Closed Loop Incident Process (CLIP)

HP Universal CMDB – HP Business Availability Center – HP SiteScope –
HP Operations Manager for Windows – HP Operations Manager *i* –
HP Service Manager

for the Windows operating system

Software Version: 1.5

Deployment and Configuration Guide

Document Release Date: December 2009
Software Release Date: December 2009

SSG - Solution Services Group

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®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, and Windows® XP 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.

Acknowledgements

- This product includes software developed by Apache Software Foundation (http://www.apache.org/licenses).
- This product includes OpenLDAP code from OpenLDAP Foundation (http://www.openldap.org/foundation/).

- This product includes GNU code from Free Software Foundation, Inc. (http://www.fsf.org/).
- This product includes JiBX code from Dennis M. Sosnoski.
- This product includes the XPP3 XMLPull parser included in the distribution and used throughout JiBX, from Extreme! Lab, Indiana University.
- This product includes the Office Look and Feels License from Robert Futrell (http://sourceforge.net/projects/officelnfs).
- This product includes JEP - Java Expression Parser code from Netaphor Software, Inc. (http://www.netaphor.com/home.asp).

Documentation Updates

The title page of this document contains the following identifying information:

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

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

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

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web 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 register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

Welcome to This Guide

This guide provides information for setting up and configuring the Closed Loop Incident Process (CLIP) solution that provides a change management process using HP Universal CMDB, HP Business Availability Center, HP SiteScope, HP Operations Manager for Windows, HP Operations Manager *i*, and HP Service Manager.

This chapter includes:

How This Guide Is Organized

This guide contains the following chapters:

Chapter 1 Introduction to CLIP

Provides an introduction to CLIP integrations and briefly describes how the following products work with each other:

- HP Universal CMDB (UCMDB)
- HP SiteScope (SiteScope)
- HP Business Availability Center (BAC)
- HP Operations Manager for Windows (OMW)
- HP Operations Manager *i* (OMi)
- HP Service Manager (Service Manager)

Chapter 2 SiteScope – BAC Integration Configuration

Provides information about setting up HP SiteScope and HP Business Availability Center in order to perform the integration.

Chapter 3 BAC – HPOM Integration Configuration

Provides information about setting up HP Business Availability Center and HP Operations Manager for Windows in order to perform the integration.

Chapter 4 OMI Installation and Configuration

Provides information about installing and setting up HP Operations Manager *i* in order to perform the integration.

Chapter 5 Service Manager – UCMDB Integration Configuration

Provides information about setting up HP Service Manager and HP Universal CMDB in order to perform the integration.

Chapter 6 Service Manager – OMW Integration Configuration

Provides information about setting up HP Service Manager and HP Operations Manager for Windows in order to perform the integration.

Chapter 7 Service Manager – BAC Integration Configuration

Provides information about setting up HP Service Manager and HP Business Availability Center in order to perform the integration.

Who Should Read This Guide

This guide is intended for a system implementer or system administrator who will be establishing and maintaining a connection between the HP Universal CMDB, HP SiteScope, HP Business Availability Center, HP Operations Manager for Windows, HP Operations Manager *i*, and HP Service Manager systems. This guide assumes that you have administrative access to all systems. The procedures in this guide may duplicate information available in the relevant documentation for these products, but is provided here for convenience.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

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:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

1

Introduction to CLIP

This chapter includes:

Concepts

Note: If you have any feedback or comments, please contact rahav@hp.com.

Closed Loop Incident Process – Overview

To better serve their businesses, today's IT organizations need to transform their infrastructure and operations from reactive to predictive service operations management. This approach closely aligns the management of IT and services to be delivered with value to the business, as well as the need to keep critical business services running at peak performance.

To this end, HP has developed the HP Closed Loop Incident Process (CLIP) concept. CLIP is an integrated solution that brings together HP offerings for IT Service Management (ITSM), Business Service Management (BSM), and Business Service Automation (BSA). It enables integrated processes that allow the IT operations and service desk teams to proactively and quickly predict, detect, and remedy harmful problems that could impact the business.

The following HP products are part of CLIP 1.5: HP Universal CMDB, HP Business Availability Center, HP SiteScope, HP Operations Manager for Windows, HP Operations Manager *i*, and HP Service Manager.

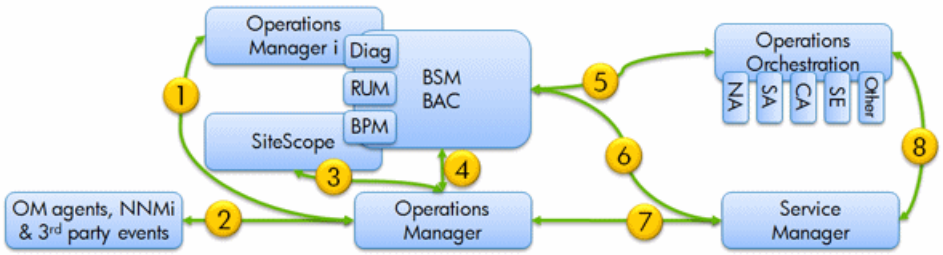
HP Operations Orchestration can be added to this solution by connecting a Service Manager record in the knowledge base to a specific workflow in HP Operations Orchestration, and launching it from Service Manager.

Note: This guide assumes that the CLIP products are installed in the following default locations:

- **UCMDB – C:\hp\UCMDB**
- **BAC – C:\HPBAC**
- **SiteScope – C:\SiteScope**
- **OMW – C:\Program Files\HP\HP BTO Software**
- **Service Manager – C:\Program Files\HP\Service Manager 7.11\Server**

CLIP 1.5 Architecture

The following diagram displays a typical deployment of the CLIP solution.



Hardware and Software Requirements

The instructions in this document assume that products are installed in the default location; if this is not the case, you will need to make the appropriate modifications to file paths mentioned in this document.

This section also includes:

➤ "Supported Versions" on page 15

➤ "Enterprise Hardware and Software Requirements" on page 17

Supported Versions

Product	Version	instructions
UCMDB	8.02 or later **Recommended**: 8.02	For installation instructions, see the *HP Universal CMDB Deployment Guide*.
BAC	8.02 or later **Recommended**: 8.02	For installation instructions, see the *HP Business Availability Center Deployment Guide*.
SiteScope	9.54 or later **Recommended**: 10.1	For installation instructions, see *HP SiteScope Deployment Guide*.

Product	Version	instructions
OMW	8.10 or later **Recommended**: 8.10	For installation instructions, see the *HP Operations Manager for Windows Installation Guide*. In addition, for OMW version 8.10 you must install the following patches, in order: ➤ OVOW_00044 (Agent) ➤ OVOW_00051 (Server) ➤ OVOW_00032 (Accessories) All patches may be downloaded from: http://support.openview.hp.com/selfsolve/patches
OMi	8.10 or later **Recommended**: 8.10	For installation instructions, see Chapter 3, "OMI Installation and Configuration" in this guide.
Service Manager	7.10 or later **Recommended**: 7.11	For installation instructions, see *HP Service Manager Installation Guide*.

Important: Make sure that each application you install is up and running before you perform any configuration steps.

Enterprise Hardware and Software Requirements

UCMDB Requirements

Recommendations	2 servers (including HA) ➤ at least 2 dual-core CPUs ➤ 8 GB RAM ➤ 12 GB RAM Virtual memory ➤ /PAE LB for UCMDB – 1 server (dedicated hardware such as F5 or other vendors) Reverse Proxy for UCMDB – 1 server (with Apache 2.2.x, for example) DB server ➤ at least 2 dual-cores ➤ at least 8 GB RAM
Can be virtual	Performance of HP Universal CMDB on VMware can be expected to be slower than with a regular installation. A VMware platform is therefore not recommended for an enterprise deployment of HP Universal CMDB and is supported only for standard deployments.

BAC Requirements

Recommendations	Servers Computer/Processor ➤ Windows: One of the following: ➤ Intel Dual Core Xeon Processor 2.4 GHz or higher ➤ AMD Opteron Dual Core Processor 2.4 GHz or higher Number of CPUs: ➤ Two-server (standard deployment): 1 dual core CPU ➤ Two-server (enterprise deployment): 2 dual core CPUs ➤ Solaris: ➤ Minimum: Dual UltraSPARC IV 1.8 GHZ, 6 GB RAM or 4 GB RAM with 2 GB of swap space Operating System ➤ Windows: Highly recommended for enterprise deployment: ➤ Windows Server 2003 R2 Enterprise x64 Edition, Service Pack 2 ➤ Windows Server 2003 Enterprise x64 Edition, Service Pack 2 Also supported: ➤ Windows Server 2003 32-Bit Enterprise Edition, Service Pack 1 or 2 ➤ Windows Server 2003 R2 32-Bit Enterprise Edition, Service Pack 2 Minimum for all deployments: ➤ Windows Server 2003 32-Bit Standard Edition, Service Pack 1 or 2 ➤ Solaris: ➤ Sun Solaris 9 ➤ Sun Solaris 10 (recommended) ➤ Sun Solaris Zones **Note:** Regardless of the operating system version, the entire Distribution (with OEM support) and the latest recommended Patch Cluster are required.

	Web Server ➤ Windows: ➤➤ Microsoft Internet Information Server (IIS) 6.0 ➤➤ Apache HTTP Server 2.2.11 (adapted by HP for HP Business Availability Center and installed during HP Business Availability Center server installation) ➤ Solaris: ➤➤ Sun Java System Web Server 6.1, Service Pack 5 ➤➤ SSL-compatible Apache HTTP Server 2.2.11 (adapted by HP for HP Business Availability Center and installed during HP Business Availability Center server installation) Memory ➤ Two-server standard deployment - recommended: 4 GB RAM ➤ Two-server enterprise deployment - recommended: 8 GB RAM Windows Server 2003 Enterprise x64 Edition, SP 2, can support up to 16 GB RAM.) Virtual Memory/ Memory Swap Space ➤ Two-server standard deployment - recommended: 6 GB RAM ➤ Two-server enterprise deployment - recommended: 12 GB RAM **Note:** The virtual memory/memory swap space should always be at least 1.5 times the physical memory size. Free Hard Disk Space ➤ Minimum: 10 GB, recommended: 20 GB

	Databases ➤ Standard deployment ➤➤ 1 dual core ➤➤ at least 2 G RAM (recommended: 4 G RAM) ➤ Large deployment ➤➤ at least 2 dual cores or 1 quad core ➤➤ at least 4 G RAM (recommended: 8 G RAM) Oracle certification (must include latest critical patches) ➤ Certified ➤➤ Oracle 10.2.0.3 Enterprise Edition, 64 BIT, on Linux Enterprise Edition ➤➤ Oracle 10.2.0.3 RAC Enterprise Edition, 64 BIT, on Linux Enterprise Edition ➤➤ Oracle 10.2.0.3 Enterprise Edition, 64 BIT, on Solaris 10 ➤➤ Oracle 10.2.0.4 Enterprise Edition, 64 BIT, on Linux Enterprise Edition ➤ Supported ➤➤ Oracle 10.2.0.3 Enterprise Edition, 32 BIT, on Windows 2003 Enterprise Edition with SP 2 ➤➤ Oracle 10.2.0.3 Enterprise Edition, 64 BIT, on AIX 5L ➤➤ Oracle 10.2.0.3 Enterprise Edition, 64 BIT, on HP-UX 11.31 ➤➤ Oracle 10.2.0.4 RAC Enterprise Edition, 64 BIT, on Linux Enterprise Edition Microsoft SQL Server ➤ Certified ➤➤ Microsoft SQL Server 2005 Enterprise Edition with SP 2, 32 BIT, on Windows 2003 Enterprise Edition with SP 2 ➤➤ Microsoft SQL Server 2005 Enterprise Edition with SP 2, 64 BIT, on Windows 2003 Enterprise Edition with SP 2 MDAC components on BAC: 2.8 SP1 Refresh – Installed automatically with your BAC server installation.

	BAC site availability ➤ Windows display (relevant only for the Gateway Server machine) ➤ Color palette setting: at least 256 colors (recommended: 32,000 colors) ➤ Solaris display (relevant only for the Gateway Server machine) ➤ X-Server installed. ➤ Resolution: at least 1024 x 768 ➤ Windows supported browsers: ➤ Microsoft Internet Explorer (IE) 6.0, SP 2 (recommended) or Microsoft Internet Explorer (IE) 7.0 ➤ Solaris supported browsers: ➤ FireFox 2.0 All supported browsers must be set to accept all cookies. ➤ Acrobat Flash 8.0 or later ➤ Java support: 6u4 or later (recommended: 6u10)
Can be virtual	➤ Business Process Monitors can be run in a VMware environment, but HP will not address or resolve any support issues arising from Business Process Monitors running in a VMware environment. ➤ HP Business Availability Center capacities and performance will vary according to the various server resources, such as CPU, memory, and network bandwidth, allocated to HP Business Availability Center components. ➤ A Gigabit network card should be used. ➤ It is strongly recommended that you do not run a database server containing HP Business Availability Center databases on VMware if the database files reside on a VMware virtual disk. ➤ VMware is the only virtualization technology supported by HP Business Availability Center for Windows.

SiteScope Requirements

Recommendations	➤ Computer/Processor: Pentium III, 800 MHZ or higher ➤ Operating systems: ➤ Microsoft Windows 2000 Server/Advanced Server SP 4 ➤ Microsoft Windows 2003 Standard/Enterprise SP 1, SP 2 ➤ Microsoft Windows Server 2003 R2 SP 1 ➤ Memory: 1 GB minimum (recommended: 2 GB or more) ➤ Free hard disk space: 2 GB or more (recommended: 10 GB or more) ➤ Web browser: ➤ Microsoft Internet Explorer (IE) 6.0 SP1 or later ➤ All versions of Firefox, starting with 1.0 and including 3.0
Can be virtual	Refer to the SiteScope documentation for details on deploying SiteScope on a VMware platform.

For SiteScope requirements on other operating systems, see the see *HP SiteScope Deployment Guide*.

OMW Requirements

Recommendations	Hardware ➤ Minimum: PC with at least 1.4 GHz Intel Pentium III (or compatible) processor (AMD Opteron and Athlon 64 CPU supporting in 32-Bit mode). Recommended: 3.0 GHz or higher Intel Pentium 4 processor (dual CPU system). ➤ Minimum: 768 MB physical memory, with at least 512 MB virtual memory (page file). Recommended: 2GB physical memory. ➤ Minimum: 6.5 GB disk space required for installation (depending on selected product options). The management server only supports installation on NTFS volumes. Recommended a minimum 1 GB free hard disk space; high-performance hard drive. If you are installing HPOM in a cluster, the following minimum disk space requirements apply for installation: ➤ First cluster node: minimum 5.5 GB. ➤ Subsequent cluster node: minimum 2.25 GB Additional 3rd party SPIs or other integrated HPOM applications may require additional disk space. ➤ DVD-ROM drive required unless you are installing from a network share. ➤ Minimum: 17-inch monitor with 1024x768 resolution and at least 256 colors. Recommended: 19-inch monitor with 1280 x 1024 resolution recommended (if used as console system) and at least 256 colors. ➤ Multiprocessor systems are supported. Software ➤ Windows 2008 (32-Bit), or Windows 2003 SP1, SP2, or R2 (32-Bit) Standard Edition, Enterprise Edition, or Data Center Edition. Hotfix KB925336 for Windows Server 2003 is recommended. ➤ Adobe Acrobat Reader 7.0 (or later) is required to view the documentation. ➤ Internet Explorer 6.0 or later

	➤ Internet Information Services (IIS) 6.0. On Windows 2008, in the Server Manager install the role Web Server (IIS) with the following role services: ➤ Common HTTP Features: —Static Content —Default Document ➤ Application Development: —ASP.NET —ASP ➤ Security: —Basic Authentication —Windows Authentication ➤ IIS 6 Management Compatibility: —IIS 6 Metabase Compatibility —IIS 6 Management Console On Windows 2003, ensure that the following IIS components are available: ➤ Common Files (must be selected for any IIS installation) ➤ World Wide Web (WWW) server ➤ Active Server Pages (.asp) enabled on the management server to support the web console. ➤ Internet Information Services Manager (forced by WWW server selection) ➤ Microsoft Cluster is supported. ➤ Supported databases ➤ Microsoft SQL Server 2005 Express Edition (32-Bit) ➤ Microsoft SQL Server 2005 Standard or Enterprise Edition (32 and 64-Bit) ➤ Microsoft SQL Server 2000 Enterprise Edition (32-Bit)The name of the database instance is user-configurable.

Can be virtual	➤ Business Process Monitors can be run in a VMware environment, but HP will not address or resolve any support issues arising from Business Process Monitors running in a VMware environment. ➤ HP Business Availability Center capacities and performance will vary according to the various server resources, such as CPU, memory, and network bandwidth, allocated to HP Business Availability Center components. ➤ A Gigabit network card should be used. ➤ It is strongly recommended that you do not run a database server containing HP Business Availability Center databases on VMware if the database files reside on a VMware virtual disk. ➤ VMware is the only virtualization technology supported by HP Business Availability Center for Windows. ➤ Refer to the SiteScope documentation for details on deploying SiteScope on a VMware platform. The relevant HP Business Availability Center components that are supported on virtualization platforms are: ➤ HP Business Availability Center servers (Gateway and Data Processing) 8.0x – VMware ESX Server 3.x or later, Solaris 9 and 10 Zones Performance of an enterprise environment on VMware can be expected to be up to 30% slower than in a regular installation. ➤ Business Process Insight 8.0x – VMware ESX Server 3.x ➤ Business Process Monitor 8.02 – Not Supported ➤ SiteScope 10.00 – VMware ESX Server 3.0 or later, VMware Virtual Center 2.x ➤ SiteScope 10.10 – VMware ESX Server 3.0 or later, VMware Virtual Center 2.x ➤ HP Diagnostics Agents/Probes 8.0x – VMware ESX 3.x Server and Solaris 10 Zones ➤ HP Diagnostics Server 8.0x – VMware ESX 3.x Server and Solaris 10 Zones ➤ HP Universal CMDB 8.0x – VMware ESX 3.x Server or later ➤ HP Discovery and Dependency Mapping 8.0x – VMware ESX 3.x Server or later

OMi Requirements

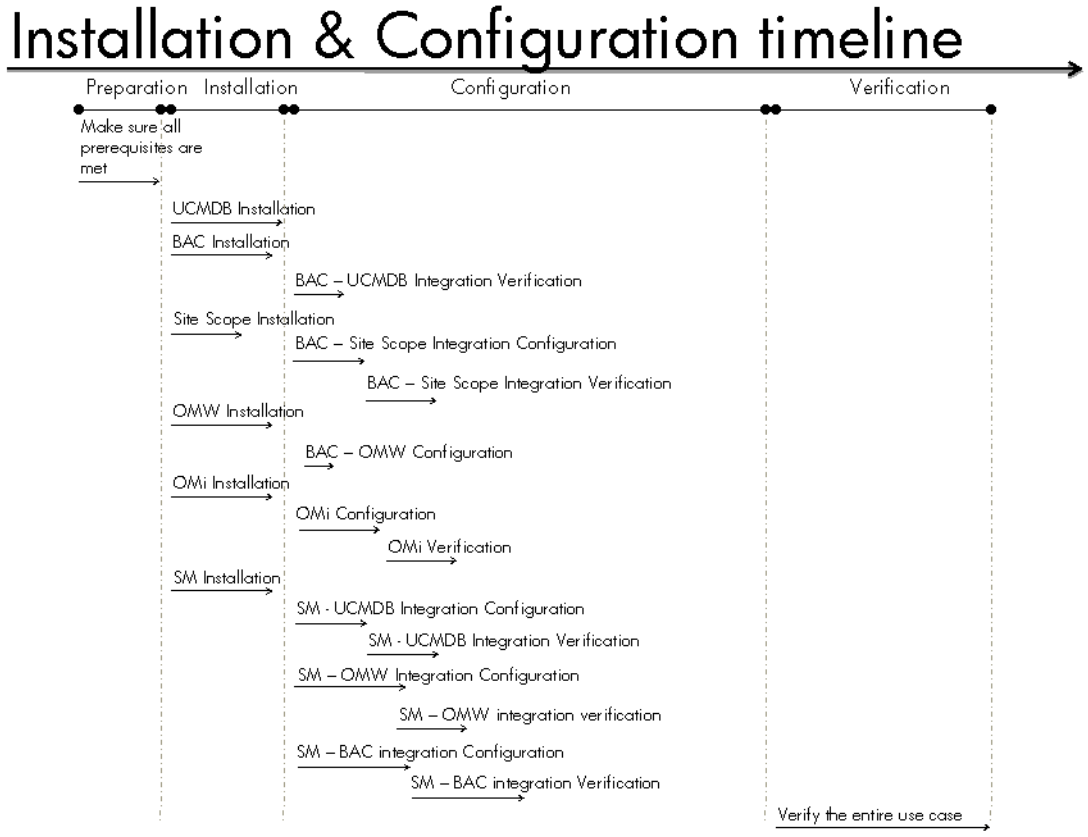
Recommendations	Free disk space ➤ For single-machine deployment: 350 MB ➤ For multiple-machine deployment: ➤ Gateway Server: 330 MB ➤ Data Processing Server: 150 MB ➤ Database (without any content): 750 MB
Can be virtual	N/A

Service Manager Requirements

Recommendations	1 HTTP Server ➤ 2 CPUs/cores ➤ 4 GB RAM 2 Web application servers (including HA) ➤ 8 CPUs/cores ➤ 16 GB RAM 2 SM Servers (including HA) ➤ 8 CPUs/cores ➤ 32 GB RAM ➤ Windows Server 2003 x64 1 SE (Search Engine) Server ➤ 1 dual-core CPU ➤ 4 GB RAM 2 Load Balancers for HA implementation.
Can be virtual	HP Service Manager has not been tested for scalability as a VMWare guest.

CLIP Project Planning

The following diagram provides a visual display of the various tasks that must be done in order to use the CLIP solution.



HP Universal CMDB – Overview

HP Universal CMDB (UCMDB) enables you to manage all the CIs contained in a managed world. A managed world refers to any self-contained environment that can be described using a topology model (defined with HP's Topology Query Language (TQL)).

Integration Class Model

The integration comes with a class model that maps UCMDB CI types, relationships, and attributes to objects and attributes that Service Manager recognizes. In general, Service Manager recognizes fewer CI types than UCMDB. Service Manager manages certain UCMDB CI types, such as a TCP/IP port, as CI attributes rather than a separate CI type. The integration class model groups UCMDB CI types to match how they are managed in Service Manager.

If you want to change the CIs that your UCMDB system sends to your Service Manager system, you need to edit both the integration class model and the integration queries that support the model.

Integration TQL Queries

The integration uses a collection of TQL queries to gather CI attribute information from UCMDB and sends it to the Service Manager system. If you want to change what CI types or attributes are part of the integration, you must also edit the integration queries to support your updated CI types and attributes.

HP Business Availability Center – Overview

HP Business Availability Center (BAC) helps companies optimize the performance and availability of applications in production and proactively resolve problems when they arise, thus assisting critical production applications to perform as required and deliver business results.

HP Business Availability Center helps customers model their business processes and services by providing a framework for mapping the complex and dynamic dependencies between applications and their supporting infrastructure. HP Business Availability Center helps customers optimize business availability by proactively detecting problems in order to prioritize problem resolution based on business impact and service level compliance.

HP SiteScope – Overview

HP SiteScope (SiS) is an agentless monitoring solution designed to ensure the availability and performance of distributed IT infrastructures—for example, servers, operating systems, network devices, network services, applications, and application components. This Web-based infrastructure monitoring solution is lightweight, highly customizable, and does not require that data collection agents be installed on your production systems.

SiteScope provides different tools, such as templates, the Publish Template Changes wizard, and automatic template deployment that enable you to develop a standardized set of monitor types and configurations into a single structure. SiteScope templates can be speedily deployed across the enterprise and quickly updated to make sure that the monitoring infrastructure is compliant with the standards set in the template. SiteScope also includes alert types that you can use to communicate and record event information in a variety of media. You can customize alert templates to meet the needs of your organization.

HP Operations Manager for Windows – Overview

HP Operations Manager for Windows (OMW) is a distributed, client/server software solution designed to provide service-driven event and performance management of business-critical enterprise systems, applications, and services.

OMW enables management of distributed, heterogeneous e-business infrastructures and includes support for a broad range of Windows and UNIX systems and applications, including e-commerce, web and application servers, conferencing and email, databases, ERP software, and more.

HP Operations Manager *i* – Overview

HP Operations Manager *i* (OMi) uses information from multiple sources to compile and display a comprehensive and detailed overview of the health of your IT operation. With OMi, you can:

- monitor, investigate, and manage the events that occur in your organization's IT environment
- correlate events across multiple domains
- create tools to check and fix problems
- compile and display a detailed overview of the health of your systems including diagrams, reports, charts, and graphs, which you can use both to view trends and drill down to the root cause.

HP Service Manager – Overview

HP Service Manager stores the managed or expected state of CIs and CI relationships as attribute values in a CI record. To be part of the integration, a CI attribute in your UCMDB system must map to a managed field in the Service Manager CI record. You can add, remove, or update the managed fields that are part of the integration by tailoring the Service Manager web services that manage the integration.

Service Manager runs according to a set of rules that define what actions you want the system to take whenever a CI's actual state does not match the expected state as defined in the CI record. You define these rules from the Discovery Event Manager (DEM) in Service Manager where you can do the following:

- Automatically update a CI record to match the attribute values listed in the actual state. (This is the default behavior.)
- Automatically create a change record to review the differences between the actual state and the managed state.
- Automatically create an incident record to review the differences between the actual state and the managed state.

2

SiteScope – BAC Integration Configuration

This chapter includes:

Concepts

Tasks

Overview

SiteScope acts as a monitoring foundation for HP offerings such as Business Availability Center and OMW. With SiteScope, you gain the real-time information you need to verify infrastructure operations, stay apprised of problems, and solve bottlenecks before they become critical.

Set Up BAC for Integration with SiteScope

The following steps describe how to define a SiteScope server on a BAC machine.

1 Create a profile database:

a Open the BAC management console.

b Select **Admin** > **Platform** > **Manage Profile Database**.

c Click **Add** and enter the details for the new schema.

d Select the **Make this my default profile database** check box and click **Apply**.

2 Select **Admin** > **System Availability Management**.

3 Click the **New SiteScope** button to define a new SiteScope Server. Enter the following server details in the Main Settings and Distributed Settings sections of the form:

Name	Recommended Value	Description
Display Name	**<user defined>**	The display name of the SiS server.
Host Name	**<user defined>**	The fully qualified name of the SiS server.
Port Number	**8080**	The SiS port number.
Gateway server name/IP address	**<user defined>**	The fully qualified name of the BAC Gateway server.
SiteScope agent machine location	**<user defined>**	The fully qualified name of the SiS server.
Gateway server authentication user name	**admin**	The BAC user name.
Gateway server authentication password	**<user defined>**	The BAC user password.

This completes the process of defining a SiteScope server in BAC. You can now define new SiteScope monitors to monitor your network by clicking the **New** button and then selecting **New Group** or **New Alert**.

Note: To view the relevant SiteScope monitors, select **Dashboard** > **System Monitors View**.

3

OMI Installation and Configuration

This chapter includes:

Concepts

Tasks

Overview

OMi links the operations management world with the business service management world and can be seen as *the* event management foundation for the complete HP BSM solution. OMi provides a new, enhanced event console and is able to process events that originate from various HP BSM components such as such as UCMDB, BAC, SiteScope, OMW, OMi, and Service Manager.

Install OMi

The following steps describe how to install OMi first on the Data Processing Server systems, and then on the Gateway Server systems.

1. Stop BAC.
2. Extract the .ISO file located in **\\rubicon\BACIntegrations\Vega\Latest** and execute the **install_hpomi.vbs** file.

Note: OMi requires the Microsoft Visual C++ 2005 Redistributable in order to run. If it is missing, the installer prompts you to accept its installation.

---

3. Click **OK** to continue with the OMi installation.
4. When the installer has finished initializing, click **Next**.
5. In the Introduction (Install) screen, click **Next**.
6. In the license agreement screen, agree and click **Next**.
7. In the Choose the application and data folders screen, click **Next**.
8. In the Install Checks screen, click **Next**.
9. In the Pre-Install Summary screen, click **Install**.

   If the installation was not successful, review the installation log file for any errors by clicking the **View log file** link in the Installation Complete window to view the log file in a web browser.
10. Click **Done** to close the installation program.

This process installs one instance of OMi. If your machine deployment consists of two or more machines, repeat these instructions for all Data Processing Server machines and then for all Gateway Server machines.

Configure OMi

Perform the following steps to create an Oracle database for OMi on a Data Processing Server.

1. Stop BAC.
2. On each BAC server, open a new command prompt window and enter the following command to launch the OMi configuration wizard:

   %TOPAZ_HOME% \bin\opr-configuration.bat -setup

   The default value of the system variable *%TOPAZ_HOME%* is C:\HPBAC.
3. When the OMi Configuration Wizard opens, click **Next**.
4. In the OMi Database Settings window, select **Create a new database or user schema** and click **Next**.
5. In the Database Server Type window, select **Oracle Server** and click **Next**.
6. Enter the required data for the Oracle database configuration as follows:

Name	Recommended Value	Description
Host name	**<user defined>**	The fully qualified host name of the machine on which the Oracle database server is installed.
Port	**1521 (default)**	The database port number
SID	**<user defined>**	The system identifier or name of the database that uniquely identifies the Oracle database being used.
Admin User Name	**<user defined>**	The user name of the database administrator (who has administrative permissions) on the Oracle server.
Admin User Password	**<user defined>**	The database administrator's password.

7. Click **Next**.

8 Enter the required data for the new schema as follows:

Name	Recommended Value	Description
New schema name	**<user defined>**	The name of the schema you are creating (for example, HPOMi_DB_Schema).
New schema password	**<user defined>**	The password for that schema.
Confirm password	**<user defined>**	Re-enter the password to confirm it.
Default tablespace	**users (default)**	The name of the dedicated default tablespace reserved for schemas.
Temporary tablespace	**temp (default)**	The name of the dedicated temporary tablespace reserved for session data.

9 Click **Next**.

10 Enter the OMW server information to set up the event and Topology Synchronization, and click **Next**.

Name	Recommended Value	Description
OMW Server DNS name	**<user defined>**	The fully qualified domain name of the OMW server (for example, HPOMWSrv.example.com).
OMW Server Port number	**8080** (default)	Enter the correct web service port number.
OMW Server Username for OMW	**<user defined>**	The OMW user name. For Topology synchronization only
OMW Server Password for OMW	**<user defined>**	The OMW password. For Topology synchronization only
OMW Server Type	OM for Windows	For Topology synchronization only

11 In the Summary window, click **Finish**.

Set Up BAC for Integration with OMW

To configure the OMW server in BAC for OMi connectivity, do the following:

1 In BAC, select **Admin** > **Platform** > **Infrastructure Settings**.

2 In the **Foundations** drop-down list, select **Integration with other applications**.

3 Enter the full name of your OMW server in the **OM host** field.

Validate OMi Installation and Configuration

This task includes the following steps:

➤ "Verify the HP Operations Manager i Service and Process Names" on page 39

➤ "Verify OMi Menu Entries in the BAC Management Console" on page 39

Verify the HP Operations Manager *i* Service and Process Names

1 Start BAC.

2 Check that the OMi service name **OPR** and the process name **opr-backend** appear in the **Nanny Status** and the **HAC Status**.

OMi has been successfully installed and configured when the **opr-backend** process is listed and running on one Data Processing Server.

Verify OMi Menu Entries in the BAC Management Console

1 Make sure BAC is running.

2 Open a browser window and enter the Gateway Server address to start the BAC management console.

3 Log on to the BAC management console using an account with administrative privileges.

4 After you have logged on, on the Applications page select **Operations Management**.

5 Select **Admin** > **Operations Management** to see the OMi-related menu entries.

Import Content Packs

OMi uses content packs to exchange customized configuration data between OMi installations. A content pack can contain a complete snapshot of all (or any part of) rules, tools, mappings, and assignments that you define and configure.

To import content packs:

1 Make sure BAC is running.

2 Open BAC in a browser on one of the Data Processing Server machines.

3 Log on to the BAC management console using an account with administrative privileges.

4 Select **Admin** > **Operations Management** > **Manage Content** tab > **Content Packs**.

5 Click the **Import Content Pack Definitions and Content** button.

6 Browse to the location of the content packs. The default location is: *%TOPAZ_HOME%***HPBAC****conf****opr****content**.

7 Select a content pack (for example, MM-INF.xml), and click **Open**.

8 Select **Overwrite** and click **Import** to import the content pack.

The Information dialog window appears, showing you the number of artifacts (for example, health indicator definition artifacts) that you have imported.

9 Click **OK**.

Repeat this procedure to load additional content packs.

Connect HP Operations Manager *i* to OMW

Connecting HP Operations Manager *i* to OMW enables bidirectional synchronization of events between the two systems.

This task includes the following steps:

- "Add a Gateway Server as a Node to OMW" on page 41
- "Establish a Trust Relationship" on page 42
- "Configure a Message Forwarding Policy" on page 43

Add a Gateway Server as a Node to OMW

Before establishing an SSL trust relationship, you must add the Gateway Servers as nodes to OMW. This trust relationship is necessary for event synchronization between the OMi and OMW systems.

Note: To add a managed node, you must be a member of the HP-OVE-ADMINS group on the OMW management server.

To add a node to OMW:

1. Start OMW by selecting **Start** > **Programs** > **HP** > **HP Operations Manager** > **HP Operations Manager Console**.
2. Right-click **Nodes** and select **Configure** > **Nodes**.

   The Configure Managed Nodes dialog box opens.
3. In the right-hand pane, right-click **Managed Nodes** and select **New Node**.

   The Base Settings dialog box opens.
4. Enter the fully qualified domain name and the display name for the node you want to add.
5. Select **Enter manually** and click **Next**.

   The OS Setup dialog box opens.
6. In the System Type field, select **x86/x64 Compatible**.

7. Select the appropriate values for Operating System, Bit Length, and Version, and click **Next**.

   The Advanced Settings dialog box opens.

8. Clear the **Automatic deployment of policies and packages** check box.

9. Select the **Automatically grant certificate** check box.

10. Click **Finish** to close the Advanced Settings dialog box and return to the Configure Managed Nodes dialog box.

11. In the Configure Managed Nodes dialog box, click **OK**.

12. In the Agent Installation dialog box, click **Cancel**.

    After the dialog box closes, the OMi system node appears in the list of nodes in OMW.

Establish a Trust Relationship

To enable successful connection and communication between OMi and OMW, you must establish a trust relationship between the two systems.

To configure certificates for OMi:

1. Make sure BAC is not running.

2. Open a command prompt and change directory to *%TOPAZ_HOME%***bin**.

3. To start the certificate configuration script, execute the following command:

   ```
   opr-certificate-configuration.bat
   ```

The output of the command output informs you that a certificate request was sent to the OMW server.

To grant certificates in OMW:

1. In the left pane of the OMW console, click **Certificate requests**.

2. In the right pane of the Certificate requests window, right-click the entry for your OMi system. You can identify your system by the values listed in the **Mapped Node** and the **Requesting Client** columns.

3. Select **All Tasks** > **Grant** to grant a certificate request to the OMi system.

4 Confirm the certificate grant by clicking **OK** in the Grant Certificate Request window. When you have successfully granted the certificate request, the window closes.

Configure a Message Forwarding Policy

To enable event synchronization between OMW and OMi, you must create a message forwarding policy on OMW that contains the node name of the OMi system.

To set up a policy on OMW:

1 In the Operations Manager tree in OMW, select **Policy management** > **Server policies grouped by type** > **Server-based Flexible Management**.

2 Right-click **Server-based Flexible Management** (or a blank space in the right window pane) and select **New** > **Policy**. The Server-based Flexible Management Editor dialog box is displayed.

3 Insert the following text for the new policy into the blank window of the **General** tab:

```
TIMETEMPLATES
    # none
    RESPMGRCONFIGS
        RESPMGRCONFIG DESCRIPTION "Forward all messages to HP OMi"
        SECONDARYMANAGERS
        ACTIONALLOWMANAGERS
            MSGTARGETRULES
            MSGTARGETRULE DESCRIPTION "Forward all messages rule"
                MSGTARGETRULECONDS
                MSGTARGETRULECOND DESCRIPTION "Forward all messages"
                MSGTARGETMANAGERS
                    MSGTARGETMANAGER
                    TIMETEMPLATE "$OPC_ALWAYS"
                    OPCMGR IP 0.0.0.0 "<HP OMi fully qualified HN>"
```

4 Replace <HP OMi fully Qualified HN> in the text with the fully qualified hostname of the Gateway Server system that should receive OMW messages (for example, HPGwSrv.example.com).

5 Click **Check Syntax** to ensure that there are no syntax errors in the text of the new policy.

6 Click **Save and Close**.

7 In the **Save As** dialog box, enter a name and a description for the new policy, and click **OK**.

8 In the Policy Management folder, right-click the new policy and select **All Tasks** > **Deploy on**.

9 In the **Deploy server policy on** dialog box, select the name of your OMW management server.

10 Click **OK** to deploy the server-based flexible management policy on the OMW management server.

Validate Event Synchronization

The following steps describe how to verify that you have configured OMi properly to perform the integration.

➤ "Verify Message Forwarding from OMW to OMi" on page 44

➤ "Verify OMi Event Synchronization with OMW Messages" on page 45

Verify Message Forwarding from OMW to OMi

1 In OMW, open a command or a shell prompt.

2 To create a new message, execute the following command:

```
opcmsg a=App o=Obj msg_text="Hello"
```

If you have correctly configured the server-based flexible management, the message arrives at the OMW management server and is forwarded to HP OMi. You can view the events with the HP OMi event browser.

If the message is sent multiple times, no new message is generated by OMW. These messages are regarded as duplicates and only the message duplicate count is increased.

To generate a new message, modify the message text

```
opcmsg a=App o=Obj msg_text="Hello_002"
```

Every new message is now forwarded to the HP OMi system.

Verify OMi Event Synchronization with OMW Messages

In this section, you check whether a change in an event is synchronized in OMi and OMW.

Choose an event that has been synchronized in OMW and OMi earlier and change its severity, for example, from minor to major.

To change the severity of an event:

1. Log on to the BAC management console.
2. Select **Applications** > **Operations Management**.
3. In the Event Browser pane of the Event Perspective window, select the event for which you want to change the severity.
4. In the Event Details pane of the Event Perspective window, click the **Edit** button on the General tab.
5. From the **Severity** drop-down list, choose another severity (for example, major) and click **Save**.
6. In OMW, verify that the severity of the event has been set to the new value.

4

Service Manager – UCMDB Integration Configuration

This chapter includes:

Concepts

Tasks

Overview

This section describes the necessary steps to configure and verify the integration between UCMDB and Service Manager.

Your UCMDB system stores the actual state of CIs and CI relationships as CI attributes. Typically, UCMDB uses one or more discovery mechanisms (feeders) to automatically detect CI attribute values. The UCMDB to Service Manager integration only uses a subset of the CI attributes available in a UCMDB system.

Set Up UCMDB for Integration with Service Manager

This task lists the steps necessary to configure HP Universal CMDB in order to perform integration with HP Service Manager.

This task includes the following steps:

Prerequisites

See "Hardware and Software Requirements" on page 15.

Log on to your UCMDB system as an administrator. Verify that all UCMDB services are running.

Deploy the Service Manager Integration Package

1 Copy the **smIntegration.zip** file from **c:\hp\UCMDB\UCMDBServer\root\lib\integration_packages** on the UCMDB machine to a location on your local machine.

2 Open the UCMDB management console.

3 Select **Settings** > **Package Manager**.

UCMDB displays a list of installed packages.

4 Click the **Deploy Packages to Server (from local disk)** button.

5 Click the **Add** button.

6 Select the **smintegration.zip** file that you just copied, and click **OK**.

Add a Changes Adapter Data Store

This data store acts as a source adapter for querying the CMDB for changes. The Changes adapter updates CI attributes in UCMDB during synchronization.

1 Select **Settings** > **Federated CMDB**.

2 Click the **Data Stores** tab.

3 Click the **New Data Store** button and enter the following information:

Name	Recommended Value	Description
Adapter	**CmdbChangesAdapter**	The name of the adapter that will be used.
Name	**<user defined>**	A unique name for the data store, which should not include spaces. For example: CI_Changes
CustomerID	**1**	The customer ID for HP Universal CMDB. If you are using HP Software-as-a-Service, use your customer ID number instead of 1.
Host	**<user defined>**	The name of the your UCMDB system. For example: localhost

4 Click the **Test Connection** button and then click **OK**.

5 Click **Next**.

6 Select the following TQL queries:

- applicationData
- businessServiceData
- hostData
- hostRelationsData
- networkData1
- networkData2

- networkRelationsData
- printerData

7 Click **Finish**.

Add an RMI Adapter Data Store

This data store acts as a source adapter during UCMDB to Service Manager synchronization. The RMI adapter updates CI relations in UCMDB.

1 Click the **New Data Store** button.

To access this button, select **Settings** > **Federated CMDB** and click the **Data Stores** tab.

2 Enter the following information:

Name	Recommended Value	Description
Adapter	**CmdbRmiAdapter**	The name of the adapter that will be used.
Name	**<user defined>**	A unique name for the data store, which should not include spaces. For example: Relationships
CustomerID	**1**	The customer ID for HP Universal CMDB. If you are using HP Software-as-a-Service, use your customer ID number instead of 1.
Host	**<user defined>**	The name of the your UCMDB system. For example: localhost

3 Click the **Test Connection** button and then click **OK**.

4 Click **Next**.

5 Select the following TQL queries:

- applicationRelationsData
- businessServiceRelationsData

6 Click **Finish**.

Add a ServiceDesk Adapter Data Store

This data store acts as a target adapter during UCMDB to Service Manager synchronization. The Service Desk adapter updates CI relations and CI attributes in Service Manager.

1 Click the **New Data Store** button.

To access this button, select **Settings** > **Federated CMDB** and click the **Data Stores** tab.

2 Enter the following information:

Name	Recommended Value	Description
Adapter	**ServiceDeskAdapter**	The name of the adapter that will be used.
Name	**<user defined>**	A unique name for the data store. For example: cmdb2sm
Host	**<user defined>**	The name of the your Service Manager system. For example: mysmserver
Port	**<user defined>**	The communications port of your Service Manager system. For example: 13080 (default)
User	**<user defined>**	The operator name of a Service Manager system administrator.
Password	**<user defined>**	The password of the Service Manager system administrator.

3 Click the **Test Connection** button and then continue clicking **OK** to each confirmation message that appears.

Note:

The following message may appear when you attempt to test the connection:

```
The dataStore3 has problem with configuration:
"A default configuration is not defined.
To define a configuration, access \fcmdb\CodeBase\ServiceDeskAdapter,
locate the configuration file with the appropriate version suffix, and delete the suffix."
```

This occurs because an incorrect adapter configuration file has been used.

The adapter comes with three different configurations (for versions 6.xx, 7.0x, and 7.1x).

To solve this problem, choose the correct configuration file from **c:\hp\UCMDB\UCMDBServer\j2f\fcmdb\CodeBase\ ServiceDeskAdapter**, and remove the extra suffix from the file. For example, change serviceDeskConfiguration.xml.7.1x to serviceDeskConfiguration.xml. Then, restart the UCMDB server.

---

4 Click **Next**.

5 Select all the CI types and attributes that you want to receive from Service Manager.

6 Click **Finish**.

Transfer CIs from UCMDB to Service Manager

The integration requires a one-time transfer of CIs from UCMDB to Service Manager to populate the Service Manager system with CIs. The integration then updates the list of CIs in Service Manager when UCMDB discovers new CIs or new attribute values. The integration accomplishes the transfer of CI data using replication jobs in the UCMDB system. HP recommends that you schedule these jobs to keep your CIs and CI attributes up to date.

This task includes the following steps:

1 Define a Changes replication job between UCMDB and Service Manager.

a Click the **Replication Jobs** tab.

To access this button, select **Settings** > **Federated CMDB**.

b Click the **New Replication Job** button.

c Enter the following information:

Name	Recommended Value	Description
Name	**<user defined>**	A unique name for the replication job. For example: cmdb2sm
Source Data Store	**<user defined>**	The name of the source data store in UCMDB that you created in "Add a Changes Adapter Data Store" on page 49.
Target Data Store	**<user defined>**	The name of the target data store in UCMDB that you created in "Add a ServiceDesk Adapter Data Store" on page 51.

d Select all queries by clicking the **Active** check box. In addition, click the **Permit deletion in target** check box for each query.

e Click **OK**.

f Click the **Ad Hoc Full Replication** button to run the replication job.

g When the **Confirm synchronizing** window appears, click **Yes**.


h Click the **Statistics** button to show synchronization progress status.

i To see the updated synchronization status, click the **Refresh** button.

2 Define an RMI replication job between UCMDB and Service Manager.

a Click the **New Replication Job** button.

To access this button, select **Settings** > **Federated CMDB and click the Replication Jobs** tab.

b Enter the following information:

Name	Recommended Value	Description
Name	**<user defined>**	A unique name for the replication job. For example: cmdb2smBusinessRels
Source Data Store	**<user defined>**	The name of the source data store that you created in "Add an RMI Adapter Data Store" on page 50.
Target Data Store	**<user defined>**	The name of the target data store that you created in "Add a ServiceDesk Adapter Data Store" on page 51.

c Select all queries by clicking the **Active** check box. In addition, click the **Permit deletion in target** check box for each query.

d Click **OK**.

e Click the **Ad Hoc Full Replication** button to run the replication job.

f When the **Confirm synchronizing** window appears, click **Yes**.


g Click the **Statistics** button to show synchronization progress status.

h To see the updated synchronization status, click the **Refresh** button.

3 Schedule replication jobs.

a Select **Settings** > **Scheduler**.

The Job Scheduler form opens.

b Click  to add a job to the Job Scheduler.

c In the **Name** field, type a unique name for the job.

d Click  in the **Actions** section to add an action definition to the job.

e In the **Actions** list, select **Run Replication Job** and click **Next**.

f In the **Run Replication Job** list, select the replication jobs you want to schedule.

g Click **Finish**. UCMDB displays the action in the action list.

h In the Scheduler section, select the frequency for the replication job to run, as well as the required replication job time constraints.

i Click **OK**.

Make Integration Components Visible in UCMDB

The CITs added by deploying the **smIntegration** package are not automatically visible under the IT Universe node of the CI Type Selector. To view these CI Types in the tree, and to be able to edit or create new TQL queries with the proper links, do the following:

1 Select **Settings** > **Infrastructure Settings Manager**.

2 Click the **Foundations** radio button and then select **UCMDB common** from the drop-down list.

3 Click the **Edit Setting** button for the **Link Root** entry and type **link** in the **Value** field.

4 Click the **Edit Setting** button for the **Object Root** entry and type **data** in the **Value** field.

5 Log off of UCMDB and then log on again.

Configure DDMi as an Additional UCMDB Feeder – Optional

This task lists the steps necessary to configure DDMi to operate as an additional feeder mechanism for HP Universal CMDB.

This task includes the following steps:

- "Add an DDMi Adapter Data Store" on page 56
- "Change the DDMi Adapter Name" on page 57
- "Define a Replication Job between DDMi and UCMDB" on page 58
- "Define a Replication Job between DDMi and UCMDB" on page 58
- "Verify the DDMi to UCMDB Replication Job" on page 59

Add an DDMi Adapter Data Store

1 Select **Settings** > **Federated CMDB**.

2 In the **Data Stores** tab, click the **New Data Store** button. The New Data Store dialog box opens.

3 Enter the following information:

Name	Recommended Value	Description
Adapter	**EDDBAdapter**	The name of the adapter that will be used to retrieve the external data from the DDMi database.
Name	**ed**	The name of the data store. You must use the name **ed** if you are integrating DDMi with Service Manager. To change the EDDB Adapter Name, you must modify the **webserviceAdapters.xml** file. For details, see "Change the DDMi Adapter Name" on page 57.
Host	**<user defined>**	The name of the DDMi server

Name	Recommended Value	Description
Port	**8108**	The port through which you access the DDMi database.
User	**<user defined>**	The user name needed to access the DDMi database.
Password	**<user defined>**	The password needed to access the DDMi database.
URL	**dbtype=mysql;dbname=aggregate**	Use this field to define a specific URL to connect to the DDMi database.

4 Click the **Test Connection** button and then click **OK**.

5 Click **Next** and then click **Next** again, without choosing any CI types.

6 Select the following TQL queries:

- hostData
- hostRelationsData
- networkData1
- networkData2
- networkRelationsData
- printerData

7 Click **Finish**.

Change the DDMi Adapter Name

If you change the name of the DDMi Adapter, you must update the **webserviceAdapters.xml** file as follows:

1 In the UCMDB server file system, navigate to **c:\hp\UCMDB\UCMDBServer\j2f\fcmdb\CodeBase\ServiceDeskAdapter\webserviceAdapters.xml**.

2 Edit the file to update the adapter name as follows:

```
<adapters>
  <!-- The names of all the data stores that are defined in UCMDB that are used for the
SM web service should be listed here.
In case the adapter is not the owner change the value to "no" -->
  <adapter name="<Name>" owner="yes"/>
```

Note: The adapter name <Name> is the name that you assigned when creating the data store in step 3.

Define a Replication Job between DDMi and UCMDB

1 Select **Settings** > **Federated CMDB**.

2 Click the **Replication Jobs** tab.

3 Click the **New Replication Job** button.

4 Enter the following information:

Name	Recommended Value	Description
Name	**<user defined>**	A unique name for the replication job. For example: DDMi_to_UCMDB
Source Data Store	**<user defined>**	The name of the source data store in UCMDB that you created in "Add an DDMi Adapter Data Store" on page 56.
Target Data Store	**<user defined>**	The name of the target data store in UCMDB that you created in "Add an RMI Adapter Data Store" on page 50.

5 Select all queries by clicking the **Active** check box. In addition, click the **Permit deletion in target** check box for each query.

6 Click **OK**.

Verify the DDMi to UCMDB Replication Job

1 Select the relevant UCMDB feeder to UCMDB replication job name.

To access this button, select **Settings** > **Federated CMDB** and click the **Replication Jobs** tab.

2 Click the **Ad Hoc Full Replication** button.

3 When the **Confirm synchronizing** window appears, click **Yes**.

4 Click the **Statistics** button to show synchronization progress status.

5 To see the updated synchronization status, click the **Refresh** button.

6 Select **Modeling** > **Query Manager**.

7 Verify that CI Type Selector has been updated with the new CI types from the integration.

Set Up Service Manager for Integration with UCMDB

This task lists the steps necessary to configure HP Service Manager, in order to perform the integration with HP Universal CMDB.

This task includes the following steps:

Prerequisites

See "Hardware and Software Requirements" on page 15.

Log on to your UCMDB system as an administrator. Verify that all UCMDB services are running.

Add the UCMDB Connection Information to the System Information Record

The integration process requires the UCMDB connection information to obtain CI attribute information from UCMDB.

1. Log on to your Service Manager system as an administrator.
2. Select **Menu Navigation** > **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record**.
3. Click the **Active Integrations** tab.
4. Select the HP Universal CMDB option. The form displays the UCMDB web service URL field.

5 In the UCMDB web service URL field, type the URL to the HP Universal CMDB web service API. The URL has the following format: **http://<UCMDB server name>:<port>/axis2/services/ucmdbSMService**.

Replace <UCMDB server name> with the host name of your UCMDB server, and replace <port> with the communications port that your UCMDB server uses.

6 Enter your UCMDB user name and password.

7 Replicated CIs may appear in Service Manager as changes and not as new CIs. If you want to view the replicated CIs as new CIs in Service Manager, do the following:

a Select **Menu Navigation** > **Tailoring** > **Web Services** > **Discover Event Manager Rules**.

b Click **Search**. The list of replicated CIs is displayed.

c Select the items for which you want to display the CIs in Service Manager.

d In the **Rules** tab, click the **Add the record** radio button.

e Click **Save**.

f Rerun the replication job in UCMDB. The CIs will now appear in Service Manager as new items.

Enable Federated Data to be Viewed in UCMDB

1 In the UCMDB server file system, navigate to **c:\hp\UCMDB\UCMDBServer\j2f\fcmdb\CodeBase\ServiceDeskAdapter**.

2 Depending on the version of Service Manager that you have installed, copy either the **ucmdbIntegration7_1x.unl** or **ucmdbIntegration7_0x.unl** file to any location on your Service Manager server.

3 In Service Manager, type **db** in the command box and click  to execute the command.

4 Right-click in the right-hand pane and select **Import/Load** from the menu.

5 Click the **Browse** button next to the **File Name** field toy locate the *.unl file that you downloaded in step 2.

6 After you have selected the correct file, click **Load FG**. Be sure to acknowledge any message that appears.

Verify UCMDB-SM Ticket Data Federation

1 Log on to Service Manager.

2 Create the following items and assign each one to a CI in UCMDB:

- Change
- Incident
- Problem

3 Log on to UCMDB.

4 Select **Modeling** > **View Manager**.

5 Create a new view and drag the following CI types into the view:

- Planned Change
- IT Incident
- IT Problem

6 Click **Save**.

7 Click the **Calculate TQL Result Count** button and verify that each CI Type has at least one instance.

Verify UCMDB Integration with Service Manager

1 Log on to the Service Manager system as an administrator. After you perform a replication job to populate the Service Manager system with CIs from UCMDB, the **Actual State** tab will be visible in CI records.

2 Ensure that CIs for the following items are visible in Service Manager.

- business services
- applications
- hosts

3 Verify that relationships exist between the following:

- business services and applications
- applications and hosts

5

Service Manager – OMW Integration Configuration

This chapter includes:

Concepts

Tasks

Overview

This section describes the steps to install and configure the integration of HP Service Manager with OMW.

In order for the updates to run immediately, both machines must be in the same time zone.

Install SCAuto on a Service Manager Server

1 Log in to the Service Manager server as a user with local administrator privileges.

Caution: Do not install the applications over existing versions of SCAuto. You must uninstall first, or install into a new folder.

---

2 Insert the SCAuto Applications version 4.0.2 installation media into the appropriate drive of the server. If you are installing on a system that has auto-run enabled, the installation media browser starts automatically. If auto-run is disabled, follow these steps to start the installation media browser manually:

a Navigate to the installation media folder.

b Double-click **setupwin32.exe**. The HP SCAuto for OMW installation program opens.

Note: If you are installing SCAuto on a fresh image, ensure that Java has been previously installed.

---

3 When requested, accept the license agreement by clicking **Next**.

4 Accept the default installation path and click **Next**.

Warning: You must install SCAuto for OMW in a folder containing only ASCII characters in the folder name. The applications cannot start if installed in a folder with non-ASCII characters in the folder name.

---

5 Select a typical configuration. Modify the data as required for your configuration.

Name	Description
Server name	The name of your server.
Server port	Any free port on the server.
MAPI profile	Required for mail notifications from SCAuto.

6 Click **Install**.

Run the SCAuto Listener

To ensure that the SCAuto listener is started with Service Manager, add the **scautolistener:12680** command to the **sm.ini** file located in the **C:\Program Files**\HP\Service Manager 7.11\Server**RUN** directory.

Add SCAuto Event Processing to Service Manager

Perform the following steps in Service Manager to enable SCAuto event processing:

To run event processing:

1 Open the System Status window by entering **Status** in the command box and clicking **Enter**.

2 Click the **Start Scheduler** button. A list of schedulers is displayed.

3 Double-click the Event Services processor line to activate the event processor in Service Manager that is in charge of processing events received from OMW.

To schedule event processing to run at system startup:

1 Select **Menu Navigation** > **System Administration** > **Ongoing Maintenance** > **System** > **Startup Information**.

2 In the **Type** field, type **startup**, then click **Enter**.

3 Scroll down to the bottom of the form and add a new scheduler. Enter the following information:

Field	Recommended Value	Description
Name	**<user defined>**	
RAD Application	**scheduler**	The name of the RAD Application to run. RAD is an internal Service Manager scripting language.
Class	**event.startup**	One of the RAD Application classes.
Wakeup Interval (secs.)	**60**	
Priority	**1**	The event's priority.

4 Click **Save**:

Install SCAuto for OMW

Caution: Do not install the applications over existing versions of SCAuto. You must uninstall first, or install into a new folder.

---

1 Log in to the Windows OMW Management server as a user with local administrator privileges.

Note: If you are installing SCAuto on a fresh image, ensure that Java has been previously installed.

---

2 Insert the SCAuto for OMW version 1.3.1 installation media into the appropriate drive of the server. If you are installing on a system that has auto-run enabled, the installation media browser starts automatically. If auto-run is disabled, follow these steps to start the installation media browser manually:

   a Navigate to the installation media folder.

   b Double-click **setupwin32.exe**. The HP SCAuto for OMW installation program opens.

3 When requested, accept the license agreement by clicking **Next**.

4 Accept the default installation path and click **Next**.

Warning: You must install SCAuto for OMW in a folder containing only ASCII characters in the folder name. The applications cannot start if installed in a folder with non-ASCII characters in the folder name.

---

5 Use the same host name and port number that you used when installing SCAuto event processing.

6 Click **Install**.

7 Open the **scito.ini** file, which is located in the default installation location (**C:\Program Files\HP\HP SCAuto for OMW 1.3.1**):

   a Verify that the **scauto** entry specifies your Service Manager host and SCAuto port.

   b If desired, to limit the event types processed by the integration, add a line containing scevents.

   Following is an example of these entries:

```
scauto:vmamqa73.devlab.ad.12680
scevents:(pmo,pmu,pmc)
```

Modify Data Types Sent from OMW to Service Manager – Optional

1. In the Operations Manager management console, select **Policy Management** > **Policy Groups** > **Service Center** in the navigation tree.
2. Right-click the **Forward messages to Service Center** policy.
3. Select **All tasks** > **Deploy on**.
4. Select the OMW server node.
5. Select the **Enable** radio button and click **OK** to apply the changes.
6. Start the **HP SCAuto for OMW** service as follows:
   a. Open the Microsoft Windows Control Panel and click **Administrative Tools** > **Services**.
   b. Select the **HP SCAuto for OMW** service and click  .

Modify the Service Manager-OMW Messages Flow

In Service Manager version 7.10 and earlier, out of the box the incident information in SM is updated with changes in OMW messages. Each incident is closed when the message is acknowledged.

In Service Manager version 7.11 and later, the following changes must be made:

1. On the OMW machine, browse to the following directory:

   <SCAuto installation directory>\EventMap\ToSC

2. In the **eventmapSCfromOMW.tcl** file, search for eventObject set_evfield category example, and replace the word “example” with “incident”.
3. Save and close the updated file.
4. Stop and then restart the SCAuto service on that machine.

To set up the backwards flow of messages:

This procedure enables a message to be acknowledged in OMW when an incident is closed in Service Manager. This occurs by posting an event into the eventout table, where it is read by SCAuto and then fed as an update to OMW.

1 In the Service Manager console, select **Menu Navigation** > **Tailoring** > **Format Control**. The Format Control window opens.

2 Search for the **IM.template.close** form by entering this string in the **Name** field, and then click **Enter**.

3 Click the **Subroutines** button.

4 Right-click the open form and select **Show expanded form**. Scroll down to the bottom of the form and add a new subroutine. Enter the following information:

Field	Recommended Value	Description
Application Name	**axces.write**	The name of the application that runs during the subroutine.
Names/Values	**record/$file** **name/pmc**	The names and values of the subroutine's parameters.
Add	**true**	
Update	**true**	
Delete	**true**	
Error Message	**failed to execute pmc**	The error message that appears if the subroutine fails.

5 In the Format Control window, search for IM.template.update. In the Name field, replace pmc with pmu.

6 Save the changes to the Format Control window and restart the Service Manager service for the changes to take effect.

7 Verify that the **Process input events synchronously** field is disabled for events of pmo, pmu, and pmc types. To do this:

a Select **Menu Navigation** > **Tailoring** > **Event Services** > **Registration**.

b Enter pmo, pum, or pmc as the event code, and click **Search**.

Verify Service Manager-OMW Configuration

The following steps describe how to verify that you have configured Service Manager and OMW properly to perform the integration.

- "OMW > Service Manager Ticket Opening" on page 72
- "OMW > Service Manager Ticket Update" on page 73
- "OMW > Service Manager Ticket Close" on page 73
- "Service Manager > OMW Ticket Close" on page 74

OMW > Service Manager Ticket Opening

The following procedure triggers a message in OMW that matches the filter for forwarding to SM (default is severity Major/Critical).

1 On the OMW machine, open a command prompt and run the following command:

opcmsg a="Application Name" o="Object Value" msg_text="Testing SCAuto for OMW" severity=critical

2 The following occurs:

- A new critical message appears in the OMW management console.
- A new incident appears in Service Manager. The incident's description is the text of the message that appeared in the OMW management console.
- A Normal status message appears in the OMW management console, which contains the opened ticket number.

OMW > Service Manager Ticket Update

1 In the OMW management console, change the severity of the critical message that you created in the "OMW > Service Manager Ticket Opening" procedure.

2 The following occurs:

➤ In Service Manager, the **sysmodcount** value has increased by 1 for the specified incident.

Note: To view the sysmodcount value, do the following:

➤ Select **Menu Navigation** > **Incident Management** > **Incident Queue**.

➤ Select **Autoformat View** in the **View** drop-down list.

➤ Incident details are updated (for example, when you change the severity of a message, the incident's urgency and priority also change).

OMW > Service Manager Ticket Close

1 In the OMW management console, acknowledge the message that was created in the "OMW > Service Manager Ticket Opening" procedure.

2 The following occurs:

➤ The corresponding incident is closed in Service Manager.

➤ In the OMW console, a confirmation message with Normal status is received.

Service Manager > OMW Ticket Close

1 In Service Manager, close the incident ticket.

2 The following occurs:

- In OMW, the message that was created in the "OMW > Service Manager Ticket Opening" procedure is acknowledged.
- A confirmation message appears indicating that the incident was closed.

6

Service Manager – BAC Integration Configuration

This chapter includes:

***Concepts**

***Tasks**

Concepts

Overview

This section describes how to configure the Service Manager - BAC integration to show the number of incidents in BAC that are received from Service Manager.

Tasks

Set Up Service Manager for Integration with BAC

This task lists the steps necessary to configure Service Manager in order to perform integration with BAC.

This task includes the following steps:

Prerequisites

Make sure that the Service Manager web tier has been installed. For instructions, see the *HP Service Manager Installation Guide*.

Disable Query Security

1 Open Service Manager's **web.xml** file in a text editor.

Note: The file's location depends on the web container that you are using. In Tomcat, the location is **\Apache Software Foundation\Tomcat 5.5 \webapps\webtier-7.11\WEB- INF\web.xml**.

---

2 In the file, locate the **<!-- Specify the ServiceCenter server host and port location** --> section.

3 Verify that the following strings exists in that section:

```
<init-param>
   <param-name>querysecurity</param-name>
   <param-value>false</param-value>
</init-param>
```

4 Restart the Tomcat web container using the **Net stop tomcat** and **Net start tomcat** commands.

Load the Clocks .unl File

1 Type **db** in the command box and click  to execute the command.

2 Right-click in the right-hand pane and select **Import/Load** from the menu.

3 Click the **Browse** button next to the **File Name** field. Select the following file:

\\rubicon.mercury.co.il\BACIntegrations\ServiceManager\7.10\ BAC8.01_SM7\ Clocks_extaccess_sm702_10nov08.unl

4 Click **Load FG**. Be sure to acknowledge any message that appears.

5 Check the output window for errors.

Update the Clocks WSDL

1 Select **Menu Navigation** > **Tailoring** > **Web Services** > **WSDL Configuration**.

2 In the **Service Name** field, enter **Clocks** and click **Search**.

3 Select the Fields tab and add the following entry:

Field	Caption	Type
Total	temp	StringType

4 Click **Save** and then click **OK**.

5 Click **Search** again, select the Fields tab, and clear the entry that you just created.

6 Click **Save** and then click **OK**.

Add the Type Field to the logical.name Link Line

1 Log on to your Service Manager system as an administrator.

2 Select **Menu Navigation** > **Tailoring** > **Tailoring Tools** > **Links**.

3 In the **Name** field, enter **probsummary**, and click **Search**.

4 Right-click to the left of the line that contains **logical.name** in the **Source Field Name** field and select **Select Line** from the shortcut menu.

5 In an empty row, add **type** in both the **Source Field** and **Target Field** columns.

6 Click **Save**, then click **Back**, and then click **OK**.

Set Up BAC for Integration with Service Manager

This task lists the steps necessary to configure BAC in order to perform integration with Service Manager.

This task includes the following steps:

➤ "Create a Service Manager Monitor in SiteScope " on page 78

➤ "Specify the Service Manager Web Tier URL in the Infrastructure Settings " on page 80

Create a Service Manager Monitor in SiteScope

1 Select **Admin** > **System Availability Management**.

2 Select your SiteScope instance.

3 Click the **New** button and select **New Group**.

4 Enter a logical name and click **Save**.

5 Select the group that you just created.

6 Click the **New** button and select **New Monitor**. The **New Monitor** window appears.

7 In the available monitors list, select the HP Service Manager monitor.

8 Enter the following parameters in the HP Service Manager monitor window:

Name	Recommended Value	Description
Name	**<user defined>**	The logical name of the new monitor (for example, SM2BACNumberIncidents)
HP ServiceManager Web Service Endpoint	**http:\\<Service Manager machine>:<Service Manager port>/sc62server/PWS**	The location of the Service Manager's WSDL file (used for SiteScope connection to the Service Manager Web service).
Username	**<user defined>**	The username of the Service Manager account
Password	**<user defined>**	The password for the Service Manager account
Synch Flag (checkbox)	**Selected**	When this checkbox is selected, the first time the integration is run, a full synchronization of incidents is performed.
Synch Time	**<user defined>**	The time that is used as the baseline for synchronization, meaning that only the number of incidents from this specified time and later will be fetched.

Leave all other parameters as their default values.

9 Install JDK on the SiteScope machine.

Note: The **target_name** entry is case-sensitive.

---

10 Copy the **peregrine.jar** file from **C:\SiteScope\conf\ems\peregrine\lib\7.1x** to **C:\SiteScope\WEB-INF\lib**.

11 In a text editor, open the **incidentAttributesMapping.config** file, located in the **c:\SiteScope\conf\ems\peregrine** directory.

12 Locate the **target_name=configurationItem** entry and change it to **target_name=affectedItem**.

13 In a text editor, open the **build.properties** file.

- Set the **clocks.wsdl.url** value to **http://<Service Manager server>:<Service Manager port>/sc62server/PWS/Clocks?wsdl**.
- Set the **prob.wsdl.url** value to **http://<Service Manager server>:<Service Manager port>/sc62server/PWS/IncidentManagement?wsdl**.

14 Open a command prompt window and run **create-peregrine-jar.bat**.

Specify the Service Manager Web Tier URL in the Infrastructure Settings

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.

2 In the **Foundations** drop-down list, select **Integration with other applications**.

3 In the **HP ServiceCenter - Ticketing Integration** section, enter the Service Manager web tier URL, for example:

http://vmbto15.devlab.ad:8080/webtier-7.11/

Index

T

U

V

W