `ovtomcatbctl` CLI. Help is available with `ovtomcatbctl -h` command.

OVTomcatB Control Script Usage is listed in Table 3.

Table 3 OVTomcatB Control Script Usage

Option	Parameter
`-adduri`	*[-allowlinking] <webapp_name> <webapp_path> <webapp_description> <webapp_workdir>*
`-disablehttp`	—
`-disablehttps`	—
`-checkport`	*<portnumber>*
`-configure`	—
`-enablehttp`	—
`-enablehttps`	—
`-getconf`	—
`-help`	*N/A*
`-removeuri`	*<webapp name>*
`-restart`	—
`-sethttpport`	*<portnumber>*
`-sethttpsport`	*<portnumber>*
`-setshutdownport`	*<portnumber>*
`-start`	—
`-status`	—
`-stop`	—
`-version`	—
`-setiniheapsize`	*<size of heap>*
`-setmaxheapsize`	*<size of heap>*

Changing the HPOM Web Service Credentials

After a synchronization is specified, the credentials for the HPOM Web Service interface are cached. Changing the credentials in the HPOM DMA console (Connections page) has no effect unless Tomcat is restarted.

To change the current credentials, follow these steps:

1. Change the credentials on the HPOM server.
2. Change the credentials on the HPOM DMA console.
3. Stop and start the Tomcat server:

```
ovc -stop ovtomcatB
ovc -start ovtomcatB
```

Changing Log File Parameters

Logging can be controlled by adjusting the XPL parameters. Use the XPL utility **`ovconfchg -edit`** to set any of the following parameters. After setting the XPL configuration, you must restart the appropriate application, for example, `dmamsg` or `tomcat`.

➤ The level parameter only affects HPOM DMA log files. It does not have any affect on the XPL system log file.

Table 4

Parameter Name	Parameter Namespace	Default	Location and Name
`filecount`	`xpl.log.OvLogFileHandler`	10	Specifies the maximum number of log files to maintain in the log file history.
`filesize`	`xpl.log.OvLogFileHandler`	1	Specifies the maximum number of megabytes a log file may contain before a switch-log is done.
`level`	`xpl.log.OvLogFileHandler`	INFO	Specifies the logging level of the `OvLogFileHandler`. Possible values are any of those supported by the Java logging facility. The levels in descending order are SEVERE, WARNING, INFO, CONFIG, FINE, FINER, and FINEST. Each level enables all logs made at its level and those above it. For example, level INFO includes all SEVERE, WARNING, and INFO logs. In addition there is a level OFF that can be used to turn off logging, and a level ALL that can be used to enable logging of all messages.

Smart Message Mapping

Troubleshooting Smart Message Mapping includes the following guides:

- Messages Mapped to Wrong Nodes on page 214
- No Messages are Mapped on page 214
- Changing Service IDs on page 215

Messages Mapped to Wrong Nodes

If messages are being mapped to the wrong node, send a test message with a dedicated service ID and node for the target service:

```
opcmsg a=“app” o=“obj” severity=“warning”
service_id=“<key1>:<key2>:…@@<your node>” msg_t=“test”
```

Make sure that the values for `key1`, `key2`, ... are attribute values of the target service.

If another service is still being colored, check if that service also has the same set of keys.

No Messages are Mapped

Check that messages are being sent:

1. Disable MSI and send message to server.

   Message should be visible in the message browser. If not, the problem is not related to HPOM DMA.

2. Check that Smart Message Mapping and HPOM web server is running.
3. Check that server side MSI is activated.
4. Restart Smart Message Mapping:

   a. Open command line and execute:

   ```
   ovc -stop dmamsg
   ovc -start dmamsg
   ```

b. Look into the HPOM web service log files and check that Smart Message Mapping has resynchronized services:

```
Nov 28, 2007 8:45:33
AM;28;10;com.hp.ov.om.dma.smart.HpOmMessageMapper;init;co
m.hp.ov.om.dma.smart;INFO;**** OM DMA Smart Message
Mapping logging initialized ****Nov 28, 2007 8:45:33
AM;33;11;com.hp.ov.om.dma.smart.MessageRouter;sync;com.hp
.ov.om.dma.smart;INFO;Resynchronizing services.Nov 28,
2007 8:54:00
AM;2807;11;com.hp.ov.om.dma.smart.MessageRouter;sync;com.
hp.ov.om.dma.smart;INFO;Resynchronizing services done.
```

5. Send a test message and make sure that target node is set.

6. Check that services have a hosted on attribute set. Follow the steps in the Enrichment Simulator. Verify that the enriched data have the hosted on set correctly.

Changing Service IDs

If the Service ID directly maps to an existing service ID in the service tree, HPOM DMA does not change the service ID. To enable Smart Message Mapping to change the service ID, remove the SPI service tree.

Analyzing Synchronization Error Messages

The following errors can be identified by messages in the HPOM DMA log file:

- **TQL Not Found**

  TQL queries are either not installed or not accessible in UCMDB.

- **Service Type Definition Missing in HPOM**

  Either STDs have not been uploaded to HPOM, or a new type of object has been returned by the TQL queries in UCMDB.

- **CI could not be Saved due to Invalid Attribute Value**

  Some characters, such as `\`, are not allowed for certain attribute types. The error message identifies the object and attribute. The character must be mapped in the attribute mapping.

- **Service or Node Already Exists**

  A TQL query returns the same service or node multiple times because different discovery sources have added the same object to UCMDB (for example, `testnode.example.com` and `TESTNODE`). The query must be adapted or the data in UCMDB must be rationalized.

Analyzing LDAP Configuration Errors

The following are common LDAP problems:

- **Unreachable LDAP Server**

  The LDAP server is not reachable from the host, and the port number or the protocol prefix do not match.

  Defaults (RFC): `ldap + 389`, `ldaps + 636`

- **Specify Correct Branches**

  Correct branches for user accounts and groups must be specified:

  — Do not use white-space characters surrounding group names.

  — Multiple group names must be separated by a semicolon (`;`).

  — HPOM DMA uses the group `SONATA-USER` internally for users authenticating using the local users store.

Analyzing UCMDB Web Service with SoapUI

You can use a generic SOAP client to examine the data transmitted by UCMDB independent of HPOM DMA. It can be used to simulate the HPOM DMA access.

Use a generic SOAP client when:

- A data dump does not help. You suspect that the problem occurs between UCMDB and the normalized dump.
- You want a detailed analysis of the TQL results as transmitted using the Web Service.

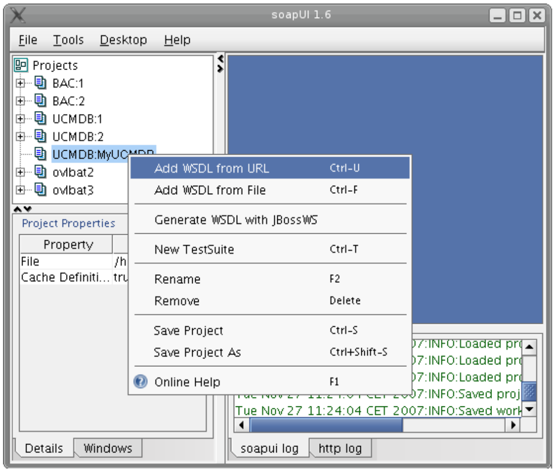
SoapUI is a free generic SOAP client from Eviware. Go to the following web site and download the latest version:

http://www.soapui.org

To use SoapUI to examine the data transmitted by UCMDB:

1 Start the SoapUI application and select UCMDB system from which your data is being sent.

2 From the **File** menu, select **New WSDL Project** and create a project for your UCMDB system.



```
07:INFO:Loaded pro
07:INFO:Loaded pro
07:INFO:Loaded pro
07:INFO:Saved proj
Tue Nov 27 11:24:04 CET 2007:INFO:Saved work
```

3 From the shortcut menu, select **Add WSDL from URL**.

4 Enter the URL from the HPOM DMA Connection page and append **?wsdl** to it. For example:

```
http://MyUCMDB.example.com:8080/axis2/services/
UcmdbService?wsdl
```

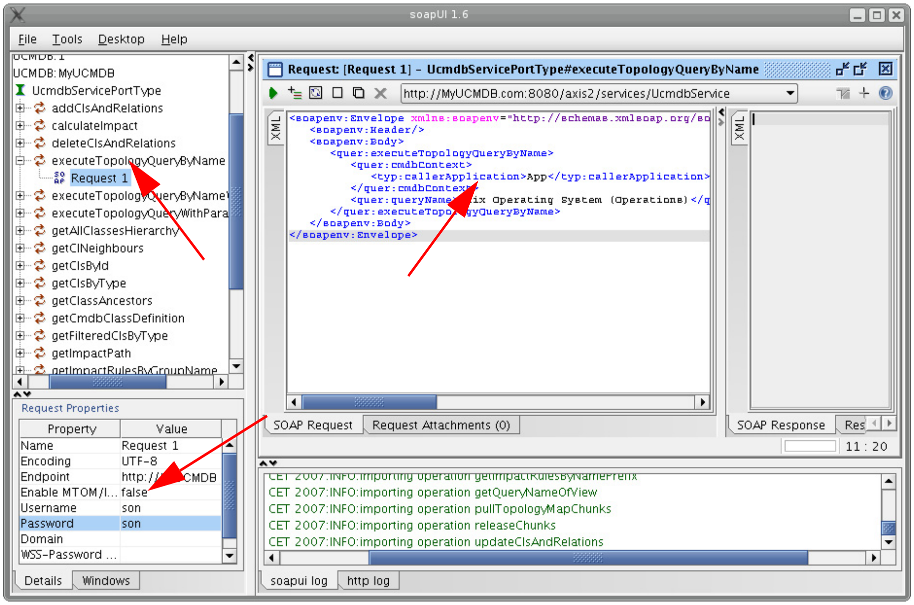
The SoapUI creates default requests for all operations.

5 Prepare a request in SoapUI as follows:

a Open the request for `executeTopologyQueryByName`.

b Enter user name and password.

c Enter any value for `callerApplication` and the name of the TQL query into the request.



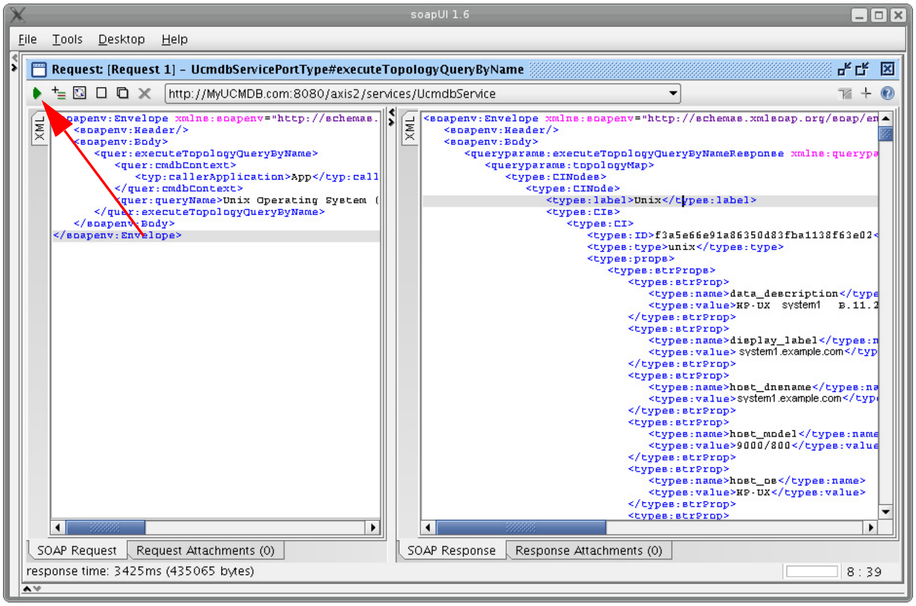
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/so
   <soapenv:Header/>
   <soapenv:Body>
      <quer:executeTopologyQueryByName>
         <quer:cmdbContext>
            <typ:callerApplication>App</typ:callerApplication>
         </quer:cmdbContext>
         <quer:queryName>Unix Operating System (Operations)</q
      </quer:executeTopologyQueryByName>
   </soapenv:Body>
</soapenv:Envelope>
```

Request Properties

Property	Value
Name	Request 1
Encoding	UTF-8
Endpoint	http://UCMDB
Enable MTOM/I...	false
Username	son
Password	son
Domain	
WSS-Password ...	

```
CET 2007:INFO:importing operation getImpactRulesByNamePrefix
CET 2007:INFO:importing operation getQueryNameOfView
CET 2007:INFO:importing operation pullTopologyMapChunks
CET 2007:INFO:importing operation releaseChunks
CET 2007:INFO:importing operation updateClsAndRelations
```

6 Execute a request in SoapUI by clicking the execute icon (green arrow).



soapUI 1.6
File
Tools
Desktop
Help
Request: [Request 1] – UcmdbServicePortType#executeTopologyQueryByName
http://MyUCMDB.com:8080/axis2/services/UcmdbService
XML
XML
SOAP Request
Request Attachments (0)
SOAP Response
Response Attachments (0)
8 : 39

```
<soapenv:Envelope xmlns:soapenv="http://schemas.
   <soapenv:Header/>
   <soapenv:Body>
      <quer:executeTopologyQueryByName>
         <quer:cmdbContext>
            <typ:callerApplication>App</typ:call
         </quer:cmdbContext>
         <quer:queryName>Unix Operating System (
      </quer:executeTopologyQueryByName>
   </soapenv:Body>
</soapenv:Envelope>
```

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/en
   <soapenv:Header/>
   <soapenv:Body>
      <queryparams:executeTopologyQueryByNameResponse xmlns:querypa
         <queryparams:topologyMap>
            <types:CINodes>
               <types:CINode>
                  <types:label>Unix</types:label>
                  <types:CIs>
                     <types:CI>
                        <types:ID>f3a5e66e91a86350d83fba1138f63e02<
                        <types:type>unix</types:type>
                        <types:props>
                           <types:strProps>
                              <types:strProp>
                                 <types:name>data_description</type
                                 <types:value>HP-UX  system1   B.11.2
                              </types:strProp>
                              <types:strProp>
                                 <types:name>display_label</types:n
                                 <types:value> system1.example.com</typ
                              </types:strProp>
                              <types:strProp>
                                 <types:name>host_dnsname</types:na
                                 <types:value>system1.example.com</typ
                              </types:strProp>
                              <types:strProp>
                                 <types:name>host_model</types:name
                                 <types:value>9000/800</types:value
                              </types:strProp>
                              <types:strProp>
                                 <types:name>host_os</types:name>
                                 <types:value>HP-UX</types:value>
                              </types:strProp>
                              <types:strProp>
```

response time: 3425ms (435065 bytes)

The right pane displays the RAW result.

➤ If the result is chunked, use `pullTopologyMapChunks` to retrieve them.

A HPOM DMA Reference Information

This chapter describes the standard HPOM DMA installation. The following information is available:

- Installation Locations on page 221
- Configuration Files on page 223
- Log Files on page 226
- Standard Synchronization Package Locations on page 230
- Objects Installed on HPOM on page 227
- HPOM DMA Default Synchronization Package and other standard synchronization packages on page 232.

Installation Locations

The HPOM DMA installation installs the files in the following locations:

- *UNIX*
  - ***<InstallDir>***

    `/opt/OV/`
  - ***<DataDir>***

    `/var/opt/OV/`
  - ***<SharedDir>***

    `/var/opt/OV/shared/server`

- *Windows*
  - ***<InstallDir>***

    Default:
    `C:\Program Files\HP\HP BTO Software`
  - ***<DataDir>***

    Default:
    `C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software`
  - ***<SharedDir>***

    Default:
    `C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\server`

Configuration Files

All HPOM DMA configuration files are stored in:

<SharedDir>/conf/dma

These files are used during run time and can be changed by users.

The initial configuration files are available (unchanged) for backup purposes, in:

<InstallDir>/newconfig/DataDir/conf/dma

Table 5 Configuration Files and Descriptions

Location and Name	Purpose
<SharedDir>/conf/dma	
DefaultSyncTask.settings	Contains the information that can be accessed through the Connection and Configuration web page.
schedule.xml	Specifies when a synchronization should be triggered. This information can be accessed from the Schedule web page.
nodetypes.xml	Defines which UCMDB CI types are imported as nodes into the HPOM node groups. For each rule that matches, the node is also added to the all node groups defined in the rule. For details, see the *HPOM DMA Extensibility Guide*.
containmentrelations.xml	Contains a list of regular expressions. All UCMDB relation type names that match this regular expression become a containment relation when the relation is synchronized into the Service Navigator using DMA. For details, see the *HPOM DMA Extensibility Guide*.

Table 5 Configuration Files and Descriptions

Location and Name	Purpose
`users.properties`	Contains the HPOM DMA console users' information written by the `dmauser` tool.
`ldap.properties`	Contains the configuration information required by LDAP authentication.
`MachineTypes.xml`	Contains all currently installed HPOM machine types (UNIX only).
`MachineTypes_template.xml`	Contains list of currently supported machine types (UNIX only).
`sync-packages`	Contains a subdirectory for each synchronization package. Each synchronization package contains several configuration files. For details, see the *HPOM DMA Extensibility Guide*.
<*SharedDir*>/conf/dma/sync-packages/<syncPackage>/ See Standard Synchronization Package Locations on page 230 for a description of the files installed with HPOM DMA. Detailed information about synchronization packages is available in the *HPOM DMA Extensibility Guide*.	
`bundle.xml`	Contains general information about this synchronization package, including name, description, priority and UCMDB TQL queries used. This file cannot be accessed through HPOM DMA web console.
`nodemapping.xml`	Contains the rules for the node group mapping.
`servicemapping.xml`	Contains the rules for the Service Type Definition mapping.
`attributemapping.xml`	Contains the rules for attribute enrichment.
`usermapping.xml`	Contains the rules for the User Profile mapping.

Table 5 Configuration Files and Descriptions

Location and Name	Purpose
preUpload.groovy	Contains the script to be executed after syncronization.
postUpload.groovy	Contains the script to be executed after syncronization.
• **UCMDB** ***<UCMDB-Install-Dir>*\j2f\AppServer\webapps\hpdma-uilaunch.war** • **BAC** ***<BAC-Install-Dir>*\AppServer\webapps\hpdma-uilaunch.war**	
ucmdbWebService.properties	This properties file is used by the UI Launch redirect generator script and is located on the UCMDB or BAC system. It contains the URL, user name and password for both the UCMDB web service and the UCMDB or BAC UI launch.

Log Files

The HPOM DMA log files are listed in Table 6. For information how to configure HPOM DMA log files, see Changing Log File Parameters on page 213.

Table 6 HPOM DMA Log Files

Logging	Platform	Location and Name
Synchronization	All	`<SharedDir>/log/dma/sync.<*>.<locale>` Accessible from the HPOM DMA console
HPOM for UNIX Web Service	UNIX	`<SharedDir>/log/om/ciws.<*>.<locale>`

HPOM for Windows Web Service	Windows	`<SharedDir>\log\om\ws.trace.txt`
		`http://<host>/omws/trace.txt`

Smart Message Mapper	All	`<SharedDir>/log/dma/msgmap.<*>.<locale>`
HPOM DMA Web Console (CWC)	UNIX	`<DataDir>/tmp/cwc.log`
	Windows	`<drive>:\Windows\system32\cwc.log`
TomcatB	UNIX	`<DataDir>/log/tomcat/ovtomcatb.out`
	Windows	`<DataDir>/log/tomcat/stdout.log`
Default HPOM DMA Log File	All	`<SharedDir>/log/system.<#>.<locale>`

Installation	UNIX	`/var/tmp/HPDma_<version>_HPOvInstaller.txt`
		`/var/tmp/HPOvInstaller/HPDma_<version>/*`

	Windows	`C:\Documents and Settings\Administrator\Local Settings\Temp\HPOvInstaller\HPDma_<version>`

Objects Installed on HPOM

HPOM DMA installs the following objects for HPOM:

- Node Groups
- Root Service
- Propagation and Calculation Rules
- Service Type Definitions on page 228
- Policies and Templates on page 229

Node Groups

HPOM DMA includes two HPOM node groups that are automatically created during installation:

- `CMDB`
- `CMDB_Removed`

Root Service

HPOM DMA includes one HPOM root service that is automatically created during installation:

- `CMDB`

Propagation and Calculation Rules

HPOM DMA includes the following HPOM calculation and propagation rules:

- Calculation Rule: `ucmdb_generic_CR ("Most Critical")`
- Propagation Rule: `ucmdb_generic_PR ("Unchanged")`

Service Type Definitions

HPOM DMA includes the following HPOM Service Type Definitions and their associated GUID values:

- Informix (ucmdb_informix)
- NT (ucmdb_nt)
  - Cpu (ucmdb_cpu)
  - Disk (ucmdb_disk)
  - Drive (ucmdb_drive)
  - File system (ucmdb_filesystem)
  - Memory (ucmdb_memory)
  - Printer (ucmdb_printer)
  - Service (ucmdb_service)
  - SSH (ucmdb_ssh)
  - Windows OS User (ucmdb_winosuser)
- Oracle Windows (ucmdb_oracle_windows)
- Oracle UNIX (ucmdb_oracle_unix)
- SQLServer (ucmdb_)
- SQLServer 6.5 (ucmdb_sqlserver_65)
- Sybase (ucmdb__sqlserver)
- Unix (ucmdb_unix)
  - Logical Disk (ucmdb_logicaldisk)
  - OS User (ucmdb_osuser)
- Business Process Group (ucmdb_bp_group)
- Business Process Step (ucmdb_bp_step)
- BPM Transaction from Location (ucmdb_bp_tx_from_location)

Where appropriate, existing HPOM or SPIs tools are assigned to the HPOM DMA Service Type Definitions.

Policies and Templates

The HPOM DMA policies or templates are listed in Table 7. For information on how to assign and deploy these policies or templates, see Assigning the OM DMA Template Group on page 99 or Assigning and Deploying the OM DMA Policy Group on page 109.

➤ When monitoring HPOM DMA in cluster installations, policies and templates should be enabled on the active node and disabled on all inactive nodes.

For information about policy or template deployment in cluster installations, see the appropriate HPOM documentation:

- For HPOM for UNIX installed on a cluster, template assignments must be done on Virtual Nodes. For details, see the chapter entitled “Working with Virtual Nodes” in the *HTTPS Agent Concepts and Configuration Guide*.
- For HPOM for Windows installed on a cluster, policies must be controlled by the agent Application Package Manager (APM). For details, see the HPOM for Windows online help.

Table 7 HPOM DMA Policies and Templates

Name	Group	Description
HPOM DMA Synchronization log	OM DMA	Monitors failure of the HPOM DMA synchronization from UCMDB to HPOM.
HPOM DMA Smart Message Mapping log	OM DMA	Monitors the HPOM DMA synchronization log file from UCMDB to HPOM.
HPOM Web Service log	OM DMA	Monitors the HPOM Web Service log.
uCMDB missing Node	OM DMA	Monitors whether a node in UCMDB previously synchronized to HPOM is now missing from the current synchronization.

Standard Synchronization Package Locations

This section describes the directory and file structure of synchronization packages in the file system. Each of these synchronization package directories must contain a `bundle.xml` file. Some synchronization packages also include `servicemapping.xml`, `nodemapping.xml`, and `attributemapping.xml` files.

```
<SharedDir>/conf/dma/sync-packages/default
      attributemapping.xml
      bundle.xml
      servicemapping.xml

<SharedDir>/conf/dma/sync-packages/dmaInformix
      bundle.xml
      nodemapping.xml
      servicemapping.xml

<SharedDir>/conf/dma/sync-packages/dmaMSSQLServer
      bundle.xml
      nodemapping.xml
      servicemapping.xml

<SharedDir>/conf/dma/sync-packages/dmaOracle
      bundle.xml
      nodemapping.xml
      servicemapping.xml

<SharedDir>/conf/dma/sync-packages/dmaOS
      bundle.xml
      nodemapping.xml (UNIX only)

<SharedDir>/conf/dma/sync-packages/dmaSybase
      bundle.xml
      nodemapping.xml

<SharedDir>/conf/dma/sync-packages/dmaWinOS
      bundle.xml
      nodemapping.xml (UNIX only)

<SharedDir>/conf/dma/sync-packages/dmaScriptAutomaticPolicyDistribution
      bundle.xml
      postUpload.groovy (UNIX only)

<SharedDir>/conf/dma/sync-packages/dmaEUM
      bundle.xml

<SharedDir>/conf/dma/sync-packages/dmaMyCompany
      bundle.xml
```

```
<SharedDir>/conf/dma/sync-packages/dmaGroupHostResources
      bundle.xml
      preUpload.groovy
```

HPOM DMA Default Synchronization Package

The default synchronization package is deployed as part of the standard installation. It contains the default mappings to enable synchronization of nodes and services from UCMDB or BAC into HPOM.

Priority: `10` (LOW)

The default synchronization package is the package with the lowest priority in HPOM DMA. This package is taken only if no other mappings apply.

Service Mapping

By default, all services are assigned to the default service type definition in accordance with the following pattern: `ucmdb_`*`<CI Type>`*.

The service type definitions must exist in HPOM. For details on how to upload service type definitions, see the *HPOM DMA Extensibility Guide*.

Attribute Mapping

This section include information on attribute mappings used for the following elements:

- All CI Types on page 232
- SQLServer, Oracle, and Sybase Database CI Types on page 233
- Host, NT, and Unix CI Types on page 233

All CI Types

Required fields (must be selected in TQL query definition):

`display_label` (Display Label)

The default attribute mapping defines mapping for:

- `display_label`

  Example

  The display label for Oracle database is set to:

"[oracle] my_database on mynode.example.com"

Example

The display label for other types is set to:

"[disk] c:\"

The display label for nodes and service groups is not changed.

- CMDBCiCaption

  The UCMDB display label is not mapped, but rather manipulated for better readability and to achieve uniqueness. As a result, you also need to map the original UCMDB display label into a service attribute. This is needed for Smart Message Mapping.

SQLServer, Oracle, and Sybase Database CI Types

Required fields (must be selected in TQL query definition):

- database_dbtype (Type)
- database_dbversion (Version)
- display_label (Display Label)

Host, NT, and Unix CI Types

Required fields (must be selected in TQL query definition)

host_dnsname	(Host DNS Name)
host_os	(Host Operating System)
host_osversion	(Host Operating System Version)
host_model	(Host Model)
display_label	(Display Label)
data_description	(Description)

Keywords are required for Smart Message Mapping:

- Make sure that the content of attributes includes enough information, for example, caption.

- When identifying a host CI, make sure that the caption is identical to the host DNS name. This is used as a fallback by Smart Message Mapping when a message cannot be definitely mapped to a service.

The default attribute mapping defines mapping for:

- Hosted on relationship

  Without setting the `hosted_on` relationship, the Smart Message Mapping cannot work.

- `CmdbObjectID` and `CmdbCiType`.

  Required for UI launch tools/applications of synchronized services. `ID` is mapped to `CmdbObjectID` and `CiType` is mapped to `CmdbCiType`.

  These attributes are also added to the service.

The following standard mappings are included:

- AIX Attribute Mapping on page 235
- HP-UX Attribute Mapping on page 235
- Linux Attribute Mapping on page 235
- Solaris Attribute Mapping on page 236
- Windows Attribute Mapping on page 236
- Other Attribute Mapping on page 237

`ovo_systemType`, `ovo_osType` and `ovo_osVersion` are required to specify the appropriate machine type in HPOM.

➤ These are not all the possible mappings, as it is not possible to discover all combinations of HPOM for Windows requests with the standard discovery from UCMDB. If the appropriate mapping is not available, the HPOM for Windows discovery attempts to find the information.

AIX Attribute Mapping

Table 8 summarizes the default attribute mappings for AIX nodes.

Table 8 Attribute Mapping for AIX

UCMDB Attributes			HPOM Attributes		
CiType	**host_os**	**host_osversion**	**ovo_systemType**	**ovo_osType**	**ovo_osVersion**
unix	AIX	starts with 51	Power PC Family	AIX_32	5L 5.1
unix	AIX	starts with 52	Power PC Family	AIX_32	5L 5.2
unix	AIX	starts with 53	Power PC Family	AIX_32	5L 5.3

HP-UX Attribute Mapping

Table 9 summarizes the default attribute mappings for HP-UX nodes.

Table 9 Attribute Mapping for HP-UX

UCMDB Attributes				HPOM Attributes		
CiType	**host_os**	**host_model**	**description**	**ovo_systemType**	**ovo_osType**	**ovo_osVersion**
unix	HP-UX	ia64	contains B.11.22	Itanium Compatible	HP-UX_64	B.11.22
unix	HP-UX	ia64	contains B.11.23	Itanium Compatible	HP-UX_64	B.11.23
unix	HP-UX	ia64	contains B.11.31	Itanium Compatible	HP-UX_64	B.11.31
unix	HP-UX		contains B.10.20	Itanium Compatible	HP-UX_64	B.10.20
unix	HP-UX		contains B.11.00	Itanium Compatible	HP-UX_64	B.11.00
unix	HP-UX		contains B.11.11	Itanium Compatible	HP-UX_64	B.11.11
unix	HP-UX		contains B.11.23	Itanium Compatible	HP-UX_64	B.11.23
unix	HP-UX		contains B.11.31	Itanium Compatible	HP-UX_64	B.11.31

Linux Attribute Mapping

No mapping specified.

Solaris Attribute Mapping

Table 10 summarizes the default attribute mappings for Solaris nodes.

Table 10 Attribute Mapping for Solaris

UCMDB Attributes				HPOM Attributes		
CiType	**host_os**	**host_osversion**	**host_model**	**ovo_systemType**	**ovo_osType**	**ovo_osVersion**
unix	SunOS	2.6		SPARC Family	Solaris_32	2.6
unix	SunOS	5.7		SPARC Family	Solaris_32	7
unix	SunOS	5.8		SPARC Family	Solaris_32	8
unix	SunOS	5.9		SPARC Family	Solaris_32	9
unix	SunOS	5.10	sun4u	SPARC Family	Solaris_64	10
unix	SunOS	5.10	i86pc	x86/x64 Compatible	Solaris_64	10

Windows Attribute Mapping

Table 11 summarizes the default attribute mappings for Windows nodes.

Table 11 Attribute Mapping for Windows

UCMDB Attributes			HPOM Attributes		
CiType	**host_os**	**host_osversion**	**ovo_systemType**	**ovo_osType**	**ovo_osVersion**
nt	Windows	4.0	x86/x64 Compatible	Windows_32	NT (4.0)
nt	Windows	5.0	x86/x64 Compatible	Windows_32	2000 (5.0)
nt	Windows	5.1	x86/x64 Compatible	Windows_32	XP (5.1)
nt	Windows	5.2	x86/x64 Compatible	Windows_32	2003 (5.3)
nt	Windows	6.0	x86/x64 Compatible	Windows_32	Server 2008 (6.0)

Other Attribute Mapping

Table 12 summarizes the default attribute mappings for all nodes not specifically specified.

Table 12 Attribute Mapping for Other Platforms

UCMDB Attributes	HPOM Attributes		
	ovo_systemType	**ovo_osType**	**ovo_osVersion**
	n/a	n/a_0	n/a

UNIX OS Synchronization Package: dmaOS

The UNIX operating system synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of UNIX nodes from UCMDB or BAC into HPOM.

Priority: `8`

TQL query used: `Unix Operating System (Operations)`

Node Mapping

Table 13 specifies the node mappings for the UNIX operating system.

Table 13 UNIX Operating System Node Mappings

CI Type	host_os	Mapped to Node Group	
		Windows	UNIX
unix	HP-UX	—	OSSPI-HPUX
unix	Linux	—	OSSPI-Linux
unix	AIX	—	OSSPI-AIX
unix	SunOS	—	OSSPI-Solaris

➤ On HPOM for Windows, operating system node mapping is not needed as nodes are automatically mapped to product defined node groups based on the operating system. Any specified node mapping is ignored.

Windows OS Synchronization Package: dmaWinOS

The Windows operating system synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Windows nodes from UCMDB or BAC into HPOM.

Priority: `8`

TQL query used: `Windows Operating System (Operations)`

Node Mapping

Table 14 specifies the node mappings for the Windows operating system.

Table 14 UNIX Operating System Node Mappings

CI Type	host_os	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX
nt	not Linux	—	WINOSSPI-Windows

➤ On HPOM for Windows, operating system node mapping is not needed as nodes are automatically mapped to product defined node groups based on the operating system. Any specified node mapping is ignored.

Informix Synchronization Package: dmaInformix

The Informix database synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Informix nodes and services from UCMDB or BAC into HPOM.

Priority: `7`

TQL query used: `Informix (Operations)`

Service Mapping

Table 15 specifies the service mappings for the Informix database.

Table 15 Informix Database Service Mappings

CI Type	DB type	Mapped to Service Type Definition
database	informix	ucmdb_informix

Node Mapping

Table 16 specifies the node mappings for the Informix database.

Table 16 Informix Database Node Mappings

Host Server Type	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX
informix	DBSPI_Informix_Nodes	Informix

Microsoft SQL Server Synchronization Package: dmaMSSQLServer

The Microsoft SQL Server database synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Microsoft SQL Server nodes and services from UCMDB or BAC into HPOM.

Priority: `7`

TQL query used: `MS SQL Server (Operations)`

Service Mapping

Table 17 specifies the service mappings for the Microsoft SQL Server database.

Table 17 Microsoft SQL Server Database Service Mappings

CI Type	Database Version	Mapped to Service Type Definition
sqlserver	6.5	ucmdb_sqlserver65
sqlserver		ucmdb_sqlserver

Node Mapping

Table 16 specifies the node mappings for the Microsoft SQL Server database.

Table 18 Microsoft SQL Server Database Node Mappings

Host Server Type	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX
sqlserver	DBSPI_SQL_Server_ Nodes	MSSQL

Oracle Synchronization Package: dmaOracle

The Oracle database synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Oracle nodes and services from UCMDB or BAC into HPOM.

Priority: `7`

TQL query used: `Oracle (Operations)`

Service Mapping

Table 19 specifies the service mappings for the Oracle database.

Table 19 Oracle Database Service Mappings

Caption from Parent	CI Type	Mapped to Service Type Definition
Databases on Windows	oracle	ucmdb_oracle_nt
Database on Unix	oracle	ucmdb_oracle_unix

Node Mapping

Table 20 specifies the node mappings for the Informix Database.

Table 20 Oracle Database Node Mappings

CI Type	Host Server Type	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX
nt	oracle	DBSPI_Oracle_Windows_ Nodes	Oracle (NT)
unix	oracle	DBSPI_Oracle_Unix_ Nodes	Oracle (Unix)

Sybase Synchronization Package: dmaSybase

The Sybase database synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Sybase services from UCMDB or BAC into HPOM.

Priority: `7`

TQL query used: `Sybase (Operations)`

Node Mapping

Table 21 specifies the node mappings for the Sybase database.

Table 21 Sybase Database Node Mappings

Host Server Type	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX
sybase	DBSPI_Sybase_Nodes	Sybase

Group Multiple Host Resource Types Synchronization Package

The HPOM DMA "Script: Group Multiple Host Resource Types" synchronization package is deployed as part of the standard installation. It contains a pre-upload script that groups multiple instances of a resource type, for example disks, under an additional subgroup.

Priority: `8`

TQL query used: `None`

➤ This script requires STDs that are not delivered as part of the HPOM DMA product. It is recommended that Automatic STD Creation is activate. For details, see Creating Service Type Definitions Automatically on page 100 and page 106.

Trigger Policy Distribution Synchronization Package

➤ UNIX only.

The HPOM DMA "Script: Trigger Policy Distribution" synchronization package is deployed as part of the standard installation. It contains a post-upload script that triggers policy distribution.

Priority: `8`

TQL query used: `None`

My Company Synchronization Package: dmaMyCompany

The My Company synchronization package is deployed as part of the standard installation. It contains examples of TQL queries and enrichment rules to help you configure customized Service Navigator views in HPOM.

Priority: `8`

TQL query used: `My Company US (Operations)`
`My Company EMEA (Operations)`
`My Company ASIAPAC (Operations)`

End User Management Synchronization Package: dmaEUM

The End User Management synchronization package is deployed as part of the standard installation. It contains a TQL query and service type definitions to enable the display of End User Management views from BAC in HPOM.

Priority: `9`

TQL query used: `End User Monitors (Operations)`

HPOM DMA Configuration Parameters in XPL

Table 22 lists the XPL configuration parameters in the used by HPOM DMA.

Table 22 OV Resource Group: Server Configuration Parameters in XPL

Name Space	Name	Type	Default	Description
`HPDmaSync`	`FailedServicesToLog`	int	100	To reduce log output, only log the most likeliest root causes of a service synchronization failure. A value of 0 logs all errors.
`opc.WebService`	`EnumerationExpiration`	int	20	Duration for which the enumeration context is valid. Default is 20 minutes.
`opc.WebService`	`EnumerationExpiration Maximum`	int	60	Maximum duration for which the enumeration context is valid. If a client specifies a longer value, the service overrides the client's request with this value. Default is 60 minutes.
`opc.WebService`	`EventQueueSize`	int	1000	Maximum number of events that an event queue stores. When the event queue contains the maximum number of events, the service discards the oldest events from the queue as new events are added. Default is 1000 events.
`opc.WebService`	`MaxItemsMaximum`	int	500	Maximum number of items that the service allows for a pull operation. If the client specifies a larger value, it is ignored and this value is used. Default is 500 items.
`opc.WebService`	`SubscriptionExpiration`	int	60	Duration for which the subscription context is valid. Default is 60 minutes.

Table 22 OV Resource Group: Server Configuration Parameters in XPL

Name Space	Name	Type	Default	Description
opc.WebService	SubscriptionExpiration Maximum	int	1440	Duration for which the subscription context is valid. If a client specifies a longer value, the service overrides the client's request with this value. Default is 1440 minutes (one day).
opc.WebService. Configuration Item	NodeGroupCreation Enabled	Boolean	false	Indicates whether Node Group Creation for CI Nodes created within the Web Service is enabled or disabled. By default, this feature is disabled and the Node Groups are not created.
opc.WebService. Configuration Item	StdCreationEnabled	Boolean	false	Indicates whether STD Creation for CI Services created within the Web Service is enabled or disabled. By default, this feature is disabled and the STDs are not created.
opc.WebService. Configuration Item	UserProfileAssignment Enabled	Boolean	false	Indicates whether User Profile assignment for CI Services created within the Web Service is enabled or disabled. By default, this feature is disabled and the User Profile properties within the CI created by the Web Service are ignored.
wsman.client	bulkcreate.chunksize	int	1000	The maximum number of items the client sends in a chunked Bulk Create operation. Default is 1000.
wsman.client	enumeration.chunksize	int	1000	The maximum number of items the client requests in a pull operation. Default is 1000.

Table 22 OV Resource Group: Server Configuration Parameters in XPL

Name Space	Name	Type	Default	Description
wsman.client	enumeration.context.timeout	int	600000	EnumerationExpiration value in ms requested by the client. This is the duration that the enumeration context should be valid for. Default is 10 minutes.
wsman.client	operation.timeout	int	300000	Timeout for each operation requested by the client in ms. After this time the server sends a timeout fault. Default is 5 minutes.
wsman.client	ssl.keystore	String		Absolute path to the keystore file containing the SSL certificates (used by the LDAP authentication and for running DMA in secured mode.

Open Source Software

WisemanA, JAXB and JAX-WS Open Source Software (OSS) product source code is packaged with HPOM DMA. The OSS source code is located in the following location:

`<InstallDir>/nonOV/wiseman/a/src`

The OSS product packages used by HPOM DMA are as follows:

- jaxb-src.zip
- jaxws-src.zip
- wiseman_src.zip

Index

hp®

invent

Java™
COMPATIBLE