

HP Business Service Management

for the Windows and Linux operating systems

Software Version: 9.13

Upgrade Guide

Document Release Date: May 2012

Software Release Date: May 2012



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

© Copyright 2005 - 2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

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

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (**<http://www.apache.org>**).

This product includes software developed by the JDOM Project (**<http://www.jdom.org>**).

This product includes software developed by the MX4J project (**<http://mx4j.sourceforge.net>**).

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

Welcome to This Guide

Welcome to the HP Business Service Management Upgrade Guide. This guide introduces you to HP Business Service Management, provides information on getting started, describes server and component configuration and installation, and provides a high level upgrade workflow.

This chapter includes:

- How This Guide Is Organized on page 7
- Who Should Read This Guide on page 8
- Additional Online Resources on page 8
- Documentation Updates on page 9

How This Guide Is Organized

This guide contains the following parts:

Part I Upgrade Workflows

Provides high-level workflows that guide you through all the steps needed to upgrade HP Business Service Management. There are different flows depending on the original version of Business Availability Center as well as the type of upgrade you are performing.

Part II Deployment Planning

Provides an overview of platform deployment and describes the system requirements required for running the HP Business Service Management platform, as well as describing the components and their supported configurations.

Part III BSM Server Installation

Describes details about installing HP Business Service Management servers, configuring database parameters, installing component setup files, and uninstalling HP Business Service Management servers on Windows and Linux platforms.

Part IV HP Business Service Management Upgrade Information

Describes background information about changes that occur while upgrading HP Business Service Management servers.

Part V Post Deployment and Troubleshooting

Provides information on post-installation tasks, troubleshooting information, and information about enabling and logging in to the HP Business Service Management servers.

Who Should Read This Guide

This guide is intended HP Business Service Management administrators responsible for upgrading HP Business Service Management.

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/hpsupport.

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.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (<http://h20230.www2.hp.com/selfsolve/manuals>).

Welcome to This Guide

Table of Contents

Welcome to This Guide	7
How This Guide Is Organized	7
Who Should Read This Guide	8
Additional Online Resources.....	8
Documentation Updates	9

PART I: UPGRADE WORKFLOWS

Chapter 1: Upgrading to BSM 9.1x - Workflows	19
Upgrade Types	19
Upgrading from BAC 7.5x and 8.x - Workflow	21
Upgrading from BSM 9.0x - Workflow	28
Upgrading from BSM 9.1x - Workflow	35
Chapter 2: Detailed Procedures Required When	
Performing Upgrade Workflows	37
Upgrading from BAC 7.5x to BAC 8.0	37
Upgrading BAC 8.x to BSM 9.1x - Staging	40
Upgrading BAC 8.x to BSM 9.1x - Direct	43
Chapter 3: Service Packs and Patches.....	47
Service Pack Installation Overview	47
Installing the BSM 9.1x Service Pack - Standard	48
Installing the BSM 9.1x Service Pack - with Workaround	
to Resolve Modeling Related Issues	52
Uninstalling a Service Pack (Rolling Back).....	61
Patch Installation	63

Chapter 4: Staging Data Replicator	65
Staging Data Replicator - Overview.....	65
Running the Staging Data Replicator (Embedded)	66
Running the Staging Data Replicator (Standalone)	67
Verifying that the SDR Server Can Communicate with the Production Server.....	70
Unsubscribing the Staging Data Replicator from the Source Server.....	71
Running the SDR with Basic Authentication.....	72
SSL Configuration for the Staging Data Replicator.....	73

PART II: DEPLOYMENT PLANNING

Chapter 5: Deployment Planning	77
Deployment Planning Checklist.....	78
Deployment Planning Considerations.....	79
Using the Capacity Calculator	83
Chapter 6: Understanding the Platform and Components.....	87
Platform Architecture Diagram	88
BSM Servers	89
BSM Database Server	92
BSM Data Sources	93
Additional Proprietary Components.....	96
Third-Party Components	97
Bus Communication Among BSM Components	98
Chapter 7: High Availability for BSM	101
Overview of High Availability Options.....	101
Load Balancing for the Gateway Server	102
High Availability for the Gateway Server.....	105
High Availability for the Data Processing Server	107
Configuring BSM Data Collectors in a Distributed Environment.....	121
Troubleshooting	122
Chapter 8: Deployment Configurations	123
One-Machine Deployment	123
Distributed Deployment	124
Load Balancing and High Availability	125
APM Starter Deployment	128

Chapter 9: System Requirements	131
HP Business Service Management Servers.....	132
HP Business Service Management Databases	135
Client Requirements for Viewing BSM	139
Server Environment Settings.....	142
HP Business Service Management on Virtual Platforms.....	143
BSM-CMS Synchronization and Content Pack Information	143

PART III: BSM SERVER INSTALLATION

Chapter 10: Installing BSM Servers on a Windows Platform	147
Overview of BSM Server Installation.....	148
Preparing Information Required for Installation	149
Installation Prerequisites	151
Working with the Web Server.....	152
Installing HP Business Service Management Servers	154
Chapter 11: Installing BSM Servers on a Linux Platform	159
Overview of BSM Server Installation.....	159
Preparing Information Required for Installation	160
Installation Prerequisites	161
Working with the Web Server.....	162
Installing HP Business Service Management Servers	163
Chapter 12: Server Deployment and Setting	
Database Parameters	167
Setup and Database Configuration Utility Overview	168
Setting Database Parameters.....	169
Required Information for Setting Database Parameters.....	171
Running the Setup and Database Configuration Utility	175
Chapter 13: Upgrade Wizard	181
Upgrade Wizard Overview	181
Preparing Information for the Upgrade Wizard	182
Tracking the Configuration Upgrade Progress.....	183
Chapter 14: Installing Component Setup Files	187
Overview of Installing Component Setup Files	187
Installing Component Setup Files.....	188
Chapter 15: Uninstalling BSM Servers	191
Complete Uninstall	191

PART IV: HP BUSINESS SERVICE MANAGEMENT UPGRADE INFORMATION

Chapter 16: Upgrading BSM with Operations Manager i (OMi) 197
 OMi Upgrade Information 198
 OMi 8.10 to 9.1x Pre-Upgrade Procedure 200
 OMi 8.10 to 9.1x Mid-Upgrade Procedure 210
 OMi 8.10 to 9.1x Post-Upgrade Procedure 225
 OMi 9.0x to 9.1x Pre-Upgrade Procedure 234
 OMi 9.0x to 9.1x Post-Upgrade Procedure 239

Chapter 17: Platform Upgrade Information 243
 Recipient Management Upgrade 243
 Downtime Upgrade 243
 User Management Upgrade 244
 Locations Updates 244
 Database Native Partitioning 247

Chapter 18: Reports Upgrade Information 249
 Custom Query Builder Upgrade 249
 Custom Reports and Favorite Filters 251

Chapter 19: Dashboard and My BSM Upgrade Information 257
 What's Changed? 258
 Custom Rules 261
 KPI Upgrade 262
 CI Status Alerts Upgrade 268
 SiteScope and EMS KPI Assignment Upgrade 270
 SiteScope KPI Assignments Associated With Custom KPIs 275
 Propagation Rule Upgrade 276
 Repositories Upgrade 277
 View Upgrade and Monitor Removal 278
 SiteScope Monitors Associated with Non-default
 CIs or Multiple CIs 282
 My BSM Upgrade 286

Chapter 20: Alerts Upgrade Information 287
 Infrastructure Settings 288
 General Information 290
 CI-Based Alerts 290
 Notification Template Upgrade 290
 Alert Permissions Upgrade 291
 Event-Based Alerts 291
 CI Status and SLA Alerts Upgrade 306
 Upgrade of Downtime for Alerts 308

Chapter 21: SOA, SAP, and Siebel Solutions	
Upgrade Information	309
Upgrade Application Management for SOA	309
Upgrade Application Management for SAP and Application Management for Siebel	311
Chapter 22: Service Level Management Upgrade Information	313
What's Changed?	314
What Happens to BSM 8.x SLAs in 9.x?.....	317
Converting 8.x SLAs to the BSM 9.x Format.....	318
Examples of SLA Conversion	322
SLA Conversion Settings	338
Chapter 23: End User Management Upgrade Information	347
Upgrade - Overview	348
Pre Upgrade Actions	349
Business Process Monitor Upgrade.....	350
Real User Monitor Upgrade.....	359
EUM Alerts Upgrade	373
CI Links Upgrade	373
Views Upgrade.....	373
Deleted CIs	377
Permissions Upgrade	379
EUM Reports Upgrade	380
Post Upgrade Actions	393
Chapter 24: SiteScope and System Availability	
Management Upgrade Information	397
SiteScope and System Availability Management Upgrader	397
Chapter 25: Upgrading Business Process Insight	403
What Changed For BPI From 8.x to 9.x.....	403
Upgrading BPI Overview	405
Upgrade Notes	406
Tasks to Complete Before Starting the BPI Server Upgrade	407
Upgrading BPI From 8.x to 9.10.....	410
Upgrading BPI From 9.10 to 9.12.....	422

Chapter 26: BAC Integrations Upgrade Information	427
HP Universal CMDB (embedded/external)	
Upgrade Information	427
Upgrading HP Universal CMDB	
Integration - Splitting Procedure	430
NNMi Upgrade Information	433
Migrating Modified UCMDB Integration (Federation) Adapters.....	434
Upgrade of the Integration of HP Operations Orchestration	434
Upgrade EMS Integrations.....	435
RTSM Upgrade Limitations	435
Chapter 27: Upgrade Diagnostics	437
Diagnostics Considerations When Upgrading BAC to 9.1x	437
Chapter 28: Upgrading TransactionVision	441
Upgrade Compatibility.....	441
What Changed for TransactionVision	442
Upgrading TransactionVision Overview.....	443

PART V: POST DEPLOYMENT AND TROUBLESHOOTING

Chapter 29: Post-Deployment	447
Starting and Stopping BSM	447
Logging In	448
Logging Out.....	450
Post-Installation Tasks.....	450
Chapter 30: Changing BSM Service Users	455
Changing the BSM Service User	455
Chapter 31: Troubleshooting	457
Troubleshooting Resources	457
Troubleshooting the Upgrade Process	458
Installation and Connectivity Troubleshooting	465

Part I

Upgrade Workflows

1

Upgrading to BSM 9.1x - Workflows

This chapter provides the workflows for upgrading your BAC or BSM environment to BSM 9.1x. For help planning your upgrade or for technical assistance, contact HP Software Support.

This chapter includes:

- Upgrade Types on page 19
- Upgrading from BAC 7.5x and 8.x - Workflow on page 21
- Upgrading from BSM 9.0x - Workflow on page 28
- Upgrading from BSM 9.1x - Workflow on page 35

Upgrade Types

There are two upgrade types: staging and direct.

Note: If your source and target environments are not running the same operating systems, you must upgrade using the staging method.

Staging

Using a **staging** environment to upgrade BSM refers to installing the new software on different machines and database schemas (referred to as the staging environment) to allow the original BAC or BSM servers to continue functioning while the upgrade is in process. The original machines are referred to as the production environment. This minimizes downtime and allows you to ensure that the new server(s) are functioning as desired before disconnecting the original server(s).

When upgrading using a staging environment, BSM is installed on the staging servers and then the wizard activates the Staging Data Replicator (SDR). This listens to the samples (data) coming in to the original server and passes them to the staging server. The SDR replicates only data samples and not configuration changes made within the databases. Therefore, any configuration changes made to the production server from the start of the SDR will not be transferred to the staging environment. For more information, see "Staging Data Replicator" on page 65.

Note: All BSM machines in the staging environment must be set to the same time zone as the source environment. Incompatible time zone settings can lead to inaccuracies in reporting historical data.

Direct

Upgrading **directly** refers to installing the new version on the same servers and database schemas as the original version. This can only be performed after uninstalling the original version and therefore results in greater downtime.

Upgrading from BAC 7.5x and 8.x - Workflow

This section provides the workflow for upgrading to BSM 9.1x from BAC 7.5x and 8.x. This procedure is also available in interactive format in the *Upgrade Workflows - Interactive Guide* from the documentation library home page. For additional information including the latest updates, refer to the latest BSM release notes.

1 Create deployment plan

Create a complete deployment plan including the required software, hardware, and components. Use the following documentation to guide you through the process of planning a deployment:

- Getting Started with BSM Guide
- "Deployment Planning" on page 77
- "Understanding the Platform and Components" on page 87
- "High Availability for BSM" on page 101
- "Deployment Configurations" on page 123
- "System Requirements" on page 131

2 Create upgrade plan

- **Upgrade Type.** There are two basic types of upgrades: staging and direct. Staging upgrades require more hardware, but result in less downtime. Direct upgrades require no additional hardware, but result in more downtime. For more information, see "Upgrade Types" on page 19.
- **Staging Data Replicator.** The Staging Data Replicator (SDR) listens to the samples (data) coming in to the original server and passes them to the staging server. If you need to run the Staging Data Replicator (SDR) on an external server, you will need an additional server to run the SDR during staging mode. For more information, see "Staging Data Replicator" on page 65.

- **Integrations.** There are a number of integrations with other products that can affect the upgrade procedure.

Product	Details
Operations Orchestration (OO)	If you were using OO with BAC 8.x, you must upgrade to OO 7.51 or later. For more information, see the support matrix.
Service Manager (SM)	If you had integration between SM and BAC 8.x via HP Universal CMDB, follow the instructions in the HP Universal CMDB upgrade procedures. For details, see "Upgrading HP Universal CMDB Integration - Splitting Procedure" on page 430.
CLIP	For information about upgrading an integration with HP CLIP 1.5, contact HP Software Support.
HP Universal CMDB	For information about upgrading HP Universal CMDB and products that integrate with it, see "HP Universal CMDB (embedded/external) Upgrade Information" on page 427.
Network Node Manager i (NNMi)	You can continue to use BSM 9.1x without upgrading your integration with NNMi. If you choose to upgrade to NNMi 9.x, there are optional upgrades to this integration. For more information, see "NNMi Upgrade Information" on page 433

- **Documentation.** The following documents are referenced in the upgrade procedures and may be needed during the upgrade process. They are all included in the BSM Documentation Library.
 - Database Guide
 - Platform Administration
 - Solutions and Integrations
 - Business Process Monitor Administration
 - Real User Monitor Administration
 - Using System Availability Management
 - Hardening Guide

3 Order and register licenses

Order licenses with a sales representative based on your deployment plan. Register your copy of HP Business Service Management to gain access to technical support and information on all HP products. You will also be eligible for updates and upgrades. You can register your copy of HP Business Service Management on the HP Software Support site (<http://www.hp.com/go/hpsoftwaresupport>).

4 Set up hardware

Set up your BSM servers and your BSM database server. Verify that your database has the following settings:

- ▶ Oracle: the Oracle Partitioning option must be enabled.
- ▶ SQL: The Compatibility Level database setting must be higher than 90 (SQL Server 2005 and higher). If you are upgrading with a staging environment, the collation must be identical in both the production and staging environments.

For information about setting up your database server, see the *HP Business Service Management Database Guide* PDF.

5 Review relevant information

Review relevant information describing changes from BAC 8.x to BSM 9.1x. Depending on your BSM configuration, review the relevant upgrade chapters Upgrade Information part below. For details, see "HP Business Service Management Upgrade Information" on page 195.

6 Upgrade to BAC 8.0

If you are using BAC 7.5x, upgrade to BAC 7.55, and then to BAC 8.0x before upgrading to BSM 9.1x. You can perform this upgrade in staging or direct mode. You do not need to complete the entire 7.55-8.x upgrade process. For details, see "Upgrading from BAC 7.5x to BAC 8.0" on page 37.

7 Install BAC 8.0x service packs

We recommend installing the latest service pack on the BAC 8.0x servers. You must install at least service pack 8.06 or higher before continuing with the upgrade. For details, see the Service Pack release notes.

8 Run pre-upgrade tool

Run the pre-upgrade tool to view a customized list of items that may need attention before starting the upgrade. For details, see the BSM 8.07 Pre-Upgrade Tool Guide pdf. This guide can be found in your BSM 8.07 installation package or in the HP Software Product Manuals website (<http://h20230.www2.hp.com/selfsolve/manuals>).

9 Upgrade External HP Universal CMDB

If you have an external HP Universal CMDB, upgrade it to version 8.06 or later so that it will be compatible with your version of BAC.

10 Import DDM Content Pack 8

You must have DDM Content Pack 8 before continuing with the upgrade. If you are working with an external HP Universal CMDB, this should be done on the external HP Universal CMDB server. If not, this is done on the BSM server. Download the content pack, along with instructions about how to install it from <https://hpln.hp.com/group/content-packs-ddm>.

11 Pre-upgrade procedures

Perform the following procedures depending on your applications:

- ▶ **Windows 2008 Server.** If you are installing BSM on Windows 2008 server, disable User Access Control.
- ▶ **OMi (Operations Manager i).** If you are migrating OMi from BAC 8.x to BSM 9.1x, perform the pre-upgrade procedures specified in "OMi 8.10 to 9.1x Pre-Upgrade Procedure" on page 200.
- ▶ **EUM.**
 - ▶ Ensure that all necessary Session Identification configurations do not have empty session ID values. Those with empty session ID values are not upgraded.
 - ▶ Check-in all BPM scripts to the Script Repository. The upgrade process does not preserve the checked-out status of scripts.
- ▶ **RTSM.** If you have custom integration adapters or if you modified out-of-the-box adapters, you will need to manually migrate these to BSM 9.1x. For details, see "Migrating Modified UCMDDB Integration (Federation) Adapters" on page 434.
- ▶ **Service Health and SLM.** If you created custom Java rules, custom rule .jar files, or custom Groovy rule files in pre-9.0 versions of BAC, contact HP Support for instructions on modifying and packaging them for BSM 9.x before upgrading. For details, see "Custom Rules" on page 261.

- ▶ **Manual Changes to Conf Directory.** If you made changes to any files in the <HP BSM root directory>\WebServer\conf directory, back up the changed files and, after the upgrade, reapply the changes to the new files (**do not copy the old files on top of the new ones**).
- ▶ **Content Packs.** Make sure your content packs are compatible with your version of HP Universal CMDB. Incompatibilities can cause problems during the upgrade. For example, installing Content Pack 9 with HP Universal CMDB 8.x could result in problems during the upgrade procedure.

12 Upgrade to 9.1x

This procedure varies depending on whether you are performing a staging or direct upgrade to 9.1x. Select the appropriate procedure:

- ▶ "Upgrading BAC 8.x to BSM 9.1x - Staging" on page 40
- ▶ "Upgrading BAC 8.x to BSM 9.1x - Direct" on page 43

13 Modify the product_name_enum

If you are planning to use Operations Manager *i*, perform the following steps:

- a** Go to **Admin > RTSM Administration > Modeling > CI Type Manager**.
- b** From the CI Types list select **System Type Manager**.
- c** Select **product_name_enum** and click **Edit**.
- d** Type **lync_server** and click **Add**.
- e** Click **OK**.

14 Restore BSM Service Changes

If you manually configured different users to run BSM services, these settings must be configured again. For details, see "Changing BSM Service Users" on page 455.

15 Perform hardening procedure

If your original environment was secured with SSL, you need to re-establish the trust to the certificate authority that issued server certificates for the BSM virtual servers. Additionally, you may need to repeat other hardening procedures. We recommend performing the hardening procedures again. For details, see the *HP Business Service Management Hardening Guide* PDF.

16 Upgrade components

We recommend that you update all components associated with BSM.

- ▶ **Sitescope.** If you are using SiteScope with BSM, we recommend upgrading to the latest supported version of SiteScope. For information about how to upgrade SiteScope, see the SiteScope Deployment Guide available from the BSM Documentation Library.
- ▶ **BPI.** For information about upgrading your Business Process Insight component along with the BSM upgrade, see "Upgrading Business Process Insight" on page 403.
- ▶ **RUM and BPM.** RUM and BPM must be upgraded after the BSM 9.1x upgrade. For information about upgrading these components, see "End User Management Upgrade Information" on page 347. For further details, see the RUM 9.1x release notes.
- ▶ **HP Diagnostics.** We recommend upgrading this component to the latest supported version. For details, see the support matrixes in the BSM release notes.
- ▶ **Data Flow Probe.** We recommend upgrading this component to the latest supported version. For details, see the support matrixes in the BSM release notes.

- ▶ **TransactionVision.** We recommend upgrading this component to the latest supported version. For details, see the support matrixes in the BSM release notes.

Upgrading from BSM 9.0x - Workflow

This section provides the workflow for upgrading to BSM 9.1x from BSM 9.0x. This procedure is also available in interactive format in the *Upgrade Workflows - Interactive Guide* from the documentation library home page. For additional information including the latest updates, refer to the latest BSM release notes.

1 Disable BSM 9.0x

Disable the BSM server(s) by selecting **Start > Programs > HP Business Service Management > Administration > Disable HP Business Service Management.**

2 Verify database settings

If you are using an Oracle database, make sure that the parameter **RECYCLEBIN** is set to **Off**, as specified in the *HP Business Service Management Database Guide* PDF.

3 Back up database schema (recommended)

We recommend backing up the database schema as close as possible to the uninstall to minimize the risk of data loss.

Note: If you have added any custom SiteScope monitors in SAM Admin > Metrics and Indicators, you must manually back up the following file and restore it to the same location after BSM 9.1x is installed (before configuring the management database schema)
HPBSM\AppServer\webapps\site.war\WEB-INF\sam\hi-mapping-monitors.xml.

4 Back up certificate authority configurations

Note: These steps are subject to change. Check the latest release notes for any updates.

In order to preserve your certificate authority configuration, you must back up the data before BSM 9.0x is uninstalled and restore it after the upgrade. This procedure is only required if you are using one or more of the following components:

- HP Diagnostics
- SiteScope
- Integration Adapter
- HPOM
- OMi
- NNMi

To save the certificate authority configurations, run the following commands on the Data Processing Server. Note that these are lists of commands that must be run one line at a time:

For Windows:

```
ovcm -exportcacert -file %TEMP%\migration\oldca.p12
ovcert -exporttrusted -file %TEMP%\migration\oldtrust.pem
ovcert -exportcert -file %TEMP%\migration\oldcert.p12
ovcoreid > %TEMP%\migration\oldcoreid
```

For Linux:

```
ovcm -exportcacert -file /tmp/migration/oldca.p12
ovcert -exporttrusted -file /tmp/migration/oldtrust.pem
ovcert -exportcert -file /tmp/migration/oldcert.p12
ovcoreid > /tmp/migration/oldcoreid
```

5 OMi (Operations Manager i) pre-upgrade procedure

If you are migrating OMi from 9.0 to 9.1x, see "OMi 9.0x to 9.1x Pre-Upgrade Procedure" on page 234.

6 Uninstall BSM 9.0x

Uninstall BSM 9.0x on all BSM servers. For task details, see "Uninstalling BSM Servers" on page 191.

7 Install BSM 9.10

If you have a distributed deployment, run the wizards on the Data Processing Server first. The wizards will tell you when to begin installation on the Gateway Server.

a Run the installation and post-installation wizards.

- For details about installing on a Windows platform, see "Installing BSM Servers on a Windows Platform" on page 147.
- For details about installing on a Linux platform, see "Installing BSM Servers on a Linux Platform" on page 159.

b Restore certificate authority configurations. If you backed up your certificate authority configurations in step 4, perform the following procedure (depending on your operating system) on the Data Processing Server:

- "Restoring certificate authority configurations for Windows users" on page 33
- "Restoring certificate authority configurations for Linux users" on page 35

c Perform the post-installation tasks. For more information, see "Post-Installation Tasks" on page 450.

8 Install the latest BSM 9.1x Service Pack

Perform the standard procedure for installing the BSM 9.1x service pack. For details, see "Installing the BSM 9.1x Service Pack - Standard" on page 48.

9 Run the upgrade wizard

Disable all BSM servers and run the upgrade wizard. For more details, see "Upgrade Wizard Overview" on page 181. If you have more than one Data Processing or Gateway Server, run the upgrade wizards on one of each type of server only. For each additional Data Processing and Gateway Server, run the the Setup and Database Configuration Utility. For more details, see "Setup and Database Configuration Utility Overview" on page 168.

10 Enable servers and log in

For more information, see "Starting and Stopping BSM" on page 447 and "Logging In" on page 448.

11 Modify the product_name_enum

If you are planning to use Operations Manager *i*, perform the following steps:

- a** Go to **Admin > RTSM Administration > Modeling > CI Type Manager**.
- b** From the CI Types list select **System Type Manager**.
- c** Select **product_name_enum** and click **Edit**.
- d** Type **lync_server** and click **Add**.
- e** Click **OK**.

12 Perform hardening procedure

If your original environment was secured with SSL, you need to re-establish the trust to the certificate authority that issued server certificates for the BSM virtual servers. Additionally, you may need to repeat other hardening procedures. We recommend performing the hardening procedures again. For details, see the *HP Business Service Management Hardening Guide* PDF.

13 Complete content pack upload

After starting BSM, wait for the content pack upload to finish. Check the file `<HPBSM Install Directory>/log/EJBContainer/opr-admin.log` for an entry like the following:

```
2011-05-06 10:21:19,431 [BackgroundThreadManager Thread (BG#1)] INFO
ContentPackImportService.invoke(?) - OOTB Content Packs import finished in 283.542
seconds.
```

14 OMi (Operations Manager i) post-upgrade procedure

If you are migrating OMi from 9.0 to 9.1x, see "OMi 9.0x to 9.1x Post-Upgrade Procedure" on page 239.

15 Service Health and SLM post-upgrade procedure

When you installed BSM 9.x, content that was imported using out-of-the-box content packs was categorized in the Service Health and SLM repositories as **Custom** or **Predefined (Custom)**, rather than as **Predefined**.

After you install BSM 9.13, run the Repository Data Transfer tool to automatically re-label this out-of-the-box content in the repositories as **Predefined**, using the following steps:

- a** Access the JMX console on the Gateway Server via `http://<Gateway Server name>:8080/jmx-console`, and enter the user name and password.
- b** Click **service=content-manager** in the Topaz section.
- c** Locate the **invokeRepositoryTool()** operation.
- d** Click **Invoke**.

Note: If you have customized any repository items, they are not affected by this procedure.

16 Upload content packs

Wait for the BSM services to be started again and then upload the content packs again. Execute the following command on the Gateway Server:

```
<HPBSM Install Directory>/opr/bin/ContentManager -username admin -password admin -a -forceReload
```

17 Restore BSM Service Changes

If you manually configured different users to run BSM services, these settings must be configured again. For details, see "Changing BSM Service Users" on page 455.

18 ETI display label

If you have alerts configured with an Event Template, the ETI display label needs to be manually upgraded. To upgrade the display label, execute the following JMX command from the BSM 9.1x Data Processing Server:

```
BAC.Alerts.Upgrade service=change Eti name to ID update()
```

Restoring certificate authority configurations for Windows users

To restore the certificate authority configurations that you backed up in step 4 run the following commands on the Data Processing Server:

1 ovcoreid

This produces a value which is referred to below as <newcoreid>. Note this value for future use.

2 type %TEMP%\migration\oldcoreid

This produces a value which is referred to below as **<oldcoreid>**. Note this value for future use.

3 `ovcert -remove <newcoreid>`

4 `ovcert -remove <newcoreid> -ovrg server`

5 `ovcoreid -set <oldcoreid> -ovrg server -force`

6 `ovcm -importcacert -file %TEMP%\migration\oldca.p12`

7 `ovcert -remove CA_<newcoreid>`

Make sure there are no spaces between CA_ and the value of the <newcoreid>.

8 `ovcert -remove CA_<newcoreid> -ovrg server`

Make sure there are no spaces between CA_ and the value of the <newcoreid>.

9 `ovcert -importcert -file %TEMP%\migration\oldcert.p12 -ovrg server`

Ignore any warning message while running this command.

10 `ovcm -issue -file %TEMP%\migration\newcert.p12 -name <newcoreid> -coreid <newcoreid>`

11 `ovcert -importcert -file %TEMP%\migration\newcert.p12`

12 `ovcert -importtrusted -file %TEMP%\migration\oldtrust.pem`

Ignore any warning message while running this command.

13 `ovcert -importtrusted -file %TEMP%\migration\oldtrust.pem -ovrg server`

Ignore any warning message while running this command.

14 `ovc -kill`

15 `ovc -start`

Restoring certificate authority configurations for Linux users

To restore the certificate authority configurations that you backed up in step 4 run the following commands on the Data Processing Server:

- 1** `ovcert -remove `ovcoreid``
- 2** `ovcert -remove `ovcoreid` -ovrg server`
- 3** `ovcoreid -set `cat /tmp/migration/oldcoreid` -ovrg server -force`
- 4** `ovcm -importcacert -file /tmp/migration/oldca.p12`
- 5** `ovcert -remove CA_`ovcoreid``
- 6** `ovcert -remove CA_`ovcoreid` -ovrg server`
- 7** `ovcert -importcert -file /tmp/migration/oldcert.p12 -ovrg server`
Ignore any warning message while running this command.
- 8** `ovcm -issue -file /tmp/migration/newcert.p12 -name `ovcoreid` -coreid `ovcoreid``
- 9** `ovcert -importcert -file /tmp/migration/newcert.p12`
- 10** `ovcert -importtrusted -file /tmp/migration/oldtrust.pem`
Ignore any warning message while running this command.
- 11** `ovcert -importtrusted -file /tmp/migration/oldtrust.pem -ovrg server`
Ignore any warning message while running this command.
- 12** `ovc -kill`
- 13** `ovc -start`

Upgrading from BSM 9.1x - Workflow

The information for upgrading from BSM 9.1x to the latest service pack can be found in Chapter 3, "Service Packs and Patches".

2

Detailed Procedures Required When Performing Upgrade Workflows

This chapter provides detailed procedures that are required when performing the workflows listed in the Workflows for Upgrading to BSM 9.1x chapter. Perform only the procedures that are relevant to the workflow you are using.

This chapter includes:

- Upgrading from BAC 7.5x to BAC 8.0 on page 37
- Upgrading BAC 8.x to BSM 9.1x - Staging on page 40
- Upgrading BAC 8.x to BSM 9.1x - Direct on page 43

Upgrading from BAC 7.5x to BAC 8.0

This procedure is performed as part of the workflow "Upgrading from BAC 7.5x and 8.x - Workflow" on page 21. Perform the steps in this procedure only at the point in the workflow where you are instructed to do so.

Note: This upgrade is only supported starting with version BAC 7.55 and later.

This upgrade can be performed in four ways: staging-direct, direct-direct, staging-staging, and direct staging. The three factors in determining which method is recommended for your environment are the source operating system, the target operating system, and whether you want to upgrade using the staging or direct method. Use the following table to determine your recommended upgrade path.

		Target Environment		
		Preferred Upgrade Method	Linux	Windows
Source Environment	Solaris	Staging	Staging-Staging	Staging-Direct
		Direct	Direct-Staging	Direct-Staging
	Windows	Staging	Staging-Staging	Staging-Direct
		Direct	Direct-Staging	Direct-Direct

Note: If you are migrating to a different operating system in 9.1x (for example, BAC 7.5x was running on Windows and BSM 9.1x will be running on Linux), you must perform use the staging-staging method.

Staging-Direct Method

This method involves upgrading to 8.x in staging mode, upgrading the 8.x servers to 9.1x in direct mode, and then moving the 9.1x servers to production. It requires one extra set of BSM servers.

Note: All BSM machines in the staging environment must be set to the same time zone as the source environment. Incompatible time zone settings can lead to inaccuracies in reporting historical data.

To perform the staging-direct upgrade:

Upgrade your BAC 7.5x environment to BAC 8.x in staging mode by following the instructions in the Upgrade section of the *BAC 8.0 Deployment Guide*. This guide is included in the BAC 8.0 DVD. In the upgrade wizard, skip the SDR and Data Import/Export steps, but make sure that you reach the end of the wizard. Also, do not move the new servers to production mode or perform any post-installation tasks specified in the 8.x documentation. Maintain the original 7.5x servers in production mode.

Continue with step 7 in the main upgrade procedure, "Upgrading from BAC 7.5x and 8.x - Workflow" on page 21.

Direct-Direct Method

This method involves upgrading to 8.x directly, and then upgrading to 9.1x directly. It does not require any additional BSM servers.

To perform the direct-direct upgrade:

Upgrade your BAC 7.5 environment to BAC 8.x directly by following the instructions in the Upgrade section of the *BAC 8.0 Deployment Guide*. This guide is included in the BAC 8.0 DVD.

Continue with step 7 in the main upgrade procedure, "Upgrading from BAC 7.5x and 8.x - Workflow" on page 21.

Staging-Staging Method

This method involves upgrading to 8.x in staging mode, and then upgrading to 9.1x in staging mode as well. After both staging processes are complete, you move the 9.1x servers to production. It requires two extra sets of BSM servers. This method should only be used if you are migrating to a different operating system in 9.1x (for example, BAC 7.5 was running on Windows and BSM 9.1x will be running on Linux).

Note: All BSM machines in the staging environment must be set to the same time zone as the source environment. Incompatible time zone settings can lead to inaccuracies in reporting historical data.

To perform the staging-staging upgrade:

Upgrade your BAC 7.5 environment to BAC 8.x in staging mode by following the instructions in the Upgrade section of the *BAC 8.0 Deployment Guide*. This guide is included in the BAC 8.0 DVD. However, in the upgrade wizard, do not move the new servers to production mode or perform any post-installation tasks specified in the 8.x documentation. Maintain the original 7.5x servers in production mode.

Continue with step 7 in the main upgrade procedure, "Upgrading from BAC 7.5x and 8.x - Workflow" on page 21.

Upgrading BAC 8.x to BSM 9.1x - Staging

This procedure is performed as part of the workflow "Upgrading from BAC 7.5x and 8.x - Workflow" on page 21. Perform the steps in this procedure only at the point in the workflow where you are instructed to do so.

1 Prerequisites

All BSM machines in the staging environment must be set to the same time zone as the source environment. Incompatible time zone settings can lead to inaccuracies in reporting historical data.

2 Install BSM 9.10 on staging server(s)

If you have a distributed deployment, run the wizards on the Data Processing Server first. The wizards will direct when to begin running the wizards on the Gateway Server.

a Run the installation and post-installation wizards.

Important: If you are upgrading from 7.5 using the staging-staging method, at the end of the post-installation wizard, specify that you are upgrading from **8.x**, not **7.5**.

- For details about installing on a Windows platform, see "Installing BSM Servers on a Windows Platform" on page 147.
- For details about installing on a Linux platform, see "Installing BSM Servers on a Linux Platform" on page 159.

- b Perform the post-installation tasks.** For more information, see "Post-Installation Tasks" on page 450.
- c OMi (Operations Manager i).** If you are migrating OMi from BAC 8.0x to BSM 9.1x, perform the procedures specified in "OMi 8.10 to 9.1x Mid-Upgrade Procedure" on page 210.

3 Install the latest BSM 9.1x Service Pack

Perform the standard procedure for installing the BSM 9.1x service pack. For details, see "Installing the BSM 9.1x Service Pack - Standard" on page 48.

4 Run the Upgrade Wizard

For background information and further details, see "Upgrade Wizard Overview" on page 181.

- **Disable BSM servers.** Disable all BSM servers before running the upgrade wizard.
- **Multiple servers.** If you have more than one Data Processing or Gateway Server, run the upgrade wizards on one of each type of server only. For each additional Data Processing and Gateway Server, run the Setup and Database Configuration Utility. For more details, see "Setup and Database Configuration Utility Overview" on page 168.
- **Disable IDM-SSO.** In the Upgrade Wizard, after the data from the management database has been transferred to the new system, disable IDM-SSO on the new environment. To do so, log into the JMX console (<http://<Gateway Server name>:8080/jmx-console>) and search for the SSO service (service=SSO). Locate the **setSingleSignOnMode** operation and in the **ParamValue** box, type **Lightweight**. Click **Invoke**.

Staging. Staging mode begins at the end of the upgrade wizard. During staging mode, the staging servers should be verified and configured as desired before moving them to production mode. For more information, see "Upgrade Types" on page 19.

5 Post-upgrade procedures

Perform the following procedures if you have these components.

- ▶ **OMi (Operations Manager i).** If you are migrating OMi from BAC 8.x to BSM 9.1x, perform the post-upgrade procedures specified in "OMi 8.10 to 9.1x Post-Upgrade Procedure" on page 225.
- ▶ **EUM.** For BPM profiles upgraded to applications, manually reconfigure the correct time zones. A configuration file was used to map time zone offsets (used by the old model) and time zone IDs (used by the new model). The first time zone ID that matched the time zone offset was used.

6 Exit staging mode

When you are confident that you are ready to use your staging servers as your production environment, perform the following tasks:

- a** Transfer the data collectors to the new server(s) by setting the Load Balancer(s) to communicate with the new servers. If you are not using Load Balancers, you must configure each data collector individually to communicate with the new server(s).
- b** End the SDR and unsubscribe it from the source server. For details, see "Staging Data Replicator" on page 65.

7 Disable evaluation mode

In the new BSM server(s), log in and select **Admin > Platform > Infrastructure Settings > Foundations > Platform Administration**. In the **HP BSM Evaluation** table, set **Enable Evaluation Mode** and **Enable Evaluation Mode for Customer** to **false**.

8 Continue with main upgrade procedure

Continue with step 13 on page 24 in the main upgrade procedure.

Upgrading BAC 8.x to BSM 9.1x - Direct

This procedure is performed as part of the workflow "Upgrading from BAC 7.5x and 8.x - Workflow" on page 21. Perform the steps in this procedure only at the point in the workflow where you are instructed to do so.

1 Back up database schemas (recommended)

We recommend backing up the database schemas as close as possible to the 8.0x uninstall to minimize the risk of data loss.

2 Back up LDAP database

Manually copy the LDAP database from the original BAC Gateway Server. The upgrade wizard will instruct you when and how to restore the LDAP database.

- a** Open the Nanny Manager management console on the production Gateway Server that is running the LDAP by using the url **http://localhost:11021**.
- b** Invoke the stopService method with **ldap** as the serviceName parameter value.
- c** Verify that the slapd process is not running. Wait until the process is stopped before proceeding.
- d** Back up the bdb folder from the **<Gateway Server installation directory>\openldap** directory in the original BAC Gateway Server. Note the folder structure. You will need to eventually restore this folder using the same structure.

3 Back up files and folders

Back up the following folders and files from the BAC 8.0x server(s). The upgrade wizard will tell you when to restore them.

- **<BAC Data Processing Server installation directory>\CMDB\adapters\adapters**
- **<BAC Data Processing Server installation directory>\CMDB\general**
- All custom rules jar files from the **<BAC Data Processing Server installation directory>\BLE\rules** folder

- ▶ If you used User Reports to create Excel reports, back them up as well. The reports are stored in the <Gateway Server>\HPBSM\AppServer\webapps\site.war\openapi\excels\ directory in folders for each customer ID.

4 Uninstall BAC 8.0x

Disable and uninstall the BAC 8.0x server(s). For details, see "Uninstalling BSM Servers" on page 191.

5 Install BSM 9.10

If you have a distributed deployment, run the wizards on the Data Processing Server first. The wizards will direct when to begin running the wizards on the Gateway Server.

a Run the installation and post-installation wizards.

- ▶ For details about installing on a Windows platform, see "Installing BSM Servers on a Windows Platform" on page 147.
- ▶ For details about installing on a Linux platform, see "Installing BSM Servers on a Linux Platform" on page 159.

b Perform the post-installation tasks. For more information, see "Post-Installation Tasks" on page 450.

c OMi (Operations Manager *i*). If you are migrating OMi from BAC 8.0x to BSM 9.1x, perform the procedures specified in "OMi 8.10 to 9.1x Mid-Upgrade Procedure" on page 210.

6 Install the latest BSM 9.1x Service Pack

Perform the standard procedure for installing the BSM 9.1x service pack. For details, see "Installing the BSM 9.1x Service Pack - Standard" on page 48.

7 Run the upgrade wizard

Disable all BSM servers and run the upgrade wizard. For more details, see "Upgrade Wizard Overview" on page 181. If you have more than one Data Processing or Gateway Server, run the upgrade wizards on one of each type of server only. For each additional Data Processing and Gateway Server, run the the Setup and Database Configuration Utility. For more details, see "Setup and Database Configuration Utility Overview" on page 168.

8 Post-upgrade procedures

Perform the following procedures if you have these components.

- **OMi (Operations Manager i).** If you are migrating OMi from BAC 8.x to BSM 9.1x, perform the post-upgrade procedures specified in "OMi 8.10 to 9.1x Post-Upgrade Procedure" on page 225.
- **EUM.** For BPM profiles upgraded to applications, manually reconfigure the correct time zones. A configuration file was used to map time zone offsets (used by the old model) and time zone IDs (used by the new model). The first time zone ID that matched the time zone offset was used.

9 Continue with main upgrade procedure

Continue with step 13 on page 24 of the main upgrade procedure.

3

Service Packs and Patches

Service packs and patches are installed on top of BSM 9.1x.

This chapter includes:

- ▶ Service Pack Installation Overview on page 47
- ▶ Installing the BSM 9.1x Service Pack - Standard on page 48
- ▶ Installing the BSM 9.1x Service Pack - with Workaround to Resolve Modeling Related Issues on page 52
- ▶ Uninstalling a Service Pack (Rolling Back) on page 61
- ▶ Patch Installation on page 63

Service Pack Installation Overview

You install the BSM 9.13 service pack on top of BSM 9.10 or 9.12. There are two procedures for installing service packs, the standard procedure and the procedure including workaround for a number of modeling related issues.

You should run the standard service pack installation procedure unless the following conditions are true, in which case you should run the workaround procedure:

1 You have an OMi license **and**

2 Either:

- ▶ You are installing this service pack on top of a running BSM 9.10 environment after having run the upgrade wizard or the Setup and Database Configuration utility on BSM 9.10 at any point in the past.

or

- ▶ You are installing this service pack on top of BSM 9.12, where BSM 9.12 was installed on top of a running BSM 9.10 environment after having run the upgrade wizard or the Setup and Database Configuration utility on BSM 9.10.

Note: If you are not sure whether or not the workaround procedure applies to you, you can check as follows:

Go to **RTSM Administration > CI Type Manager** and select the **CIT Type ConfigurationItem > InfrastructureElement > ApplicationSystem > Lync**. On the right, open the **Details** tab and locate the **name** field (not the display name field). If the value is **Lync** with a capital **L**, then you need to perform the workaround procedure. If value is **lync** with a lower-case **L**, you can perform the standard procedure.

Installing the BSM 9.1x Service Pack - Standard

This section contains the standard procedure for installing BSM 9.1x service packs.

Note: There are two versions of this procedure depending on your BSM environment. To determine which procedure you should perform, see "Service Pack Installation Overview" on page 47.

To install the 9.1x Service Pack:

1 Prerequisites

- ▶ Before installing a BSM service pack, it is recommended that you back up all BSM databases.
- ▶ Back up any files you manually changed in the BSM root directory. For example, if you configured SSL on the Apache web server, back up

<Gateway server installation directory>/Webserver/conf/httpd.conf

<Gateway server installation directory>/Webserver/conf/extra/httpd-ssl.conf

- ▶ Before installing a BSM service pack, make sure that BSM has been fully stopped on all machines and that there are no open connections (for example, from Windows Explorer) from any machines to the BSM root directory or any of its subdirectories.

2 Download and install the service pack from the SSO site

- a Go to the SSO site:

<http://support.openview.hp.com/selfsolve/patches>

- b Select **Application Performance Management (BAC) > 9.13** (or the most recent service pack) and click **Search** to locate the installation files.
- c Save the package locally and launch the relevant setup file to install the service pack.
- d Run the installation files on all BSM servers (Gateway and Data Processing).
- e Run the post-installation wizard. This wizard follows the service pack installation automatically.

3 Reapply manual changes

If you have made changes in the HP BSM root directory to files that are updated during the service pack installation, for example while performing hardening procedures on your system, you must reapply those changes after the service pack installation on all relevant BSM machines. You can access your modified files from the backup folder located at: **<HP BSM root directory>\installation\<service_pack_name>\backup\<PATH_TO_FILE>**.

For example, if you had previously customized the **ServiceManagerAdapter.groovy** script, you need to use the automatic backup to restore the customizations. The script can be found in: **<BSM root directory>/installation/HPBsm913/backup/conf/opr/integration/sm**. Either manually reapply the customizations to the newer version of the script applied with the 9.13 service pack, or copy the backed up version to its original location, overwriting the 9.13 version. (The original version of the script will work with 9.13.) For more details, see the BSM 9.13 Release Notes.

4 Reapply SSL

If you had configured SSL on a IIS web server used by BSM, you need to reapply the BSM SSL configurations. For details, see the Hardening Guide.

5 Enable BSM

Enable BSM on all servers.

6 Clear the repository type cache

The service pack contains a fix for an issue with context menus on the dashboard. If you are upgrading to BSM 9.13, you must activate the fix by clearing the repository type cache as follows:

- a** In a web browser, open `http://<gateway server>:8080/jmx-console`.
- b** Under **Topaz**, click `service=repositories_manager`.
- c** Start `cleanRepositoryTypeDBAndCache()` with `sCustId=0` and `repositoryType=contextMenu`.

7 Alter the ALL_EVENTS table

The service pack contains a fix for an issue with events that have an automatic action exceeding 255 characters in length. If you are upgrading to BSM 9.13, you (or your database administrator) must manually alter the ALL_EVENTS table in the BSM event schema database. You must increase the size of the AA_CALL column from 255 to 4000 characters.

Use one of the following SQL expressions:

For Microsoft SQL Server:

```
alter table ALL_EVENTS alter column AA_CALL nvarchar(4000)
```

For Oracle:

```
alter table ALL_EVENTS modify (AA_CALL varchar2(4000 CHAR));
```

8 Delete temporary internet files

Delete the browser's temporary Internet files on each browser that accesses BSM.

9 Return to main procedure

If you are performing this service pack installation procedure as part of a larger upgrade procedure, continue with the main procedure as follows:

- ▶ If you are upgrading from BAC 7.55 or 8.0x using the staging method for the 8.0x upgrade, continue with step 4 on page 41.
- ▶ If you are upgrading from BAC 7.55 8.0x using the direct method for the 8.0x upgrade, continue with step 7 on page 45.
- ▶ If you are upgrading from BSM 9.0x, continue with step 9 on page 31.

Installing the BSM 9.1x Service Pack - with Workaround to Resolve Modeling Related Issues

In BSM 9.10, there was an internal conflict in the Lync Content Pack, causing problems for customers with OMi licenses. Additionally, there was a topology synchronization issue. These problems only occurred if you ran the upgrade wizard or the Setup and Database Configuration utility on a BSM 9.10 server.

This section contains the procedure for installing BSM 9.1x service packs including workaround procedures.

Note: There are two versions of this procedure depending on your BSM environment. To determine which procedure you should perform, see "Service Pack Installation Overview" on page 47.

To install the 9.1x Service Pack:

1 Back up BSM

It is recommended that you back up all BSM databases.

2 Review affected CI types

This step is part of the Lync Content Pack issue workaround.

The following is a list of CI types that are involved in the next few steps of this procedure. For each of the following CI types, you will have to delete all instances of the CI types, remove related model notifications, remove the CI types themselves, and undeploy HP Universal CMDB packages as specified in the next few steps of this procedure.

- ▶ ConfigurationItem > InfrastructureElement > ApplicationSystem > Lync (class name: Lync)
- ▶ ConfigurationItem > InfrastructureElement > ApplicationSystem > Lync > Lync Site (class name: lyncsite)

- ▶ ConfigurationItem > InfrastructureElement > ApplicationSystem > Lync > Lync Pool (class name: lyncpool)
- ▶ ConfigurationItem > InfrastructureElement > RunningSoftware > Communication Server (class name: communicationserver)
- ▶ ConfigurationItem > InfrastructureElement > RunningSoftware > Communication Server > Lync Server (class name: lyncserver)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource (class name: lyncresource)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role (class name: lyncserverrole)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > Front End Server (class name: frontendserver)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > AV Conferencing Server (class name: avconferencingserver)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > Edge Server (class name: edgserver)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > Mediation Server (class name: mediationserver)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > Monitoring Server (class name: monitoringserver)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > Archiving Server (class name: archivingserver)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > Director Server (class name: directorserver)

- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > Registrar Server (class name: registrarserver)
- ▶ ConfigurationItem > InfrastructureElement > Application Resource > Lync Resource > Lync Server Role > Central Management Server (class name: centralmanagementserver)
- ▶ ConfigurationItem > InfrastructureElement > ApplicationSystem > Exchange > Exchange Database Availability Group (class name: ms_exchange_dag)

3 Delete CI instances

This step is part of the Lync Content Pack issue workaround.

Any CIs deleted as part of this procedure will be rediscovered once the setup and configuration of BSM is complete.

- a Open the IT Universe Manager from **RTSM Administration > Modeling > IT Universe**.
- b Locate the **CI Selector** Pane > **Search CIs** Tab > **CI Type** field.

Search for all instances of the CI Types listed above by selecting them in the **CI Type** field and clicking the **Start the Search** button.



- c Delete all instances that are found. This will automatically delete their child CIs as well. These CIs will be rediscovered once the setup and configuration of BSM is complete.

4 Remove model notifications

This step is part of the Lync Content Pack issue workaround.

Remove model notifications for each of the CI types listed above as follows:

- a Access the JMX console on the Data Processing server by using the following URL:
http://<BSM Data Processing Server>:21212/jmx-console
- b Navigate to **Packaging Services > listSubsystems**. Enter the customer ID (**1** for single customer system, appropriate customer ID for multi-customer system) into the **customerID** field and click **Invoke**.

- c** Click **modelnotification**, and select each notification name. An XML file opens for each notification.
- d** Search for any class name to be removed.
- e** If the class to be deleted is the only class name in the model notification xml, the whole notification must be removed. To remove the whole notification, return one page back in the JMX screen, locate the JMX process with the list of all model notifications, and click **Delete** at the right of the page.
- f** Otherwise, delete the entries for any class names listed above. An entry for a class appears between the following possible tags:
 - `<AddElement></AddElement>`
 - `<RemoveElement></RemoveElement>`
 - `<UpdateElement></UpdateElement>`

Delete the entry for the class. You must remove the entire entry, including these opening and closing tags.

For example: in the following section, the class to remove is **callhome_event**, the bold section (UpdateElement) should be deleted:

```
<AddElement>
  <ElementClassCondition>
    <ClassType>ip_address</ClassType>
    <Derived>>false</Derived>
  </ElementClassCondition>
  <ElementPropertiesCondition>
    <property-complex-expression/>
  </ElementPropertiesCondition>
</AddElement>
<AddElement>
  <ElementClassCondition>
    <ClassType>ip_subnet</ClassType>
    <Derived>>false</Derived>
  </ElementClassCondition>
  <ElementPropertiesCondition>
    <property-complex-expression/>
  </ElementPropertiesCondition>
</AddElement>
<UpdateElement>
  <ElementClassCondition>
    <ClassType>callhome_event</ClassType>
    <Derived>>false</Derived>
  </ElementClassCondition>
  <ElementPropertiesCondition>
    <property-complex-expression/>
  </ElementPropertiesCondition>
  <PropertiesFilter/>
</UpdateElement>
```

- g** Click **Save Resource** at the bottom of the JMX screen.

5 Delete CI types

This step is part of the Lync Content Pack issue workaround.

Delete each of the CI types listed above as follows:

- a** Open the CI Type Manager from **RTSM Administration > Modeling > CI Type Manager**.
- b** Right-click each CI type to be deleted and select **Delete**. Note that CI types cannot be deleted while they have relationships to other CIs. Therefore, delete the child CI types before deleting the parent CI types.

6 Undeploy HP Universal CMDB packages

This step is part of the Lync Content Pack issue workaround.

- a** Open the Package Manager from **RTSM Administration > Administration > Package Manager**.
- b** Undeploy the following HP Universal CMDB packages (all resources) in the order specified below.
 - HPOprLys
 - HPOprExc
 - CommLyncServer
 - ExchangeServer2010

7 Disable BSM

Make sure that BSM has been fully stopped on all machines and that there are no open connections (for example, from Windows Explorer) from any machines to the BSM root directory or any of its subdirectories.

8 Install the service pack

- a** Go to the SSO site:
<http://support.openview.hp.com/selfsolve/patches>
- b** Select **Application Performance Management (BAC) > 9.13** (or the most recent service pack) and click **Search** to locate the installation files.

- c** Save the package locally and launch the relevant setup file to install the Service Pack.
- d** Run the installation files on all BSM servers (Gateway and Data Processing).
- e** Run the post-installation wizard. This wizard follows the service pack installation automatically.

9 Reapply custom changes

If you have made changes in the HP BSM root directory to files that are updated during the service pack installation, for example while performing hardening procedures on your system, you must reapply those changes after the service pack installation on all relevant BSM machines. You can access your modified files from the backup folder located at: **<BSM root**

directory>\installation\<service_pack_name>\backup\<PATH_TO_FILE>.

For example, if you had previously customized the **ServiceManagerAdapter.groovy** script, you need to use the automatic backup to restore the customizations. The script can be found in: **<BSM root directory>/installation/HPBsm913/backup/conf/opr/integration/sm**. Either manually reapply the customizations to the newer version of the script applied with the 9.13 service pack, or copy the backed up version to its original location, overwriting the 9.13 version. (The original version of the script will work with 9.13.) For more details, see the BSM 9.13 Release Notes.

10 Reapply SSL

If you had configured SSL on a IIS web server used by BSM, you need to reapply the BSM SSL configurations. For details, see the Hardening Guide.

11 Enable BSM

Enable all BSM servers.

12 Deploy uCMDB packages

This step is part of the Lync Content Pack issue workaround.

- a** Open the Package Manager from **RTSM Administration > Administration > Package Manager**.
- b** Deploy the HP Universal CMDB packages (all resources) in the order specified below. The files are located in the following locations:

File locations:

- Windows: %TOPAZ_HOME%\odb\conf\factory_packages\content
- Linux: /opt/HP/BSM/odb/conf/factory_packages/content

Packages:

- CommLyncServer.zip
- ExchangeServer2010.zip
- HPOprLys.zip
- HPOprExc.zip

13 Import content packs

This step is part of the Lync Content Pack issue workaround.

- a** Navigate to Admin > Operations Management > Manage Content > Content Packs.
- b** Import the content packs below. They are located in the following locations:

File locations:

- Windows: %TOPAZ_HOME%\conf\opr\content\<locale>

- Linux: /opt/HP/BSM/conf/opr/content/<locale>

Content Packs:

- MM-Exc.xml
- MM-Lys.xml

14 Upload the topology synchronization packages

Upload the topology synchronization packages by running the following batch files depending on your operating system:

For Windows:

- "%TOPAZ_HOME%\bin\opr-sdtool.bat" -uploadpackage
"%TOPAZ_HOME%\conf\opr\topology-sync\sync-packages\default"
- "%TOPAZ_HOME%\bin\opr-sdtool.bat" -uploadpackage
"%TOPAZ_HOME%\conf\opr\topology-sync\sync-packages\nodegroups"
- "%TOPAZ_HOME%\bin\opr-sdtool.bat" -uploadpackage
"%TOPAZ_HOME%\conf\opr\topology-sync\sync-packages\operations-agent"

For Linux:

- /opt/HP/BSM/bin/opr-sdtool.sh -uploadpackage
/opt/HP/BSM/conf/opr/topology-sync/sync-packages/default
- /opt/HP/BSM/bin/opr-sdtool.sh -uploadpackage
/opt/HP/BSM/conf/opr/topology-sync/sync-packages/nodegroups
- /opt/HP/BSM/bin/opr-sdtool.sh -uploadpackage
/opt/HP/BSM/conf/opr/topology-sync/sync-packages/operations-agent

15 Clear the repository type cache

The service pack contains a fix for an issue with context menus on the dashboard. If you are upgrading to BSM 9.13, you must activate the fix by clearing the repository type cache as follows:

- a** In a web browser, open <http://<gateway server>:8080/jmx-console>.
- b** Under **Topaz**, click **service=repositories_manager**.

- c Start `cleanRepositoryTypeDBAndCache()` with `sCustId=0` and `repositoryType=contextMenu`.

16 Alter the ALL_EVENTS table

The service pack contains a fix for an issue with events that have an automatic action exceeding 255 characters in length. If you are upgrading to BSM 9.13, you (or your database administrator) must manually alter the ALL_EVENTS table in the BSM event schema database. You must increase the size of the AA_CALL column from 255 to 4000 characters.

Use one of the following SQL expressions:

For Microsoft SQL Server:

```
alter table ALL_EVENTS alter column AA_CALL nvarchar(4000)
```

For Oracle:

```
alter table ALL_EVENTS modify (AA_CALL varchar2(4000 CHAR));
```

17 Delete temporary internet files

Delete the browser's temporary Internet files on each browser that accesses BSM.

18 Return to main procedure

If you are performing this service pack installation as part of a larger procedure, continue with that procedure.

Uninstalling a Service Pack (Rolling Back)

This procedure explains how to uninstall a service pack. Follow the instructions depending on your operating system.

Note: You can roll back from BSM 9.13 to 9.12. However, rolling back to BSM 9.10 is not supported.

For instructions on completely uninstalling BSM, see "Complete Uninstall" on page 191.

To roll back a BSM service pack to a previously installed version - Windows:

- 1** Stop the HP BSM service on all servers and confirm that they are stopped.
- 2** Stop the web server process on all servers (IIS Admin Service for IIS; Apache service for Apache).
- 3** Select the service pack to remove from Control Panel > Add/Remove Programs > Change or Remove Programs. On Windows 2003 Server, select the Show Updates option to ensure that the service pack version is displayed beneath the root entry.
- 4** When the uninstall process is complete, restart the machine if requested.
- 5** Remove all subdirectories under the directory <HP BSM root directory>\EJBContainer\server\mercury\work.
- 6** Restart the web server process on all Gateway servers.
- 7** Rerun the Setup and Database Configuration Utility without changing any of the existing settings
- 8** You may also need to roll back any database that changed as a result of the upgrade. If you encounter any problems, contact HP Software Support.
- 9** Make sure to uninstall or rollback any updated data collectors as well.

To roll back a BSM service pack to a previously installed version - Linux:

- 1** Stop BSM as follows:

```
\opt\HP\BSM\script\run_hpbsm stop
```

- 2** Run the uninstall script as follows:

```
\opt\HP\BSM\uninstall\<version>\setup.bin
```

Where <version> is your HP BSM version. For example **HPBSM912**.

Patch Installation

Check the following website to see if there is a patch for your BSM version:

<http://support.openview.hp.com/selfsolve/patches>

Installation instructions can be found in the readme file bundled with the patch.

4

Staging Data Replicator

This chapter includes:

- Staging Data Replicator - Overview on page 65
- Running the Staging Data Replicator (Embedded) on page 66
- Running the Staging Data Replicator (Standalone) on page 67
- Unsubscribing the Staging Data Replicator from the Source Server on page 71
- Running the SDR with Basic Authentication on page 72
- SSL Configuration for the Staging Data Replicator on page 73

Staging Data Replicator - Overview

The Staging Data Replicator (SDR) is a tool that transfers data from the production environment to the staging environment during staging mode. The purpose of this tool is to create a window of time in which the same data can be viewed in both environments, allowing you to verify functionality and configuration settings in the staging environment.

While the SDR is running, any configuration changes made to the original BAC servers are not transferred to the staging servers. Only data samples are transferred.

Samples related to new configurations performed on the source environment may not be transferred by the SDR. To view the samples that were not transferred, view the ignored samples log at **log\sdr\ignoredSamples.log** and the general SDR log at **log\sdr\sdr_all.log**.

You can change the log level of these files through the following files:

- ▶ Embedded SDR: `HPBSM\SDR\<BSM Source Version> \conf\core\Tools\log4j\sdreplicator\sdreplicator.properties`
- ▶ Standalone SDR: `HPBSMSDR\conf\core\Tools\log4j\sdreplicator\sdreplicator.properties`

This tool is only supported in staging mode. For more information about staging mode, see "Upgrade Types" on page 19.

The SDR must be installed on a machine that can communicate with the production and staging environments. If the staging server can not communicate with the production server, the SDR must be installed as a standalone utility on a different machine.

For task details, see:

- ▶ "Running the Staging Data Replicator (Embedded)" on page 66
- ▶ "Running the Staging Data Replicator (Standalone)" on page 67

Running the Staging Data Replicator (Embedded)

The SDR typically runs embedded in the staging server as part of the upgrade wizard. However, it can also be run as a standalone utility on a different server. For details, see "Running the Staging Data Replicator (Standalone)" on page 67.

Note: If your source and destination environments are located in separate domains and you cannot configure your destination environment to recognize your source environment, you must run the SDR as a standalone utility. For details, see "Running the Staging Data Replicator (Standalone)" on page 67.

To run the SDR (embedded)

- 1** If the staging server uses basic authentication, the SDR can not communicate with the staging server unless you run the **basicauth** tool. For details, see "Running the SDR with Basic Authentication" on page 72.
- 2** If the staging server uses SSL, you will need to perform custom configurations to allow the SDR to communicate with the staging server. For details, see "SSL Configuration for the Staging Data Replicator" on page 73.
- 3** Verify that the SDR embedded in the staging server can communicate with the production server. For details, see "Verifying that the SDR Server Can Communicate with the Production Server" on page 70.
- 4** After you have completed the staging process and are prepared to move your staging environment to a production environment, stop the SDR by rerunning the upgrade wizard and selecting the appropriate option to stop the SDR.
- 5** Unsubscribe the staging data replicator from the source server. For details, see "Unsubscribing the Staging Data Replicator from the Source Server" on page 71.

Running the Staging Data Replicator (Standalone)

You can choose to run the SDR embedded in the staging server, or on a standalone server. However, if your source and destination environments are located in separate domains and you cannot configure your destination environment to recognize your source environment, you must run the SDR on as a standalone utility on a different machine. This machine must have access to both your production and staging servers.

To use the Staging Data Replicator standalone utility:

- 1** To use the Staging Data Replicator as a standalone utility, you must install it on a separate machine with access to both your production and staging servers.
 - To check that the SDR server can connect to the staging server, enter the following url in an any internet browser from the standalone server:

```
http://<_DESTINATION_>/ext/mod_mdrv_wrap.dll?type=test
```

Where **_DESTINATION** is the name of the Gateway Server or Load Balancer, depending on your configuration.

- Check that the SDR server can connect to the production server. For details, see "Verifying that the SDR Server Can Communicate with the Production Server" on page 70.
- 2** Run the appropriate replicator file, depending on the version of your production (original) server. The files are located on the SDR DVD:
 - **Windows_Setup\7.x\HPBsmSDR7.x_9.10_setup.exe**
 - **Windows_Setup\8.x\HPBsmSDR8.x_9.10_setup.exe**
 - **Solaris_Setup\8.x\HPBsmSDR7.x_9.10_setup.bin**
 - **Solaris_Setup\8.x\HPBsmSDR8.x_9.10_setup.bin**
 - **Linux_Setup\8.x\HPBsmSDR7.x_9.10_setup.bin**
 - **Linux_Setup\8.x\HPBsmSDR8.x_9.10_setup.bin**
 - 3** Follow the on-screen instructions to install the Staging Data Replicator.
 - 4** After you have completed the Staging Data Replicator installation, open the **<Staging Data Replicator root directory>\conf\b2G_translator.xml** file and modify the following:
 - **_SOURCE_HOST_NAME_.** Replace this with the host name of the source (production) Business Availability Center Gateway Server. If you have more than one Gateway Server, you can use the name of any of them for this value.

- `__DESTINATION_HOST_NAME__`. Replace this with the host name of the destination (staging) BSM Gateway Server or Load Balancer, depending on your configuration. This string appears twice within this file in the following line:

```
<ForwardURL url="http://__DESTINATION_HOST_NAME__/ext/
mod_mdrv_wrap.dll?type=md_sample_array&acceptor_name=__
DESTINATION_HOST_NAME__&message_subject=topaz_report/s
amples&request_timeout=30&force_keep_alive=true&s
end_gd=true"/>
```

- `clientid=""`. If you do not require guaranteed delivery of data when the Staging Data Replicator stops running, delete the value for this parameter. It is generally recommended that you do not modify this parameter.
- 5 Copy the following two directories from the staging server to the `C:\HPBSMSDR\dat` directory of the standalone SDR server:
 - `C:\HPBSM\SDR\<<version>\dat\da_metadata`
 - `C:\HPBSM\SDR\<<version>\dat\da_cache`
 where `<version>` is the BAC version of your production environment.
 - 6 If the staging server uses basic authentication, the SDR can not communicate with the staging server unless you run the **basicauth** tool. For details, see "Running the SDR with Basic Authentication" on page 72.
 - 7 If the staging server uses SSL, you will need to perform custom configurations to allow the SDR to communicate with the staging server. For details, see "SSL Configuration for the Staging Data Replicator" on page 73.
 - 8 Begin running the Staging Data Replicator.
 - Windows: Select **Start > HP BSM Staging Data Replicator > Administration > Enable HP BSM Staging Data Replicator**.
 - Linux: Run the following command:


```
/opt/HP/BsmSDR/bin/sdrepliator_run.sh start
```

- 9 After starting the SDR, copy the <SDR installation directory>/dat/sdr directory from the SDR server to the Gateway server in the <BSM home directory>/dat/sdr directory. This informs the upgrade wizard of the SDR initiation time which is needed for the Data Transfer Tool.
- 10 After you have completed the staging process and are prepared to move your staging environment to a production environment, stop the Staging Data Replicator.
 - Windows: Select **Start > HP BSM Staging Data Replicator > Administration > Disable HP BSM Staging Data Replicator**.
 - Linux: Run the following command:
`/opt/HP/BsmSDR/bin/sdreplicator_run.sh stop`
- 11 Unsubscribe the staging data replicator from the source server. For details, see "Unsubscribing the Staging Data Replicator from the Source Server" on page 71.

Verifying that the SDR Server Can Communicate with the Production Server

- 1 Ping the production server.
 - a Ping the production Gateway Server from the SDR server using the Gateway Server's short name. If this works, continue to step 2. If it does not work, continue with step 1 b.
 - b Ping the production Gateway Server from the SDR server using the Gateway Server's fully qualified domain name. If this works, open the relevant **hosts** file for your operating system and add the mapping between the production Gateway Server name and its IP address.
- 2 Verify connection.
 - a **Production Gateway Server runs Windows:** Run **ipconfig** on the production Gateway Server.
Production Gateway Server runs Solaris/Linux: Run **ifconfig -a** on the production Gateway Server.
 - b Verify all the listed IP addresses are open to connection to and from the server running the SDR.

If this is not feasible, contact HP Software Support.

- c Verify that the ports 383, 1098, 1099, 2506, and 2507 are open on the SDR server.

Unsubscribing the Staging Data Replicator from the Source Server

This procedure unsubscribes the SDR from the source server's bus, preventing data from accumulating in the source server. It is performed after you have completed the staging process and disabled the SDR.

Note: You do not have to perform this procedure if you are immediately uninstalling the previous version of Business Availability Center from the source server.

To unsubscribe the SDR:

- 1 Stop the SDR.
 - a Open the nanny jmx console from **http://<machine name>:11021**
 - b Select **Foundations: type=NannyManager**
 - c Open **showServiceInfoAsHTML**
 - d Stop the **HPBSMSDR-x.x** process.
- 1 Open the **<Staging Data Replicator root directory>\conf\b2G_translator.xml** file and locate the two **<Message Selector>** elements.
- 2 Within the **<Message Selector>** elements, replace the attribute value of **enabled** to 0 (the default is **enabled="1"**) in the following line:


```
<MessageSelector name="customer_name" value="Default Client"
enabled="0" />
```
- 3 Start the SDR.
 - a Open the nanny jmx console from **http://<machine name>:11021**

- b** Select **Foundations: type=NannyManager**
 - c** Open **showServiceInfoAsHTML**
 - d** Start the **HPBSMSDR-x.x** process.
- 4** Wait several minutes, and then stop the SDR as described in step 1.

Running the SDR with Basic Authentication

If the staging server is using basic authentication, the SDR cannot communicate with the staging server without a user name and password. The **basicauth** tool allows you to enter this data into the BSM in an encrypted format, thereby enabling the SDR to communicate with servers that use basic authentication.

To configure SDR to work with basic authentication:

From the command prompt, run the **basicauth** file using the following syntax:

```
<Staging Data Replicator root directory>\bin basicauth [-embedded [8.x | 7.x] | standalone] [enabled username password | disabled]
```

Where:

-embedded is for an SDR that is embedded in the destination environment. In this case, you need to specify the version of your production (source) server as either 7.x or 8.x.

-standalone is for a standalone SDR.

enabled is to enable basic authentication. Specify a valid username and password. This tool encrypts the password before it is saved in the configuration file.

disabled is to disable basic authentication.

SSL Configuration for the Staging Data Replicator

If the staging server uses SSL, you need to perform the following procedure to allow the SDR to communicate with the staging server.

To configure the SDR to support SSL:

1 Configure SDR to use SSL.

In the **<SDR root directory>\conf\b2g_translator.xml** file, locate ForwardURL and change **http** to **https**.

2 Configure the SDR to trust the BSM certificate.

- a Obtain a copy of the certificate used by the web server on the BSM Gateway Server or certificate of Certificate Authority that issued BSM web server certificate. This file must be a DER encoded binary X.509 (.CER) file.
- b Import the above-mentioned certificate into SDR's truststore. For details, see "Configuring the Truststore" on page 71 in the *HP Business Service Management Hardening Guide* PDF.

Default truststore for SDR is **<SDR root directory>\JRE\lib\security\cacerts**.

Example:

```
<SDR root directory>\JRE\bin>keytool -import -trustcacerts -alias <your
CA certificate alias name> -keystore ../lib/security/cacerts -file <CA
certificate file>
```

- c If you are not using the default truststore with SDR, configure the SDR to use a non-default truststore, and add additional options in the file **<SDR root directory>\bin\sdrreplicator_run.bat**, as follows:

- Locate the following line:

```
SET PROCESS_OPTS=%PROCESS_OPTS% -
Dconf.file=%PRODUCT_HOME_PATH%\conf\b2g_translator.xml -
Dprop.file=%PRODUCT_HOME_PATH%\conf\b2g_translator.properties -
Dmsg.filter.file=%PRODUCT_HOME_PATH%\conf\b2g_exclude_samples.xml
```

► At the end of this line, add the following:

```
-Dnet.ssl.trustStore=<keystore path>  
-Dnet.ssl.trustStorePassword=passphrase
```

Part II

Deployment Planning

5

Deployment Planning

This chapter includes:

- ▶ Deployment Planning Checklist on page 78
- ▶ Deployment Planning Considerations on page 79
- ▶ Using the Capacity Calculator on page 83

Deployment Planning Checklist

Deploying HP Business Service Management in an enterprise network environment is a process that requires resource planning, system architecture design, and a well-planned deployment strategy. The checklist below describes some of the basic issues that should be considered prior to installation. HP Software Professional Services offers consulting services to assist customers with BSM strategy, planning and deployment. For information, contact an HP representative.

Use this checklist to review the basic issues that your organization should consider when planning the HP Business Service Management deployment.

✓	Step
	Analyze the IT processes and organizational structure and culture that can affect, or be affected by, the deployment.
	Map the customer environment.
	Analyze the organization's goals and identify the key IT-enabled business processes to achieve these goals.
	Identify the target users (those with a vested interest in the business processes), for example, executives, LOB managers, marketing managers, customer support personnel, support engineers, and so forth.
	Align the project with current performance management practices.
	Map the architecture of the monitored infrastructure, including identifying the processes, systems, system resources, and other infrastructure elements to monitor in each of the applications.
	Define the project deliverables, including setting expectations regarding measurements, features, the deployment scope, and maturity levels.
	Identify the appropriate HP Business Service Management functionality.
	Build a deployment roadmap.
	Define success criteria for the project.
	Define performance and availability objectives for each monitored business process.
	Define measurement types to be supported at each deployment stage.

✓	Step
	Form HP Business Service Management administration and operations team(s).
	Plan the practical aspects of the deployment, including system architecture and capacity planning using the capacity calculator; and database environment and security considerations, and so forth.

Deployment Planning Considerations

This section provides different information that may be useful while planning a BSM deployment. This section contains:

- "How to determine the hardware requirements that will satisfy the expected capacity?" on page 80
- "How to determine which deployment type to choose? (One-machine or distributed)?" on page 80
- "How many BSM machines do I need?" on page 80
- "Should I deploy BSM on virtual machines?" on page 81
- "What specific Hardware should I purchase?" on page 81
- "How to choose your operating system? (Windows\Linux)" on page 81
- "How much disk space is required for the database schemas?" on page 81
- "Do I need a CMS, or is RTSM enough for my needs?" on page 81
- "Which web server to choose?" on page 82
- "What disaster recovery aspects should I consider?" on page 82
- "What network aspects should I consider?" on page 82

How to determine the hardware requirements that will satisfy the expected capacity?

Use the BSM 9 Deployments and Capacity Calculator for planning the BSM deployment. The calculator determines the required hardware profile per deployment type. When using the calculator, consider expected growth in the near future. For details, see "Using the Capacity Calculator" on page 83.

How to determine which deployment type to choose? (One-machine or distributed)?

BSM can be installed either as a one-machine deployment or as a distributed deployment (Gateway and Data Processing Servers installed on separate machines). To choose the deployment type, consider the following:

- ▶ The hardware required for each type as reflected in the Deployments and Capacity Calculator results. For large capacities, the one-machine deployment might require a machine with a very large RAM that will not be recommended/supported by your IT.
- ▶ One-machine deployment is more economic in terms of resources since many of the common components are deployed only once.
- ▶ In terms of best practices - both are recommended and supported.

How many BSM machines do I need?

- ▶ The basic BSM deployment consists of either 1 one-machine installation or 1 Gateway (GW) installation + 1 Data Processing (DPS) installation.
- ▶ To increase availability & reliability of BSM, it is recommended to deploy at least 1 additional one-machine installation/GW+DPS installation pair. For more information, see "Benefits of a Multi-Server Deployment" on page 126.
- ▶ To scale the number of BSM concurrent users you can add additional Gateway machines (or additional one-machine installations)
- ▶ Do not inflate your BSM deployment by adding more machines than required. The number of TCP resources consumed per machine is correlated to the number of BSM machines in the deployment and is limited.

Should I deploy BSM on virtual machines?

- BSM (GW and DPS installations, either as one-machine or as a distributed installation) can be deployed on virtual machines. For more information, see "HP Business Service Management on Virtual Platforms" on page 143.
- Regardless of your choice, it is unadvisable to run the database used by BSM on a virtual machine.

What specific Hardware should I purchase?

BSM requires specific hardware profiles, but does not require specific brand. For details about hardware requirements, see "System Requirements" on page 131.

How to choose your operating system? (Windows\Linux)

- If you are migrating from a previous version of BSM, see the *BSM 9.1x Upgrade Guide* for information about which migration paths are supported.
- Both operating systems are recommended and supported. For specific information regarding supported versions, see "System Requirements" on page 131.

How much disk space is required for the database schemas?

The required disk space for BSM schemas is influenced by many variables. For more information about the main considerations, see the *HP Business Service Management Database Guide* PDF.

Do I need a CMS, or is RTSM enough for my needs?

RTSM is designed to support BSM operational use cases only. For topology-based integrations between BSM and other HP centers, it is recommended to install a central CMDB instance that will serve as the CMS instead of integrating directly with the RTSM instance. For more information, see the *RTSM Best Practices guide*.

Which web server to choose?

BSM supports both Microsoft IIS and Apache web servers (bundled within BSM installation). In terms of best practices, both are recommended and supported.

What disaster recovery aspects should I consider?

You can setup an additional BSM deployment that will act as a Disaster Recovery System. Such a deployment can be added at any given time on demand and does not have to be considered when planning your primary environment. For more information, see "Disaster Recovery for BSM" on page 165.

What network aspects should I consider?

It is recommended that all BSM Servers are installed on the same network segment.

If BSM servers are installed on multiple network segments, it is highly recommended that the number of hops and the latency between the servers be minimal. Network-induced latency may cause adverse effects to the HP Business Service Management application and can result in performance and stability issues. We recommend the network latency should be no more than 5 milliseconds, regardless of the number of hops.

Placing firewalls between BSM servers is not supported.

Using the Capacity Calculator

The capacity calculator Excel spreadsheet should be used to determine the scope and size of your BSM deployment. You input the information regarding the scope of your deployment in terms of numbers of applications running, users, and expected data. The capacity calculator calculates the configuration of your deployment and the hardware requirements of each machine in the BSM deployment. This information can be uploaded automatically while running the UpgradeWizard which is run after installing or upgrading BSM.

Note: In a Linux environment, the capacity calculator Excel spreadsheet can be opened and edited using the **Calc** spreadsheet application of OpenOffice.org.

The capacity calculator Excel file includes the following sheets:

- ▶ **Deployment Calculator.** Includes the Capacity Questionnaire table, where you enter your capacity and deployment data, and the Output tables, where your capacity levels and machine requirements are automatically calculated for you.
- ▶ **Certified Deployments.** Includes detailed information on hardware requirements, included components, and capacity for the certified deployments.
- ▶ **Detailed Capacities.** Gives detailed data regarding the numbers used to calculate capacity levels of **Small**, **Medium**, **Large**, and **Extra Large** for each BSM application, users, metric data, and model size.
- ▶ **Level Override.** This sheet should be used only by very experienced BSM administrators. It enables the option to override the capacity levels calculated in the capacity calculator.

To use the capacity calculator:

1 Locate the Excel sheet named **BSM_9_Deployment_and_Capacities.xls** in your installation media. The file can be found in the **Documentation** folder in the main BSM installation DVD or you can download the latest version from the HP Software Product Manuals Web site (<http://h20230.www2.hp.com/selfsolve/manuals>). Search the web site for the term "capacity calculator".

2 In the **Deployment Calculator** sheet **Capacity Questionnaire** columns:

- ▶ Select which applications you are running by selecting **Yes** or **No** as appropriate in the cells next to the name of each application.
- ▶ Enter the required data for each application that you are running and for the number of **Logged in Users**.

You can hover over each cell to read a tooltip description of the information required for each application.

Tip: When entering the number of BPM Applications, use the number of BPM Profiles in your BAC/BSM 8.x system.

3 After you enter your data, the **Output** tables on the right of the **Deployment Calculation** sheet automatically update to give you the required information regarding your deployment.

- ▶ The **Output - Application/Level** table on the top right indicates the scope of your deployment, giving you sizing information. This includes users, size of your model, size of your expected metrics data, application status (on or off), and sizing for each application.
- ▶ The **Output - Machine Requirements** table in the lower right indicates, for each installation type (one machine or distributed), the required memory in gigabytes and the number of CPU cores for each server installation.

Decide which Deployment Type (one machine or distributed) is applicable to your deployment.

- 4 Save the Excel file in a location that is accessible to the servers where you are installing BSM.

You can now prepare the hardware environment and install BSM based on these recommendations.

To apply the capacity calculator data during installation:

When running the Setup and Database Configuration utility in the Server Deployment page, browse to the location where you saved the Capacity Calculator with your data. Upload the file, and the data from the Excel sheet automatically updates the fields in the wizard.

For details on using the utility, see "Running the Setup and Database Configuration Utility" on page 175.

Using the Capacity Calculator After Installation

After you have BSM installed, you may want to make changes to your deployment. You can add applications, change the number of logged in users or any of the other numbers related to running applications. You can edit your capacity calculator and determine if the scope of your deployment has changed.

You can upload the data from the updated capacity calculator's Excel file directly into the Server Deployment page in Platform Administration. This page enables you to update the information that you entered in the Server Deployment page while running the Setup and Database Configuration utility without having to run the wizard.

If you do not have the appropriate license for an application, the application does not appear in the list of available applications in the Server Deployment page, either during installation or in the Platform Admin page. You can add licenses for applications after BSM is deployed in the License Management page in Platform Admin. After you add a license, you must go to the Server Deployment page to enable the application.

For details on updating a deployment, see "How to Update Your BSM Licenses, Applications, or Deployment Scope" in *Platform Administration*. For any changes to take effect while updating a deployment, you must restart BSM.

6

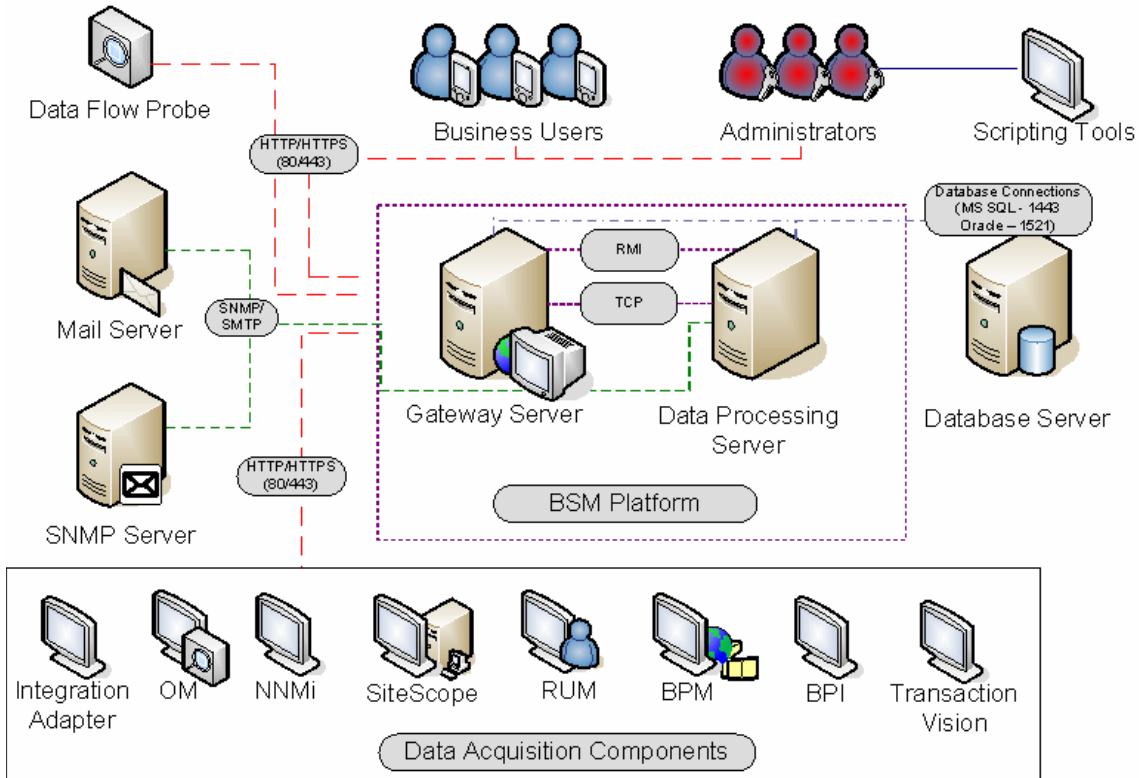
Understanding the Platform and Components

This chapter includes:

- ▶ Platform Architecture Diagram on page 88
- ▶ BSM Servers on page 89
- ▶ BSM Database Server on page 92
- ▶ BSM Data Sources on page 93
- ▶ Additional Proprietary Components on page 96
- ▶ Third-Party Components on page 97
- ▶ Bus Communication Among BSM Components on page 98

Platform Architecture Diagram

The below diagram illustrates the general BSM platform architecture and the communication protocols used among the components.



BSM Servers

The HP Business Service Management platform consists of proprietary servers and components, data sources, scripting tools, and third-party servers, such as database and mail servers, that you set up in the enterprise network environment. This chapter provides an overview of the HP Business Service Management platform and components.

HP Business Service Management is powered by a set of servers that are responsible for running the applications, facilitating system management, data handling, reporting, and alerting. You install the following HP Business Service Management servers on one or more Microsoft Windows or Linux machines in your enterprise network environment:

- ▶ **HP Business Service Management Gateway Server.** Responsible for running HP Business Service Management applications, producing reports, operating the administration areas, receiving data samples from the data collectors and distributing this data to the relevant HP Business Service Management components, and supporting the bus. To work with HP Business Service Management, the Gateway server machine must run a Web server.
- ▶ **HP Business Service Management Data Processing Server.** Responsible for aggregating data, running the Business Logic Engine, and controlling the RTSM service.

You can install the HP Business Service Management servers according to a number of different deployment strategies. Distributed deployments, in which multiple server machines are installed, can benefit from various high availability and load balancing options. For details on the recommended deployment strategies, see "Deployment Configurations" on page 123.

Notes and Best Practices for Server Deployment

Note the following when deploying HP Business Service Management servers:

- ▶ Access to the HP Business Service Management server machine must be available, either through HTTP or HTTPS, from any standard Internet or intranet connection.
- ▶ The HP Business Service Management servers should be on dedicated machines and should not run other applications.
- ▶ Installing HP Business Service Management servers together with most other HP products on the same physical machine may result in port conflicts, performance issues, or other unexpected behavior. The coexistence of HP Business Service Management servers with HP SiteScope or HP Operations Manager agent has been tested and is supported.
- ▶ Sun Java 6 (update 20) is copied onto the machine during server installation as part of the HP Business Service Management installation.
- ▶ If HP Business Service Management servers are installed on multiple network segments, it is highly recommended that the number of hops and the latency between the servers be minimal. Network-induced latency may cause adverse affects to the HP Business Service Management application and can result in performance and stability issues. We recommend the network latency should be no more than 5 ms, regardless of the number of hops. For more information, contact HP Software Support.
- ▶ All HP Business Service Management servers, as well as the database servers, must be installed in the same time zone, with the same daylight savings time configuration, and be set to the same time.
- ▶ If your BSM database server is using an SQL Server platform, make sure the Compatibility Level database setting is set to reflect the version of SQL that you are using in each of the 9.1x database schemas. For example if you are using SQL SERVER 2005, the compatibility level should be 90.
- ▶ HP Business Service Management does not support setting the time zone to half hour time zones relative to GMT, for example GMT+6:30 Indian. This may cause problems during data aggregation, which is performed on the hour.

Web Servers

To work with HP Business Service Management, the Gateway server(s) must run a Web server. In Linux environments, you must use the Apache HTTP Server. In Windows environments, you can select between:

- ▶ **Microsoft Internet Information Server (IIS).** If you plan to run HP Business Service Management on IIS, you should install the IIS prior to HP Business Service Management installation. During HP Business Service Management server installation, the IIS settings are automatically configured to work with HP Business Service Management.

Notes:

- ▶ When using the IIS Web Server, BSM only supports the IIS default application pool.
- ▶ If you are installing on Windows 2008 and using IIS 7, you must create the appropriate roles for the IIS. For details, see "Microsoft Internet Information Server (IIS)" on page 153

-
- ▶ **Apache HTTP Server.** A version of the Apache HTTP server is installed during HP Business Service Management server installation. It has been adapted by HP for HP Business Service Management. If you plan to use HP Business Service Management with the Apache HTTP Server, you select the Apache HTTP Server during installation.

For information on setting up the Web server to work with HP Business Service Management, see "Working with the Web Server" on page 152 (Windows platforms), or "Working with the Web Server" on page 162 (Linux platforms).

BSM Database Server

HP Business Service Management requires the following types of databases/user schemas, which you set up on either Microsoft SQL Server or Oracle Server:

- ▶ **Management database.** For storage of system-wide and management-related metadata for the HP Business Service Management environment. HP Business Service Management requires one management database.
- ▶ **RTSM.** For storage of configuration information as configuration items (CIs) that is gathered from the various HP Business Service Management and third-party applications and tools, or created/configured by BSM users. This information is used when building HP Business Service Management views.
- ▶ **RTSM history database.** For storage of changes, over time, of the RTSM configuration items (CIs). This information can be viewed in the form of CI changes as well as snapshots.
- ▶ **Profile database(s).** For storage of raw and aggregated measurement data obtained from the HP Business Service Management data collectors. Although only one profile database is required, you can store profile data in multiple databases, if required.
- ▶ **Business Process Insight database.** For storage of the Business Process Models created using the Business Process Insight Modeler. For details on the Business Process Insight database, see "BPI Server Database Requirements" in the *Business Process Insight Server Administration Guide*.
- ▶ **Event schema.** For storage of events and OMi topology synchronization.

Part of the process of deploying HP Business Service Management servers requires connecting to these databases. If you are installing HP Business Service Management for the first time, you can manually create these databases directly on the database server(s) before server installation, or you can allow HP Business Service Management to create the databases for you, using the Setup and Database Configuration utility.

For detailed information on deploying the database servers in your system for use with HP Business Service Management, and creating the databases/user schemas manually, see the *HP Business Service Management Database Guide* PDF.

The procedure for setting database parameters is described in "Server Deployment and Setting Database Parameters" on page 167.

Note: If you need to verify the integrity of the databases, you can run the database schema verification. For details, see Appendix D, "Database Schema Verification" in the *HP Business Service Management Database Guide* PDF.

BSM Data Sources

HP Business Service Management data sources are responsible for collecting performance and event data from various points throughout the infrastructure, as well as from external locations, and feeding it into a central repository. The data is used to monitor and analyze events and the performance of business applications and IT infrastructure and alert staff to performance and threshold breaches. Some data collectors can also report the topology that they are monitoring to HP Business Service Management.

Data Collectors

Data collectors are installed and administered separately. Downloading and running data collectors require separate licensing. Each data collector can be downloaded from the HP Business Service Management Downloads page, accessed from Platform Administration (**Admin > Platform > Setup and Maintenance > Downloads**). For details, see "Downloads Overview" in *Platform Administration*.

You can install the following data collectors on machines in your enterprise network environment or at remote locations:

- ▶ **Business Process Monitor (BPM)**. Emulates the end-user experience by running transactions (virtual business processes) and collecting availability and response time data.
- ▶ **SiteScope**. Collects key performance measurements and reports topology on a wide range of back-end infrastructure components, including Web, application, database, and firewall servers.
- ▶ **Real User Monitor (RUM)**. Measures the end-user experience of real users from a network/server perspective by monitoring real user traffic and collecting network and server performance data in real time.
- ▶ **Business Process Insight (BPI)**. Provides visibility into the health and performance of the business processes that are running over IT infrastructure to enable assessment of the business impact of delays or blockages in processes due to an IT performance problem.
- ▶ **TransactionVision**. Measures the health, performance and business impact of enterprise transactions and provides reporting on transaction activity.

Note: **HP Diagnostics** is licensed and installed separately and can act as a data collector for BSM.

After the data collectors are installed and configured, you further define their settings in End User Management Administration (**Admin > End User Management**) and System Availability Management Administration (**Admin > System Availability Management**). End User Management Administration enables you to centrally manage your monitoring environment for Business Process Monitor and Real User Monitor. System Availability Management enables you to access hosted instances of SiteScope. Business Process Insight and TransactionVision each have their own administration areas (**Admin > Business Process Insight** and **Admin > Transaction Management**).

You can deploy monitors, configure eventing and alert schemes, and manage and organize your monitor environment all from within the HP Business Service Management platform.

Data from HP Software Applications and Integrations

HP Business Service Management has the ability to integrate with BTO products, with applications that are part of Business Service Management, and with external applications.

These integrations enable the flow of data from application to application as well as the flow of events from the applications to Business Service Management and to its Operations Management component, depending on the applications. You can drill down from BSM to some of the relevant applications.

You can integrate with the following HP Software applications and tools:

- **HP BSM Integration Adapter**
- **HP Network Node Manager i**
- **HP Operations Manager**
- **HP Operations Orchestration**
- **HP Service Manager**
- **HP Release Control**

For details on these integrations, see "Business Service Management Integration with Other Applications" in *Solutions and Integrations*.

Additional Proprietary Components

BSM administrators deploy the Discovery Probe to enable the Discovery process, which aids in modeling the IT world. In addition, administrators use HP scripting tools to create the scripts that are used by Business Process Monitor to collect data for monitored applications.

Data Flow Probe

The Data Flow Probe enables you to collect data about your IT infrastructure resources and their interdependencies. This process discovers resources such as applications, databases, network devices, servers, and so on. The Data Flow Probe is the main component responsible for receiving discovery tasks from the server, dispatching them to the IT components, and sending the results back to the RTSM through the server. For details on the discovery process and Data Flow Probe deployment, see *Data Flow Management*.

Scripting Tools

HP Business Service Management scripting tools enable you to record the end-user actions that represent the key business transactions whose performance you want to monitor using Business Process Monitor. You save the transactions in recorded scripts. The table below describes the scripting tools that are available. For additional information on Business Process Monitor scripting tools, including script recording tips, see *Using End User Management*.

Tool	Description
HP Virtual User Generator (VuGen)	Enables you to record scripts for a large variety of protocols. This is the recommended tool for recording Business Process Monitor scripts. You download VuGen from the Downloads page, accessed from the Setup and Maintenance tab in Platform Administration. For details on using VuGen, see the HP Virtual User Generator documentation. For information on using HP LoadRunner scripts in HP Business Service Management, contact HP Software Support.
QuickTest Professional (for use with Windows-based Business Process Monitor only)	Enables you to record scripts for Web-based applications that include Java applets and ActiveX. For details on using QuickTest Professional, refer to the documentation installed with the product.

Third-Party Components

- ▶ **Database Server.** HP Business Service Management requires connection to a database server. The database server is used to store:
 - ▶ System-wide and management-related data, which includes administrative settings and customer-configured information
 - ▶ Profile data, which includes data collector settings and collected metrics
 - ▶ Configuration item (CI) data, which includes the CIs used to model your IT infrastructure and the relationships between them.

For more information on using database servers in HP Business Service Management, see the *HP Business Service Management Database Guide* PDF.
- ▶ **Mail Server.** The mail server is used to send alerts and scheduled reports to designated recipients.
- ▶ **SNMP Server.** A connection to an SNMP server may be implemented to receive SNMP traps sent by the HP Business Service Management alerting mechanism.

- ▶ **SiteScope Integration Monitors.** HP Business Service Management supports integration of data from third-party systems via SiteScope Integration Monitors, and to third-party systems, using HP Business Service Management APIs. For more information on SiteScope Integration Monitors, see "Working with SiteScope Integration Monitors" in *Using SiteScope*.
- ▶ **Integration Adapter.** BSM supports integration of events from third-party systems via the BSM Integration Adapter. For more information, see "HP BSM Integration Adapter" in *Solutions and Integrations*.

Note: Before performing integrations with third-party products, review the information in "Best Practices for Integrating Third-Party Data" in *Solutions and Integrations*.

Bus Communication Among BSM Components

A bus is a virtual communications channel between BSM servers.

The following functionality is provided by the Bus:

- ▶ **High availability for communication between the Gateway and Data Processing servers.**

The bus uses a JMS-based messaging system for communication between the servers. A broker process on each server receives and delivers messages between the servers. Bus clustering allows multiple brokers to detect dropped server connections and to reconnect without data loss.

► **Transfer of monitoring data.**

Data collectors send raw monitoring data via HTTP/HTTPS protocol to the Gateway Server. The Gateway Server formats the raw data and sends it to the Data Processing Server via the Bus. In the event that the Online BLE is experiencing downtime, the bus preserves the data until the Online BLE is again operational, thus guaranteeing that the Alert Engine has all of the data to perform its calculations on. Service Health uses the online BLE to listen to the Bus, and Service Level Management uses the offline BLE to listen to the Bus. Both applications display the formatted data to the user.

► **Transfer of alerts.**

Each Data Processing Server can generate alerts as a result of the data aggregation process. These alerts are sent through the bus to the Alerts Engine and on to the user's e-mail, pager, or SMS.

7

High Availability for BSM

This chapter includes:

- ▶ Overview of High Availability Options on page 101
- ▶ Load Balancing for the Gateway Server on page 102
- ▶ High Availability for the Gateway Server on page 105
- ▶ High Availability for the Data Processing Server on page 107
- ▶ Configuring BSM Data Collectors in a Distributed Environment on page 121
- ▶ Troubleshooting on page 122

Overview of High Availability Options

You can improve your system availability and reliability using high availability options that combine multiple servers, external load balancing, and failover procedures.

Implementing a high availability configuration means setting up your BSM servers so that service is continuous despite power outages, machine downtime, and heavy load.

High availability is implemented in two layers:

- ▶ **Hardware infrastructure.** This layer includes redundant servers, networks, power supplies, and so forth.
- ▶ **Application.** This layer has two components:
 - ▶ **Load balancing.** Load balancing divides the work load among several computers. As a result, system performance and availability increase.

External load balancing is a software and hardware unit supplied by an outside vendor. This unit must be installed and configured to work with BSM applications.
 - ▶ **Failover.** Work performed by the Data Processing Server is taken over by a backup server if the primary server or component fails or becomes temporarily unavailable.

Implementation of load balancing and failover is discussed in detail throughout this chapter.

Note: HP Software Professional Services offers consulting services to assist customers with BSM strategy, planning and deployment. For information, contact an HP representative.

Load Balancing for the Gateway Server

When you install multiple HP Business Service Management Gateway Servers, HP Business Service Management can utilize external load balancing mechanisms to help ensure the even distribution of processing and communication activities across the network. This is particularly important in cases of high load, to avoid overwhelming any single server.

It is generally recommended that you use one or more external load balancers at the entry to HP Business Service Management.

This section includes the following topics:

- "Configuring Load Balancing" on page 103
- "Notes and Limitations" on page 104

Configuring Load Balancing

- 1 Create two virtual hostnames. The virtual hostname must be a fully qualified domain name (FQDN), in the format `<servername>.<domainname>`. This requirement is necessary to support Lightweight Single Sign On authentication, which is enabled by default.

The first host name is for accessing the BSM Web site on the Gateway Server. This URL can be distributed to BSM users. The second host name is for the data collectors to access the Gateway Server. This URL must be used when configuring data collectors to communicate with BSM.
- 2 Enter the relevant load balancer host names in the Infrastructure Settings for the virtual servers. To do so, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Foundations**, select **Platform Administration - Host Configuration table**:
 - **Default Virtual Gateway Server for Application Users URL.** Virtual host name for the BSM Web site. The Gateway Server you are working on must be able to resolve this Virtual IP address. This means that **nslookup** for the **virtual host name for the application users** should return name and IP address when executed on this Gateway Server.
 - **Default Virtual Gateway Server for Data Collectors URL.** Virtual host name for Data Collectors. All data collectors must be able to resolve this Virtual IP address. This means that **nslookup** for the **virtual host name for the Data Collectors** should return name and IP address when executed on data collector server.
- 3 If your Load Balancer acts as a Reverse Proxy, in the Reverse Proxy Configuration pane, set the following parameters:
 - **Enable Reverse Proxy parameter = true.**
 - **HTTP Reverse Proxy IPs.** Use the internal IP addresses of the load balancers.

- 4 After changing the reverse proxy settings, restart the HP BSM service on the BSM Gateway and Data Processing servers.
- 5 Configure the load balancer for data collector access. All data collectors must be able to access the Virtual IP of the Load Balancer. Use the standard settings for the load balancer, but set the following:
 - The Load balancing method should be **Round robin**.
 - Use the following KeepAlive URI:
 - Send String: **GET /ext/mod_mdrv_wrap.dll?type=test**
 - Receive String: **Web Data Entry is up**
- 6 Configure the load balancer for user access.
 - Use the standard settings for the load balancer, but set persistency to **stickiness by session enabled** or **Destination Address Affinity** (depending on the Load Balancer). If neither of these options are available and the choice is between **Cookie based** stickiness and **IP based** stickiness, then we recommend trying **IP based** stickiness. If this is not done properly, you may experience intermittent user interface failures.
 - Use the following KeepAlive URI:
 - Send String: **GET /topaz/topaz_api/loadBalancerVerify_centers.jsp**
 - Receive String: **Success**
- 7 Configure the load balancer for data access.

Notes and Limitations

- A software load balancer is not supported.
- If you use two load balancers for failover, you must ensure that you configure the hostnames of both load balancers on the DNS server machine. You can then specify the machine name, hostname's FQDN, or URL of either load balancer when this information is required for the data collectors, or in the browser to open the HP Business Service Management site.

- If two Gateway servers are installed into different drive paths, for example, one was installed onto the C:\ drive and the other onto the E:\ drive, BSM may not be able to be accessed.

Workaround: Create a duplicate path on the C:\ drive by copying E:\<HP BSM root directory>\conf\settings to C:\HP BSM root directory>\conf\settings.

- If you use two load balancers for failover, and the load balancers each work with more than one server type, you should define a unique virtual hostname on each load balancer for each server type, map the virtual hostnames to the actual hostnames of the corresponding servers, and ensure that you configure all the virtual hostnames on the DNS server machine. You can then specify either of the relevant virtual hostnames for each data collector, or in the browser to open the HP Business Service Management site.

High Availability for the Gateway Server

HP Business Service Management provides high availability for the Gateway Servers to ensure that data gets to its destination and that the users can use BSM applications in the event of a server failure.

This section includes the following topics:

- "Protected Delivery for Incoming Data" on page 106
- "High Availability for Service Health" on page 107

Protected Delivery for Incoming Data

HP Business Service Management provides protected data delivery for monitor data. Protected data delivery means that the data is not deleted from one data store until it is forwarded to, and stored in, the next data store.

Note: HP Professional Services offers best practice consulting on this subject. For information on how to obtain this service, contact your HP representative.

HP Business Service Management supports the following mechanisms to help ensure high availability for the raw data:

- ▶ If the Web server of the Gateway Server machine fails, the data is either redirected to another Gateway Server by the load balancer, or is queued on the data collector until the Web Server is up.
- ▶ If the Web server of the Gateway Server machine receives the data, but the bus is down, the data is stored on the data collector until the bus is up again.
- ▶ If the bus receives the data, but the monitoring data loader is down, the data is stored on the bus until the monitoring data loader is up again. The data is then sent to the database.

High Availability for Service Health

HP Business Service Management provides high availability for Service Health on the Gateway Server to ensure that users can continue working with Service Health even if a Gateway Server fails while a user is in the middle of a session.

When a user logs in to HP Business Service Management and starts working with Service Health, the session information is registered on a specific Gateway Server and the load balancer sends all communications related to that session to the same Gateway Server. If that Gateway Server fails, the load balancer redirects the session to another Gateway Server and the session is re-registered on the new Gateway Server. The user continues working without any interruption of service and without having to log in to HP Business Service Management again.

The load balancer for the Gateway Server must be set with **stickiness by session enabled**. For details, see "Configuring Load Balancing" on page 103.

Caution: It is possible that in certain situations, the transition from one Gateway Server to another could take a few seconds. During this transition, errors may be received for some user actions.

High Availability for the Data Processing Server

To ensure high availability, you should install a backup Data Processing Server. For HP Business Service Management to function properly in the event of a primary Data Processing Server failure, the backup Data Processing Server can take over.

Tip: It is recommended that when you install the primary and backup Data Processing Servers, the servers should be comparable in terms of hardware, memory, and performance.

If the high availability for the Data Processing Server is enabled and a backup server is defined, in the event that one or more services becomes unavailable, the High Availability Controller performs automatic failover and moves the services to the backup server. The server retrieves the current configuration from the management database and continues to provide the services as the new active Data Processing Server.

You can also use the JMX console to manually reassign services to the backup server. You may want to do this if for example, you are planning a maintenance on one of the Data Processing Servers. Moving the services manually can reduce BSM's downtime.

Note: When deploying a new HP Business Service Management installation, the first Data Processing Server started becomes the default server for the assigned Data Processing Server services—that is, it becomes the primary Data Processing Server. If a second Data Processing Server is started, you can assign it to act as a backup server.

This section includes the following topics:

- "Services Assigned to the Server" on page 109
- "Services Managed by the High Availability Controller (HAC)" on page 111
- "Configuring Automatic Failover" on page 113
- "Reassigning Services with JMX Console" on page 115
- "Manually Reassigning Services" on page 116
- "Manually Disabling Data Aggregator Services" on page 120

Services Assigned to the Server

Various processes are assigned to the Gateway and Data Processing Servers. Each process is responsible for running specific services. You can use the JMX console to view the services running on the BSM servers or on a specific server, such as the Data Processing Server.

To view services via the JMX Web console:

1 In a Web browser, open:

<http://<Data Processing Server machine name>:8080/jmx-console>

When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

2 In the **Topaz** section, select **service=hac-manager**.

3 Under **java.lang.String listAllAssignments()** from the database, click **Invoke**.

If you want to view the services of a specific server, such as the Data Processing Server, enter the name of the server in the parameter value. If you want to view all services, leave the parameter value for the server name empty.

The processes running on the server are displayed in a table. The JMX online table contains the following columns:

Column Name	Description
Service	The name of the assigned service.
Customer	The ID of the customer to which the service is assigned. The default customer ID for an individual HP Business Service Management system (one not managed by HP Software-as-a-Service) is 1. A service with a customer id of -1 is a global service used by all customers in a SaaS deployment.
Process	The name of the Data Processing Server and the name of the JVM process handling the service. The length of time the server has been running and the last time it was pinged are also displayed.
Assigned	Whether the service assignment is currently active or not, the date the service was assigned, and the length of time it has been assigned are displayed.
State	The current state of the service. Valid states are: <ul style="list-style-type: none"> ➤ 1 – Stopped ➤ 2 – Starting ➤ 3 – Stopping ➤ 4 – Running ➤ -1 – Failed ➤ -2 – Failed to stop ➤ -3 – Failed to start The date that the service acquired the state, and the length of time that it has been in the state are displayed.
Srv. Sign	Server signature.
State Sign	State signature (should match the server signature).

Services Managed by the High Availability Controller (HAC)

The Data Processing Server services that can be managed by HAC are described in the following table, including:

- Name of the process in JVM
- Name the High Availability Controller (HAC) uses for the process
- The services running on the process
- A description of the process

JVM Process Name	HAC Process Name	Service Name	Description of Service Location of Log File
Mercury AS	mercury_as	KPI_ENRICHMENT	KPI_Enrichment service is responsible for adding dashboard KPIs to CIs that were added to the model by external monitoring systems. The KPIs to add and the CIs to which the KPIs are added are configurable.
		BSM_DT	BSM_DT handles the configured downtimes in the system. Downtimes can be configured onto CIs and can be configured to affect alerts, events, reports, KPI calculations, and monitoring.
		VERTICALS	Verticals service is for SAP that ensures compatibility with BSM. SAP service links data retrieved from SiteScope and Business Process Monitors to SAP related entities brought from the RTSM.
		EUM_ADMIN	EUM_ADMIN handles End User Management Administration where Business Process Monitors and Real User Monitors are configured for monitoring.

JVM Process Name	HAC Process Name	Service Name	Description of Service Location of Log File
mercury_odb	odb	BSM_ODB	The RTSM is a central repository for configuration information that is gathered from the various BSM and third-party applications and tools. This information is used to build HP Business Service Management views.
hpbsm_bizImpact	business_impact_service	BIZ_IMPACT	The Business Impact component enables you to see the business CIs and SLAs that are impacted by another CI in Service Health.
		LIV_SERVICE	Local Impact View enables you to also create local impact views in Service Health. These are independent of all other views. When you modify indicator definitions on a CI within a local impact view, this has no effect on this CI in all other views.
bpi_process_repository	bpi_process_repository	PROCESS_REPOS	Responsible for maintaining all Business Process Insight configurations when Business Process Insight is not installed on a separate server.
hpbsm_offline_engine	offline_engine	NOA	The New Offline Aggregator service validates and synchronizes new tasks for the offline aggregator on an hourly or daily basis.
hpbsm_marble_supervisor	marble_supervisor	DASHBOARD	Dashboard service on the Data Processing Server is responsible for online business logic calculations for Service Health.

JVM Process Name	HAC Process Name	Service Name	Description of Service Location of Log File
hpbsm_pmanager	pmanager	PM	The Partition and Purging Manager splits fast-growing tables into partitions at defined time intervals. After a defined amount of time has elapsed, data in a partition is no longer accessible for use in BSM reports. After an additional, defined amount of time, that partition is purged from the profile database.
hpbsm_opr_bakend	opr_bakend	OPR	Responsible for the Operations Management application.

Configuring Automatic Failover

You can configure automatic reassignment of services running on a primary Data Processing Server to a backup Data Processing Server. To configure the automatic reassignment of services running on a primary Data Processing Server to a backup Data Processing Server, you must define a backup Data Processing Server in the JMX console and enable automatic failover.

Note: If you enable automatic failover as well as set the **keep alive timeout** to less than ten minutes, this can cause BSM services to move to the backup server after a restart. To prevent this from happening, when disabling BSM, shut down the backup server before the primary server. When enabling BSM, enable the primary server and verify that all services have started before enabling the backup server.

Defining a Backup Server

You must use the JMX console to define or remove a backup Data Processing Server. You can also view your high availability configurations.

To use the JMX console to define a backup server:

- 1** In a Web browser, open:

http://<Data Processing Server machine name>:8080/jmx-console

When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

- 2** In the **Topaz** section, select **service=hac-backup**.

- 3** Locate **addBackupServer** and enter the following values:

- ▶ **primaryServerName**. The name of the primary server.
- ▶ **backupServerName**. The name of the backup server.

Use the machine name for both these parameters. If you are unsure of the machine name, you can use the **listservers** method described below to retrieve the name of the machines already configured.

- 4** Click **Invoke**.

To remove a backup server:

- 1** Follow steps 1 and 2 above for accessing the JMX and **hac-backup** service.

- 2** Locate **removeBackupServer** and enter the following value:

- ▶ **primaryServerName**. The name of the primary server for which you are removing the backup server.

- 3** Click **Invoke**.

To view your high availability configuration:

- 1** Follow steps 1 and 2 above for accessing the JMX and **hac-backup** service.

- 2** Locate **listservers** and click **Invoke**.

The result displays a list of **Servers** and **Backup Servers**. If there are no backup servers defined or if high availability is not enabled, you get a message saying automatic failover is disabled.

Enabling Automatic Failover

You enable either using the Infrastructure Settings in the BSM interface or in the JMX console. You can also use the JMX console to check whether high availability is enabled.

To enable automatic failure in Infrastructure Settings:

- 1** Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
- 2** Choose **Foundations**, select **High Availability Controller**, and locate the **Automatic Failover Enabled** entry in the General Properties table.
- 3** Modify the value to **true**. The change takes effect immediately.

To enable automatic failover in the JMX:

- 1** In a Web browser, open:
<http://<Data Processing Server machine name>:8080/jmx-console>
When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
- 2** In the **Topaz** section, select **service=hac-backup**.
- 3** Locate **void setAutomaticFailoverEnabled ()**, select **True**, and click **Invoke**.

To check whether automatic failover has been configured:

- 1** Follow steps 1 and 2 above for accessing the JMX and **hac-backup** service.
- 2** Locate **void getAutomaticFailoverEnabled ()**, click **Invoke**.

Reassigning Services with JMX Console

You can move services between Data Processing Servers as server availability and resource issues arise. Reassigning services can also limit downtime during maintenance of the Data Processing Servers.

You do not have to have high availability enabled to perform this procedure and the source and destination servers do not have to have been configured for high availability.

To use the JMX console to reassign services between Data Processing Servers:

- 1** In a Web browser, open:
<http://<Data Processing Server machine name>:8080/jmx-console>
When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
- 2** In the **Topaz** section, select **service=hac-backup**.
- 3** Locate **moveServices()** and enter the following values:
 - ▶ **customerId**. The default customer ID for a regular HP Business Service Management installation is **1**. HP Software-as-a-Service customers should use their customer ID.
 - ▶ **srcServer**. The name of the source server from where you are moving services.
 - ▶ **dstServer**. The name of the destination server to where you are moving the services.

Use the machine name for both these parameters. If you are unsure of the machine name, you can use the **listservers** method described above to retrieve the name of the machines already configured.
 - ▶ **groupName**. Leave this parameter value blank.
- 4** Click **Invoke**. All services running on the source server are moved to the destination server.

Manually Reassigning Services

Caution: This section is for advanced users only.

You can manually reassign services running on a primary Data Processing Server to a backup Data Processing Server should it be necessary. Since a service can only be active on one Data Processing Server, you must either remove the existing assignment, or make it inactive, before reassigning the service to a different Data Processing Server.

To reassign a service, you can either add a new assignment, or activate a previously defined, but inactive, assignment.

Tip: You can check that services have been reassigned, activated, or inactivated correctly by viewing the service status in the JMX Web console. For details, see "Services Assigned to the Server" on page 109.

Removing a Service's Assignment

Removing a service's assignment deletes the entry from the HA_TASKS table in the management database so that it must be added as a new assignment if you wish to use it again in the future.

To remove a service's current assignment:

1 In a Web browser, open:

<http://<Data Processing Server machine name>:8080/jmx-console>

When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

2 In the **Topaz** section, click **service=hac-manager**.

3 Under **removeAssignment()**, enter the following data:

- **customer_id.** The default customer ID for an individual HP Business Service Management system is **1**. HP Software-as-a-Service customers should use their customer ID in this field.

Note: The **customer_id** for the PM and NOA services is always -1, as they are services assigned to the system as a whole, as opposed to a specific customer.

- **serviceName.** The name of the service for which you are removing the current assignment.

- ▶ **serverName.** The name of the Data Processing Server to which the service is currently assigned.
 - ▶ **processName.** The name of the process (such as **mercury_as**, **mercury_online_engine**, **mercury_offline_engine**, **topaz_pm**).
- 4 Click **Invoke**. The assignment for the service is removed from the specified Data Processing Server.

Changing the Status of an Assigned Service

You can leave the assignment of a service to a specific Data Processing Server in the HA_TASKS table in the management database, but make it active or inactive by changing its assigned value.

Note: The HA_TASK_ASSIGN table from previous versions is obsolete. Use the HA_TASKS table.

To change the assigned value of an existing assignment:

- 1 In a Web browser, open:
<http://<Data Processing Server machine name>:8080/jmx-console>
When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
- 2 In the Topaz section, click **service=hac-manager**.
- 3 Under **changeAssignment()**, enter the following data:
 - ▶ **customerId.** The default customer ID for a regular HP Business Service Management installation is **1**. HP Software-as-a-Service customers should use their customer ID.

Note: The customer_id for the PM and NOA services is always -1 as they are services assigned to the system as a whole, as opposed to a specific customer.

- **serviceName.** The name of the service for which you are changing the assignment value.
 - **serverName.** The name of the Data Processing Server to which the service is assigned.
 - **processName.** The name of the process.
 - **assignValue.** The assigned value for the assignment. Any number between -9 and 9 is valid. The value **1** makes the assignment active and any other number makes it inactive.
- 4** Click **Invoke**. The assignment for the service is changed according to the **assignValue** entered.

Adding an Assignment for a Service

You can add an assignment for a service to a specific Data Processing Server and either activate it immediately, or keep it inactive until needed. This is useful when working with a primary and a backup Data Processing Server. Assignments for all the services can be created for each server, with the assignments to the primary Data Processing Server being active, and the assignments to the backup Data Processing Server being inactive.

To add a new assignment for a service:

- 1** In a Web browser, open:

<http://<Data Processing Server machine name>:8080/jmx-console>

When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

- 2** In the Topaz section, click **service=hac-manager**.

- 3** Under **addAssignment()**, enter the following data:

- **customer_id.** The ID of the customer for which the service is to be assigned. The default customer ID for an individual HP Business Service Management system (that is, one not managed by HP Software-as-a-Service) is **1**.

Note: The `customer_id` for the PM and NOA services is always -1 as they are services assigned to the system as a whole, as opposed to a specific customer.

- ▶ **serviceName.** The name of the service you are assigning.
 - ▶ **serverName.** The name of the new Data Processing Server to which the service is being assigned.
 - ▶ **processName.** The name of the process.
 - ▶ **assignValue.** The assigned value for the assignment. Any number between -9 and 9 is valid. The value **1** makes the assignment active and any other number makes it inactive.
- 4** Click **Invoke**. The assignment for the service is added for the specified Data Processing Server.

Manually Disabling Data Aggregator Services

The data aggregator can be disabled in System Health (preferred method). However, if you need to disable data aggregator services but either do not have or can not use System Health, you can perform this manual procedure.

To disable the offline aggregation and business logic engine services on the Data Processing Server:

- 1** Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Foundations**.
- 2** Select **Offline Aggregator**.
- 3** Edit the **Run Aggregator** parameter. Change the setting to **False**. The change takes effect immediately.

Configuring BSM Data Collectors in a Distributed Environment

This section describes how to configure the HP Business Service Management data collectors to work in a distributed HP Business Service Management deployment.

Business Process Monitor and Real User Monitor

For Business Process Monitors to perform their work, you must specify the Gateway Server URL in the Business Process Monitor Admin application on each host machine on which the Business Process Monitor is running. Edit the Gateway Server URL entry in the Configure Instance page for each Business Process Monitor instance. For more information, see "Business Service Management Registration Properties Area" in *the Business Process Monitor Administration* PDF.

For Real User Monitors to perform their work, HP Business Service Management requires you to specify the Gateway Server URL in the Real User Monitor Web Console. For more information, see "BSM Connection Settings" in the *Real User Monitor Administration* PDF.

Specify the Gateway Server address as follows:

- If you install one Gateway Server, specify the URL of this machine.
- If you cluster two or more Gateway Servers behind a load balancer, specify the URL of the load balancer.

If you use two load balancers for failover, specify the URL of either load balancer, and ensure that you configure the host names of both load balancers on the DNS server machine.

SiteScope

For SiteScopes to perform their work, you must specify the Gateway Server URL in each SiteScope profile, using HP Business Service Management System Availability Management (**Admin > System Availability Management**). For details, refer to "Configuring the Connection" in *Using System Availability Management*.

If you use a load balancer and have defined virtual IPs or URLs, you use the virtual IPs or URLs when defining the Gateway Server URL. If you use two load balancers for failover, specify the URL of either load balancer and ensure that you configure the hostnames of both load balancers on the DNS server machine.

For more information on configuring high availability for SiteScope, see the *HP SiteScope Failover Manager Guide* PDF.

Business Process Insight

Refer to the *Business Process Insight Server Administration Guide* PDF for details on how to configure for high availability.

Troubleshooting

This section contains troubleshooting information about High Availability related issues.

Primary DPS Server fails

If your primary DPS server was running Domain Manager process (default) and it crashes, you must reassign this process to the backup DPS.

To assign the Domain Manager process to a DPS:

From the DPS server, run the following file: **<HPBSM Home Directory>\Sonic\bin\setDomainManager.bat** (or **.sh** for linux).

8

Deployment Configurations

This chapter includes:

- One-Machine Deployment on page 123
- Distributed Deployment on page 124
- Load Balancing and High Availability on page 125
- APM Starter Deployment on page 128

Tip: It is highly recommended to use the capacity calculator to determine the scope of your deployment and the required hardware profile of each machine in your installation. For details, see "Using the Capacity Calculator" on page 83.

One-Machine Deployment

A one-machine deployment has the Gateway Server and Data Processing Server installed on the same machine.

A one-machine deployment can be used for many installations scenarios as long as the machine has the required hardware to handle the capacity.

To choose a one-machine deployment, select the **Typical** setup type in the HP Business Service Management installation wizard.

Distributed Deployment

A distributed deployment is when one instance of a Gateway Server is installed on one machine and the Data Processing Server is installed on a second machine.

To set up a distributed deployment:

During HP Business Service Management installation, specify the server type you want to install on each machine.

- ▶ When installing the Gateway Server, select **Gateway Server** as the setup type.
- ▶ When installing the Data Processing Server, select **Data Processing Server** as the setup type.

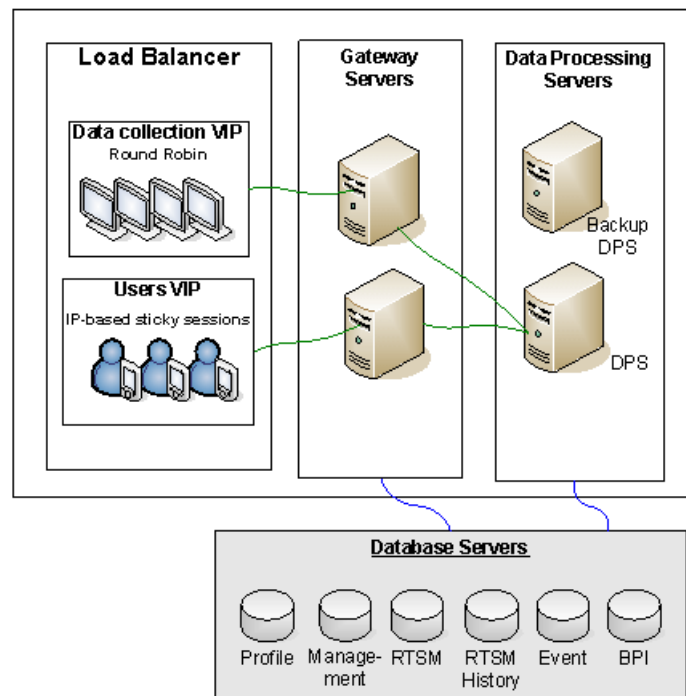
The order in which you install these servers is not important.

For details on installing HP Business Service Management on a Windows platform, see "Installing BSM Servers on a Windows Platform" on page 147. For details on using the Setup and Database Configuration utility, see "Server Deployment and Setting Database Parameters" on page 167.

Load Balancing and High Availability

Load balancing and high availability can be implemented in one-machine or distributed deployments. You configure load balancing by adding an additional Gateway Server and high availability by adding a backup Data Processing Server.

The diagram below illustrates load balancing and high availability for a distributed deployment but the same configuration can be used if the Gateway Server and the Data Processing Server have been installed on one machine.



Note: Data Processing Servers can run concurrently with additional Data Processing Servers as long as the same service is not being run concurrently on more than one machine.

Benefits of a Multi-Server Deployment

Deploying multiple servers for HP Business Service Management for either a one-machine deployment or a distributed deployment gives you the following benefits:

- ▶ Provides scaling solutions for your HP Business Service Management system.
- ▶ Multiple Gateway Servers can be placed behind a load balancer to divide load and improve system performance. For details on load balancing, see "Load Balancing for the Gateway Server" on page 102.
- ▶ Backup machines for the HP Business Service Management servers allow high availability options to be used to improve system availability and reliability. For details on high availability, see "High Availability for BSM" on page 101.

Deploying Multiple Servers

When deploying multiple HP Business Service Management servers, you must perform the following steps:

- ▶ At the end of the server installation process, use the Setup and Database Configuration utility to establish connectivity between the server and the databases. You must specify the same database and connection parameters for each HP Business Service Management server (whether the servers are at the same location or geographically separated). For details on using the Setup and Database Configuration utility, see "Server Deployment and Setting Database Parameters" on page 167.
- ▶ After installing HP Business Service Management servers, point HP Business Service Management data collectors (Business Process Monitor, SiteScope, Real User Monitor, TransactionVision, Business Process Insight) to the server or load balancer with which they must communicate to perform their work. For details, see "Configuring BSM Data Collectors in a Distributed Environment" on page 121.
- ▶ Ensure that the Gateway servers are accessible from any standard Internet or intranet connection, either through HTTP or HTTPS.

- ▶ Ensure that each server has a user account with administrative rights to the database servers.
- ▶ Create a common temporary directory to hold the temporary images created by the Gateway Servers when generating scheduled reports. For details, see "How to Modify the Location and Expiration of Temporary Image Files" in *Platform Administration*.

Notes and Limitations

- ▶ If HP Business Service Management servers, including the database servers, are installed on multiple network segments, it is highly recommended to minimize the number of hops and the latency between the servers. Network-induced latency may adversely affect the BSM application and can result in performance and stability issues. We recommend the network latency should be no more than 5 milliseconds, regardless of the number of hops. For more information, contact HP Software Support.
- ▶ Because HP Business Service Management uses Remote Method Invocation (RMI) calls between servers, placing firewalls between BSM servers is not supported.

APM Starter Deployment

The APM Starter deployment allows you to access the core functionality of BSM while using the minimum hardware. This can later be ramped up to increase performance and capacity.

APM Starter includes the following APM components: BSM one-machine server, RTSM, SiteScope and BPM deployed on the same virtual machine. More components and applications can be included at a later date. For details, speak to HP Software Support.

Note: If you anticipate that you will require greater capacity or performance within less than a year, we recommend that you plan the deployment according to these requirements and not use the APM Starter deployment.

Installation Notes

Installing an APM starter deployment is similar to most BSM installations and follows the main deployment workflow. For details, see "Deployment Workflow" on page 17. However, there are few differences.

- When installing the data collectors, install BPM first.
- When installing SiteScope, change the port to 8090.

System Capacity

The APM Starter deployment was tested to measure operating capacity. This section demonstrates the results of these tests.

Machine Details

Operating System	Windows
CPUs	4
Memory	8 GB
Database	Oracle 11, MS SQL 2008 EE SP2

Capacity

Product Area	Item	Item Type	Capacity
RTSM Capacity	CIs and relationships	Model	10000
	Active TQLs	Model	150
Users	Logged In Users	Users	25
	Service Health Users	Users	10
	Defined Users	Users	150
SLM	SLAs	SLM	10
	Total CIs	SLM	2000
BPM	Applications	MetricData	20
	Transactions	MetricData	100
	Locations	MetricData	5
	Trx-Loc Combinations	MetricData	150
	Max EPS	MetricData	1
SiteScope	Monitors	SAM	1000
	Measurements	SAM	4000
	Monitored CIs (Hosts + Software Elements)	SAM	150
	Max EPS	SAM	50

9

System Requirements

Note: The HP Business Service Management release notes, available with the HP Business Service Management package, contains the latest information on support matrixes with the supported operating systems for HP Business Service Management components. It also lists support for the current and previous HP Business Service Management versions.

This chapter includes:

- ▶ HP Business Service Management Servers on page 132
- ▶ HP Business Service Management Databases on page 135
- ▶ Client Requirements for Viewing BSM on page 139
- ▶ Server Environment Settings on page 142
- ▶ HP Business Service Management on Virtual Platforms on page 143

HP Business Service Management Servers

Computer/ Processor	<p>Windows:</p> <p>The following CPU types are supported (further CPU requirements also appear below, see Memory and CPU Requirements):</p> <ul style="list-style-type: none">▶ Intel Dual Core Xeon Processor 2.4 GHz or higher▶ AMD Opteron Dual Core Processor 2.4 GHz or higher <p>Tip: As Business Service Management performance is dependent upon processor speed, it is recommended to get the fastest possible processor speed to ensure proper performance.</p>
------------------------	--

Operating System	<p>Windows:</p> <ul style="list-style-type: none"> ▶ Windows Server 2003 Enterprise Edition SP2 or later (64 bit) ▶ Windows Server 2003 Standard Edition SP2 or later (64 bit) ▶ Windows Server 2003 R2 Enterprise Edition, including all service packs (64 bit) ▶ Windows Server 2003 R2 Standard Edition, including all service packs (64 bit) ▶ *Windows Server 2008 Enterprise Edition SP2 or later (64 bit) ▶ *Windows Server 2008 Standard Edition SP2 or later (64 bit) ▶ Windows Server 2008 R2 Enterprise Edition, including all service packs (64 bit) ▶ Windows Server 2008 R2 Standard Edition, including all service packs (64 bit) <p>Linux:</p> <ul style="list-style-type: none"> ▶ RedHat Enterprise Linux 5.3 (Intel x64 64 bit) ▶ RedHat Enterprise Linux 5.4 (Intel x64 64 bit) ▶ RedHat Enterprise Linux 5.5 (Intel x64 64 bit) ▶ RedHat Enterprise Linux 5.6 (Intel x64 64 bit) ▶ RedHat Enterprise Linux 5.7 (Intel x64 64 bit) <p>Note: For each of the supported versions of Linux, the entire Distribution (with OEM support) and the latest recommended Patch Cluster are required.</p> <p>*Important: If you are running Windows Server 2008 SP2, User Access Control (UAC) must be disabled during the installation process.</p>
Domain Name	Each BSM server must have a resolvable Fully Qualified Domain Name.

Web Server	<p>Windows:</p> <ul style="list-style-type: none"> ▶ Microsoft Internet Information Server (IIS) 6.0 ▶ Microsoft Internet Information Server (IIS) 7.0, 7.5 ▶ Apache HTTP Server 2.2.17 (adapted by HP for HP Business Service Management and installed during HP Business Service Management server installation) <p>Linux:</p> <ul style="list-style-type: none"> ▶ Apache HTTP Server 2.2.17 (adapted by HP for HP Business Service Management and installed during HP Business Service Management server installation)
------------	--

Memory and CPU Requirements

The following table lists the memory and CPU requirements according to some of the deployment scenarios available for BSM. To get the most accurate requirement information for your deployment, use the capacity calculator. For details, see "Using the Capacity Calculator" on page 83.

Certified Deployment	Server Type	Memory	CPU	Virtual Memory/ Swap Space
APM Basic	One machine	recommended 6 GB/ minimum 4 GB	4 CPU	6 GB
APM Advanced	Gateway	7 GB	8 CPU	8 GB
	Data Processing	16 GB	8 CPU	8 GB
OPS Basic	One machine	7 GB	4 CPU	6 GB
OPS Advanced	Gateway	9 GB	4 CPU	6 GB
	Data Processing	19 GB	8 CPU	8 GB

Certified Deployment	Server Type	Memory	CPU	Virtual Memory/ Swap Space
BSM Full	Gateway	9 GB	8 CPU	8 GB
	Data Processing	19 GB	8 CPU	8 GB

HP Business Service Management Databases

Hardware Requirements

The following table describes the hardware (CPU and memory) requirements recommended for the HP Business Service Management Oracle or Microsoft SQL database server:

Deployment	Number of Processors	Physical Memory
Standard	1 dual core	Minimum: 2G RAM Recommended: 4G RAM
Large	Minimum 2 dual core or 1 quad core	Minimum: 4G RAM Recommended: 8G RAM

For larger deployments, a separate database server is required for Business Process Insight and for TransactionVision. In smaller deployments, they can share the database server.

For details on the criteria for standard and large deployments of HP Business Service Management, see the *HP Business Service Management Database Guide* PDF.

Software Requirements - Oracle Server

The following table lists the Oracle servers supported for working with HP Business Service Management.

Database Release - Version	System Type
Oracle 10.2 (10.2.0.4 or later component specific release number 10.2.0.X) Enterprise Edition	64 bit
Oracle 10.2 (10.2.0.4 or later component specific release number 10.2.0.X) RAC Enterprise Edition	64 bit
Oracle 11.1.0.7 Enterprise Edition	64 bit
Oracle 11.2 (11g R2) Enterprise Edition	64 bit
Oracle 11.2 (11g R2) RAC Enterprise Edition	64 bit

Note:

- ▶ It is strongly recommended to apply the latest critical Oracle patches per your operating system. For details, consult the Oracle documentation.
 - ▶ Consult the Oracle documentation for supported platforms.
 - ▶ The Oracle Partitioning option must be enabled.
-

Examples of Tested Deployments - Oracle Server

The following table details those deployment environments that were tested by HP.

Database Release		Operating System
Version	System Type	
Oracle 11.2 (11g R2) Enterprise Edition	64 bit	Linux Enterprise Edition RHEL 5
Oracle 11.2 (11g R2) RAC Enterprise Edition	64 bit	Linux Enterprise Edition RHEL 5
Oracle 10.2.0.5 Enterprise Edition	64 bit	Linux Enterprise Edition RHEL 5
Oracle 11.2 (11g R2) Enterprise Edition	64 bit	Solaris 10

Software Requirements - Microsoft SQL Server

The following table describes the Microsoft SQL Servers supported for working with HP Business Service Management:

Database Release		
Version	System Type	Service Pack
Microsoft SQL Server 2008 R2 Enterprise Edition	64 bit	Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	32 bit	Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	64 bit	Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	32 bit	Service Pack 2
Microsoft SQL Server 2008 Enterprise Edition	64 bit	Service Pack 2

Database Release		
Version	System Type	Service Pack
Microsoft SQL Server 2005 Enterprise Edition	32 bit	Service Pack 3
Microsoft SQL Server 2005 Enterprise Edition	64 bit	Service Pack 3
Microsoft SQL Server 2005 Enterprise Edition	32 bit	Service Pack 4
Microsoft SQL Server 2005 Enterprise Edition	64 bit	Service Pack 4

Note:

- Only supported service packs should be installed.
 - Consult the Microsoft documentation for supported platforms.
-

Examples of Tested Deployments - Microsoft SQL Server

The following table details those deployment environments that were tested by HP.

Database Release			Operating System
Version	System Type	Service Pack	
Microsoft SQL Server 2008 R2 Enterprise Edition	64 bit	Service Pack 1	Windows 2008 R2 Enterprise Edition Service Pack 1

Database Release			Operating System
Version	System Type	Service Pack	
Microsoft SQL Server 2008 Enterprise Edition	32 bit	Service Pack 1	Windows 2008 Enterprise Edition Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	64 bit	Service Pack 1	Windows 2008 Enterprise Edition Service Pack 1 (64-bit)

Client Requirements for Viewing BSM

Display	<ul style="list-style-type: none"> ▶ Minimum: color palette setting of at least 256 colors Recommended: color palette setting of 32,000 colors
Resolution	▶ 1280x1024 or higher (recommended)
Supported Browsers	<ul style="list-style-type: none"> ▶ Microsoft Internet Explorer (IE) 9.0 ▶ Microsoft Internet Explorer (IE) 8.0 ▶ Microsoft Internet Explorer (IE) 7.0 ▶ Mozilla Firefox 3.6 ▶ Mozilla Firefox 5.0 ▶ Mozilla Firefox 6.0 ▶ Mozilla Firefox ESR 10.0 <p>Note: The browser must be set to accept all cookies.</p>
Flash Player	Adobe Flash 10.1 or later
Fonts	<p>The following fonts must be installed on client systems:</p> <ul style="list-style-type: none"> ▶ MS Gothic for Japanese locales ▶ Gulim for Korean locales ▶ SimSun for simplified Chinese locales ▶ Arial for all other locales

<p>Java Plug-in (to view applets)</p>	<p>Recommended: Version 6 update 31</p> <p>Supported: Version 6 update 18 and higher</p> <p>Note: You may not be able to view all HP Business Service Management applets with an earlier version of Java and you will need to download the latest version from the Java download site (http://www.java.com/en/download/manual.jsp) and install it. You may also have to disable earlier versions after download.</p> <ul style="list-style-type: none"> ➤ To do this in Internet Explorer: Select Tools > Internet Options > Advanced tab, locate the Java (Sun) item and select the check box for the correct Java version, click OK, close the browser, and reopen it. ➤ For details about how to verify the Java version in Mozilla Firefox, see the Mozilla Firefox documentation.
<p>Viewing the Documentation Library</p>	<ul style="list-style-type: none"> ➤ The Documentation Library is best viewed in Internet Explorer. ➤ The Documentation Library is best viewed from a browser with Java support. If your browser does not have Java support, download the Sun Java plug-in from the Sun Java Web site (http://java.com/en/index.jsp). Note that if Java support is not available, the Documentation Library automatically opens using the JavaScript implementation. The JavaScript implementation provides the same basic functionality as the Java implementation, however does not allow use of the Favorites tab within the navigation pane. ➤ If you experience a JavaScript error when opening the Documentation Library, disable the Show Exception Dialog Box in the Java Console and open the Help again.

Note for users having trouble opening Java applets:

If you have trouble opening Java applets in the user interface, try one or both of the following:

- ▶ If you use Internet Explorer, select **Tools > Internet Options > Connections > Local Area Network (LAN) Settings**. Clear the following options: **Automatically detect settings** and **Use automatic configuration script**.
 - ▶ Select **Control Panel > Java > General tab > Network Settings > select Direct connection** option (and not the default option to **Use browser settings**).
-

Note the following additional requirements for using your browser with HP Business Service Management:

- ▶ HP Business Service Management uses cookies. Ensure that your Web browser is set to accept all cookies.
- ▶ HP Business Service Management requires browser support for pop-up windows. HP Business Service Management will not perform properly if you use Web applications that are set to block pop-up windows in your browser.
- ▶ Users who view the HP Business Service Management site using Microsoft Internet Explorer (IE) must set their browser caching to automatically check for newer versions of stored pages.

To set IE browser caching options for HP Business Service Management:

- 1** In the browser page, select **Tools > Internet Options**. The Internet Options dialog box opens and displays the **General** tab.
- 2** Click **Settings**.
In IE 7.0, this button is located within the **Browsing History** section.
- 3** In the **Check for newer version of stored pages** list, select **Automatically**.

Server Environment Settings

<p>Time settings</p>	<p>All HP Business Service Management servers and database servers must have the same settings for the following:</p> <ul style="list-style-type: none"> ▶ Time zone ▶ Daylight Saving Time configuration ▶ Time
<p>Name resolution</p>	<p>The HP Business Service Management servers must be able to resolve the names of the machines with which they must communicate. These include all the HP Business Service Management servers, database servers, and data collectors.</p>
<p>TCP</p>	<p>Windows:</p> <p>It is highly recommended that you make the following change in your registry:</p> <p>For registry key MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, create a new key TcpTimedWaitDelay (DWORD) and set the (Decimal) value to 60.</p> <p>If this is not done, there may be a problem with exhausting the available TCP resources because the time delay default value may be too long.</p> <p>Tip: When working with the registry, it is recommended that you back it up before making any changes.</p>

HP Business Service Management on Virtual Platforms

If you are deploying HP Business Service Management on a virtual platform, the sizing guidelines for a regular installation are not applicable. The following general limitations and recommendations are applicable to an installation on a virtual machine:

- ▶ The following virtualization platforms are supported:
 - ▶ VMware ESX 3.x, 4.x, ESXi 5.x
 - ▶ Microsoft Hyper-V
- ▶ Performance of HP Business Service Management on a virtual machine can be expected to be slower than in a regular installation.
- ▶ 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 Service Management capacities and performance will vary according to the various server resources, such as CPU, memory, and network bandwidth, allocated to HP Business Service Management components.
- ▶ A Gigabit network card should be used.
- ▶ Refer to the SiteScope documentation for details on SiteScope requirements for installing on a virtual machine.

BSM-CMS Synchronization and Content Pack Information

For details about supported versions of HP Universal CMDB and Content Packs, see the BSM 9.1x Release Notes. Content Pack installation instructions are included with the Content Packs themselves.

Part III

BSM Server Installation

10

Installing BSM Servers on a Windows Platform

This chapter includes:

- ▶ Overview of BSM Server Installation on page 148
- ▶ Preparing Information Required for Installation on page 149
- ▶ Installation Prerequisites on page 151
- ▶ Working with the Web Server on page 152
- ▶ Installing HP Business Service Management Servers on page 154

Note: Before beginning any installation, review the information in the release notes for any last minute notes and limitations. Failure to follow procedures listed in the release notes could result in unexpected data loss or failure of the installation process. If you are installing a service pack, the installation instructions for that service pack are located in Chapter 3, "Service Packs and Patches".

Overview of BSM Server Installation

There are several stages to the HP Business Service Management server installation:

- 1** Installing HP Business Service Management as described in "Installing HP Business Service Management Servers" on page 154. The first wizard that opens copies the files and packages onto the machine. The post-installation wizard opens within the installation wizard and enables you to configure administration settings. These include registration and connection information, Web server and SMTP settings. It also includes bus installation and shortcut creation.
- 2** Configuring the licenses and deployment, and setting the management, RTSM, RTSM history, Business Process Insight, and Event (OMi) databases by specifying the database type and connection parameters for each database, as described in "Server Deployment and Setting Database Parameters" on page 167. You have the option of running this wizard immediately upon completing the post-installation wizard or running it after completing all installations. Alternatively, if you are installing BSM as part of an upgrade procedure, run the upgrade wizard instead.
- 3** Installing component setup files in the HP Business Service Management Downloads page, as described in "Installing Component Setup Files" on page 187.

The server Setup program gives you the option of installing both of the HP Business Service Management servers on one machine, or installing only one of the server types on the machine. For details on the different deployment configurations that are possible, see "Deployment Configurations" on page 123.

Preparing Information Required for Installation

Have the following information ready before installation:

- ▶ **Target directory names.** During installation HP Business Service Management installs the HP Software L-Core packages. If a lower version of these packages is already installed, the packages are automatically upgraded. Otherwise, the currently installed version is not overwritten. This change cannot be reversed.

During the installation, you must select directories for installing these shared packages. They include:

- ▶ HP Software Cross Platform Component
 - ▶ HP Software Cross Platform Component Java
 - ▶ HP Software Security Core
 - ▶ HP Software HTTP Communication
 - ▶ HP Software Certificate Management Client
 - ▶ HP Software Security Core Java
 - ▶ HP Software HTTP Communication Java
 - ▶ HP Software Performance Access Java
 - ▶ HP Software Graphing Component
 - ▶ HP Software Process Control
 - ▶ HP Software Certificate Management Server
- ▶ **License key.** You have the option to use an evaluation license (60 days) or import your permanent license. You can browse to a local or network location to locate your license .DAT file.

If at a later stage you need to update the license key (for example, if you acquire a license for one or more new HP Business Service Management components), you can do so within the HP Business Service Management site: Select **Admin > Platform > Setup and Maintenance > License Management** and click the **Add License from File** button. For information on updating the license key, see "Licenses" in *Platform Administration*.

- ▶ **Maintenance number.** This is the maintenance number you received with your HP Business Service Management package.

- **Administrator's e-mail address.**
- **Port number used by the Web server.** This is the port for access to the HP Business Service Management. The default is port 80.
- **Name of the Gateway Server machine.** This name must also include the domain name.
- **Name of the load balancer** (if applicable). This is the load balancer used to access the HP Business Service Management site.
- **SMTP mail server name.**
- **SMTP sender name.** This name appears on notifications sent from HP Business Service Management. This name can not contain spaces. If a name is entered with spaces the reports will not be delivered.

Note: After BSM is started you can configure an alternative SMTP server via **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

- **Information for setting database parameters.** If you plan to set the management, RTSM, RTSM history, Business Process Insight, and Event database connection parameters during Setup, see "Required Information for Setting Database Parameters" on page 171.

Installation Prerequisites

Note the following before installing HP Business Service Management servers:

- ▶ It is recommended that you install HP Business Service Management servers to a drive with at least 20 GB of free disk space. For more details on server system requirements, see "System Requirements" on page 131.
- ▶ If HP Business Service Management servers, including the database servers, are installed on multiple network segments, it is highly recommended that the number of hops and the latency between the servers be minimal. Network-induced latency may cause adverse affects to the HP Business Service Management application and can result in performance and stability issues. We recommend the network latency should be no more than 5 milliseconds, regardless of the number of hops. For more information, contact HP Software Support.
- ▶ Installing HP Business Service Management servers together with most other HP products on the same physical machine may result in port conflicts, performance issues, or other unexpected behavior. The coexistence of HP Business Service Management servers with HP SiteScope or HP Operations Manager agent has been tested and is supported.
- ▶ If you use the IIS Web server, it must be up and running prior to BSM installation.
- ▶ HP Business Service Management servers must not be installed on a drive that is mapped to a local or network resource.
- ▶ Due to certain Web browser limitations, the names of server machines running the Gateway Server must consist only of alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and periods (.). For example, if the names of the machines running the Gateway Server contain underscores, it may not be possible to log into the HP Business Service Management site when using Microsoft Internet Explorer 7.0 or later.
- ▶ During HP Business Service Management server installation, you can specify a different path for the HP Business Service Management directory (default is **C:\HPBSM**), but note that the full path to the directory must not contain spaces, cannot contain more than 15 characters, and should end with **HPBSM**.

- ▶ If you are installing BSM on a Windows Server 2008 SP2 machine, User Access Control (UAC) must be disabled during the installation process.
- ▶ During installation, the value of the Windows Registry key HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts is updated to include the following port ranges required by BSM: 1098-1099, 2506-2507, 8009-8009, 8080-8080, 4444-4444, 8083-8083, 8093-8093.

Note: These ports ranges are not removed from the registry key at BSM uninstall. You should remove the ports from the registry key manually after uninstalling BSM if they are no longer needed by any other application.

- ▶ If you plan to run HP Business Service Management servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the *HP Business Service Management Hardening Guide* PDF.

Working with the Web Server

HP Business Service Management installed on a Windows platform works with Apache HTTP Server or Microsoft Internet Information Server (IIS). You specify the web server type in the post-installation wizard. You can re-run the post-installation wizard to modify these settings.

Note: There must be only one running Web server on a server machine that uses the same port that HP Business Service Management uses. For example, if you select to use Apache HTTP Server during HP Business Service Management server installation, and you are installing on a machine on which IIS is already running, make sure to stop the IIS service and set its startup status to **Manual** before you begin the installation process.

Apache HTTP Server

HP Business Service Management uses an Apache HTTP Server version that has been adapted by HP for use with HP Business Service Management. It is installed during the server installation.

By default, the Apache HTTP Server is not enabled for SSL use. For details on configuring the Web server to use SSL, see <http://httpd.apache.org/docs/2.2/ssl/>. SSL should be enabled for all the directories in use by HP Business Service Management, as configured in the Apache configuration file (`httpd.conf` and `httpd-ssl.conf`).

Microsoft Internet Information Server (IIS)

If you are installing on a Microsoft Windows Server 2008 and using the IIS 7.X Web server, you must perform the following procedure:

- 1** In the **Control Panel**, select **Administrative Tools > Server Manager**.
- 2** Right-click **Roles** and select **Add server role** to launch the Add Roles wizard.
- 3** On the Select Role Services page, select **Web Server (IIS) role** to install.
If a popup opens with the question **Add features required for Web Server (IIS)?**, click the **Add required features** button.
- 4** Click **Next** twice.
- 5** In the Select Role Services panel, select the following roles:
 - **Application Development** section: **ISAPI Extensions** and **ISAPI Filters**.
 - **Management Tools** section: **IIS Management Scripts and Tools**
- 6** Click **Install**.

Installing HP Business Service Management Servers

You install HP Business Service Management 9.10 servers—the Gateway Server and Data Processing Server—from the HP Business Service Management DVD provided with the HP Business Service Management distribution package. Unless you install on a machine running IIS, HP Business Service Management installs Apache HTTP Server during the installation process.

You need administrative privileges for the machines on which you are installing HP Business Service Management servers.

Note: Make sure that there are no other installations or processes that may be using the Windows Installer. If there are, the BSM installation hangs and cannot continue running. You must stop the other installation, stop the BSM installation by clicking the **Cancel** button in the installation wizard, and re-run the BSM installation.

The first installation wizard copies the files and packages onto your machine. The post-installation wizard enables registration, and configuring connection, Web server, and SMTP settings.

To install HP Business Service Management servers:

- 1 Insert the HP Business Service Management DVD into the drive from which you want to install. A splash screen opens if Autorun is enabled on the machine.

If you are installing from a network drive:

- a Connect to the DVD.
- b From the **Start** menu, select **Run**.
- c Enter the location from which you are installing, followed by `HPBsm_9.10_setup.exe`. The setup file for HP Business Service Management servers is located in the **Windows_Setup** directory of the DVD. For example, enter `d:\Windows_Setup\HPBsm_9.10_setup.exe`

Note: If you are installing on a virtual machine, you must copy the .exe file, as well as the packages directory, locally. If you attempt to run the installation over the network onto a virtual machine, the installation fails.

- d** Click **OK**. Setup begins.
 - 2** Follow the on-screen instructions for server installation.
 - **Language.** If your installer has been localized to offer additional languages, select one from the options available.
-

Note: You may receive an anti-virus warning. You can proceed with the installation without taking any action and with the anti-virus software running on the machine.

- **Setup type:**
 - Select **Gateway** setup type to install the Gateway Server on the current machine.
 - Select **Data Processing** setup type to install the Data Processing Server on the current machine.
 - Select **Typical** setup type to install the Gateway Server and Data Processing Server on the same machine.

Note: If you are installing onto a machine running Windows 2008 R2 Server, you may get the following message: The installation folder for shared content is not valid. The problem may in fact be that you do not have the necessary administrator permissions to install BSM on the machine. Check with your system administrator.

- ▶ **Installation directories.** You must select the following directories for installation. Make sure that none of the paths contain black spaces.
 - ▶ Select the installation directory for HP shared content. Note that there is additional shared data in `%ALLUSERSPROFILE%\HP\BSM\`
 - ▶ Select the installation directory for product specific content. In Microsoft Windows environments, this path must be 15 characters or less, and must not contain blank spaces. If the name exceeds 15 characters or does not end with **HPBSM**, during the next step, the installation prompts you to give a different name.
-

Note: During installation you may get the following message:

- ▶ The necessary ports are in use. If the installation indicates that there are ports in use, the installation does not fail but it is recommended that you free the necessary ports. Otherwise, you will have to re-configure BSM to use a different set of ports.
-

This phase of the installation can take approximately half an hour or one hour in a virtual environment.

After the process completes, you see checkmarks next to each of the packages and applications successfully deployed. If there are errors, an Error window opens indicating which installation scripts may have failed.

3 The post-installation wizard opens. Do the following:

➤ **Register the product.**

➤ **Configure connection settings:**

➤ **Apache HTTP Server.** If port 80, the default port, is already in use by the existing Web server, HP Business Service Management notifies you to resolve the conflict. For details, see "Apache HTTP Server" on page 153. If you select Apache, you must also enter the email address of the BSM administrator.

➤ **Microsoft IIS.** If IIS is using a port other than port 80, enter the IIS port. If you select IIS, you must also select the IIS Web site address to be used by BSM.

➤ **Select the Web server type:**

If HP Business Service Management does not detect an installation of Microsoft IIS on the machine, you are offered the **Apache HTTP Server** option only. If you want to run HP Business Service Management with Microsoft IIS, click **Cancel** to exit HP Business Service Management Setup. Install IIS and rerun the HP Business Service Management installation.

➤ **Specify the SMTP mail server:**

➤ It is recommended that you specify the complete Internet address of your SMTP server. Use only alphanumeric characters.

➤ In the **Sender name** box, specify the name to appear in scheduled reports and on alert notices that HP Business Service Management sends. If HP Business Service Management was ever installed on the same machine, a default name, **HP_BSM_Notification_Manager**, may appear. You can accept this default or enter a different name.

➤ After BSM is started you can configure an alternative SMTP server via **Platform Administration > Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

If deploying on more than one server, install additional HP Business Service Management 9.10 servers using the above steps.

If you are installing a service pack, the installation instructions for that service pack are located in Chapter 3, "Service Packs and Patches".

Note: You can rerun the post-installation wizard to modify the settings. The post-installation wizard can be run from the following location: **<HPBSM root directory>\bin\postinstall.bat**. However, if you are running the post-installation wizard for the first time or it was closed before completion, use the following file instead **<HPBSM root directory>\bin\ovii-postinstall.bat**.

11

Installing BSM Servers on a Linux Platform

This chapter includes:

- ▶ Overview of BSM Server Installation on page 159
- ▶ Preparing Information Required for Installation on page 160
- ▶ Installation Prerequisites on page 161
- ▶ Working with the Web Server on page 162
- ▶ Installing HP Business Service Management Servers on page 163

Note: Before beginning any installation, review the information in the release notes for any last minute notes and limitations. Failure to follow procedures listed in the release notes could result in unexpected data loss or failure of the installation process. If you are installing a service pack, the installation instructions for that service pack are located in Chapter 3, "Service Packs and Patches".

Overview of BSM Server Installation

There are several stages to the HP Business Service Management 9.10 server installation:

- 1** Installing HP Business Service Management as described in "Installing HP Business Service Management Servers" on page 163.

- 2 Setting the database type and connection parameters for each database, as described in "Server Deployment and Setting Database Parameters" on page 167.
- 3 Installing component setup files in the HP Business Service Management Downloads page, as described in "Installing Component Setup Files" on page 187.

The server Setup program gives you the option of installing both of the HP Business Service Management servers on one machine, or installing only one of the servers on the machine. For details on the different deployment configurations that are possible, see "Deployment Configurations" on page 123.

Preparing Information Required for Installation

Have the following information ready before installation:

- **Maintenance number.** This is the number you received with your HP Business Service Management package.
- **Web server name.** This name must also include the domain name.

Note: When installing on Linux, the domain name must be entered manually.

- **Administrator's e-mail address.**
- **SMTP mail server name.**
- **SMTP sender name.** This name appears on notifications sent from HP Business Service Management.
- **Name of the Gateway Server machine.**
- **Name of the load balancer** (if any). This is the load balancer used to access the HP Business Service Management site.

- ▶ **Port number used by the Web server.** The default port is 80.
- ▶ **Information for setting database parameters.** If you plan to set the management, RTSM, RTSM history, Business Process Insight, and Event database connection parameters during Setup, see "Required Information for Setting Database Parameters" on page 171.

Installation Prerequisites

Note the following before installing HP Business Service Management servers:

- ▶ It is recommended that you install HP Business Service Management servers to a drive with at least 20 GB of free disk space. For more details on server system requirements, see "System Requirements" on page 131.
- ▶ If HP Business Service Management servers, including the database servers, are installed on multiple network segments, it is highly recommended that the number of hops and the latency between the servers be minimal. Network-induced latency may cause adverse affects to the HP Business Service Management application and can result in performance and stability issues. We recommend the network latency should be no more than 5 milliseconds, regardless of the number of hops. For more information, contact HP Software Support.
- ▶ Installing HP Business Service Management servers together with most other HP products on the same physical machine may result in port conflicts, performance issues, or other unexpected behavior. The coexistence of HP Business Service Management servers with HP SiteScope or HP Operations Manager agent has been tested and is supported.
- ▶ HP Business Service Management servers must not be installed on a drive that is mapped to a network resource.

- ▶ Due to certain Web browser limitations, the names of server machines running the Gateway Server must only consist of alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and periods (.). For example, if the names of the machines running the Gateway Server contain underscores, it may not be possible to log in to the HP Business Service Management site. To access the HP Business Service Management site in this case, use the machine's IP address instead of the machine name containing the underscore.
- ▶ If you plan to run HP Business Service Management servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the *HP Business Service Management Hardening Guide* PDF.
- ▶ You must be a root user to install HP Business Service Management on the server machine.
- ▶ The **DISPLAY** environment variable must be properly configured on the HP Business Service Management server machine. The machine from which you are installing must be running an X-Server.

Working with the Web Server

HP Business Service Management installed on a Linux platform works with Apache HTTP Server.

Note: There must only be one running Web server on an HP Business Service Management server machine.

Apache HTTP Server

HP Business Service Management uses a version of the Apache HTTP Server that has been adapted by HP for HP Business Service Management. It is installed during the server installation.

HP Business Service Management runs its Apache HTTP Server, by default, through port 80. If port 80 is already in use, there are two ways to resolve the port conflict:

- ▶ Before beginning HP Business Service Management installation, reconfigure the service using that port to use a different port.
- ▶ During HP Business Service Management installation, select a different port for the Apache HTTP Server.

By default, the Apache HTTP Server is not enabled for SSL use. For details on configuring the Web server to use SSL, see <http://httpd.apache.org/docs/2.2/ssl/>. SSL should be enabled for all the directories in use by HP Business Service Management, as configured in the Apache configuration file (**httpd.conf** and **httpd-ssl.conf**).

Installing HP Business Service Management Servers

You install HP Business Service Management 9.10 servers—the Gateway Server and Data Processing Server—from the BSM DVD provided with the HP Business Service Management distribution package.

To verify that the installation files are original HP-provided code and have not been manipulated by a third-party, you can use the HP Public Key and verification instructions provided on this HP web site: <https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>.

The only supported installation method is to mount the HP Business Service Management DVD on a machine with a DVD device. You can then either install directly from the DVD or copy the files to a directory on a Linux machine and install from there. Copying files from a Windows operating system to a Linux operating system may cause loss of files during installation.

After each stage of the installation process, you have the option to continue to the next stage or move back to the previous stage.

Note: It is recommended that you do not use an emulator application, for example Exceed, to install HP Business Service Management. Installing via an emulator may slow the pace of the installation and may adversely affect the appearance and functionality of the user interface.

To install HP Business Service Management servers:

- 1** Log in to the server as user **root**.
- 2** Insert the HP Business Service Management DVD into the drive from which you want to install. If you are installing from a network drive, mount the DVD.
- 3** Go to the installation root directory.
- 4** (Optional) You can verify that the installation files are original HP-provided code and have not been manipulated by a third-party by using the HP Public Key and verification instructions on the following website <https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>.
- 5** Run the following script:

```
/HPBsm_9.10_setup.bin
```

- 6** Follow the on-screen instructions for server installation.

Note: If HP Business Service Management detects a previous installation on the machine, a message is displayed warning that any customized configuration data will be overwritten.

- ▶ **Select the setup type:**
 - ▶ Select **Gateway** setup type to install the Gateway Server on the current machine.
 - ▶ Select **Data Processing** setup type to install the Data Processing Server on the current machine.
 - ▶ Select **Typical** setup type to install the Gateway Server and Data Processing Server on the same machine.
 - ▶ The directory to where the BSM files are copied is **/opt/HP/BSM**.
 - ▶ The installation directory for HP shared content is **/opt/OV**.
 - ▶ The data directory for HP shared content is **/var/opt/OV**.
-

Note: During installation you may get the following message:

- ▶ The necessary ports are in use. If the installation indicates that there are ports in use, the installation does not fail but it is recommended that you free the necessary ports.
-

This phase of the installation can take approximately half an hour or one hour in a virtual environment.

After the process completes, you see check marks next to each of the packages and applications successfully deployed. If there are errors, an **Errors** tab opens detailing what errors may have occurred.

- 7** The post-installation wizard opens. Do the following:
 - ▶ **Register the product. Enter Name, Company, and Maintenance number.**
 - ▶ **Configure connection settings:**
 - ▶ **Host.** Must be the fully qualified domain name (FQDN). The name of the server may appear by default but you must add the domain manually. If you use a load balancer, here you must enter the machine name for the load balancer.

- ▶ **Port.** If port 80, the default port, is already in use by the existing Web server, HP Business Service Management notifies you to resolve the conflict. For details, see "Apache HTTP Server" on page 163.
- ▶ **View the Web server type and enter the BSM administrator email address.** HP Business Service Management installs the **Apache HTTP Server**. This is the web server that must be used in Linux environments.
- ▶ **Specify the SMTP mail server:**
 - ▶ It is recommended that you specify the complete Internet address of your SMTP server. Use only alphanumeric characters.
 - ▶ In the **Sender name** box, specify the name to appear in scheduled reports and on alert notices that HP Business Service Management sends.

If deploying on more than one server, install additional HP Business Service Management 9.10 servers using the above steps.

If you are installing a service pack, the installation instructions for that service pack are located in Chapter 3, "Service Packs and Patches".

Note: You can rerun the post-installation wizard to modify the settings. The post-installation wizard can be run from the following location: **<HPBSM root directory>\bin\postinstall.sh**. However, if you are running the post-installation wizard for the first time or it was closed before completion, use the following file instead **<HPBSM root directory>\bin\ovii-postinstall.sh**.

12

Server Deployment and Setting Database Parameters

Note: If you work with Oracle Server, substitute the term **user schema** for the term **database** below.

This chapter includes:

- ▶ Setup and Database Configuration Utility Overview on page 168
- ▶ Setting Database Parameters on page 169
- ▶ Required Information for Setting Database Parameters on page 171
- ▶ Running the Setup and Database Configuration Utility on page 175

Setup and Database Configuration Utility Overview

You configure your server deployment and create and connect to the databases/user schemas necessary for running HP Business Service Management using the Setup and Database Configuration utility.

You can run the Setup and Database Configuration utility as part of HP Business Service Management server installation (described in "Installing BSM Servers on a Windows Platform" on page 147 or "Installing BSM Servers on a Linux Platform" on page 159) by selecting it in the last page of the post-installation wizard. Alternatively, you can run the Setup and Database Configuration utility independently after server installation. The steps involved are the same for both procedures, as described in "Running the Setup and Database Configuration Utility" on page 175.

When installing in a distributed environment, run the utility first on the Data Processing Server and then on the Gateway Server.

If, at a later time, you want to modify any of the database types or connection parameters, you can run the Setup and Database Configuration utility again. BSM must be disabled when running this utility (select **Start > Programs > HP Business Service Management > Administration > Disable HP Business Service Management**).

After modifying database type or connection parameters, restart all HP Business Service Management servers and data collectors.

Note: Modifying connection parameters for the management, RTSM, RTSM history, Business Process Insight, and Event databases after HP Business Service Management is up and running may cause serious data loss and integrity problems.

Before beginning this procedure, it is recommended that you review "Setting Database Parameters" on page 169 and "Required Information for Setting Database Parameters" on page 171.

For detailed information on preparing either MS SQL Server or Oracle Server in your system for use with HP Business Service Management, see the *HP Business Service Management Database Guide* PDF.

Setting Database Parameters

You must set connection parameters for the following databases:

- Management
- RTSM
- RTSM History
- Business Process Insight (BPI)
- Event

To configure the connections for these databases, you must:

- Select the type of database you plan to use— MS SQL Server or Oracle Server
- Select to create or re-use the database on MS SQL Server, or user schema on Oracle Server. See "Creating Databases" on page 170.
- Specify the connection parameters to the database or user schema. See "Connecting to Existing Databases" on page 170.

Note: If you need to change an active management database for HP Business Service Management, contact HP Software Support.

Creating Databases

You can either use the Setup and Database Configuration utility to create the databases for you on MS SQL Server or Oracle Server, or you can create these databases manually, directly in the relevant database server (for example, if your organization does not allow the use of administrator credentials during Setup). If you created the databases manually, you must still run the Setup and Database Configuration utility to connect to them.

For instructions on creating databases manually on MS SQL Server, see "Creating and Configuring Microsoft SQL Server Databases" in the *HP Business Service Management Database Guide* PDF. For instructions on creating user schemas manually on Oracle Server, see "Manually Creating the Oracle Server Database Schemas" in the *HP Business Service Management Database Guide* PDF.

Note: Each database/user schema created in HP Business Service Management (whether on the same database server or on different database servers) must have a unique name.

Connecting to Existing Databases

When running the Setup and Database Configuration utility, you select whether you want to create a new database/user schema or connect to an existing one.

You generally use the **Connect to an existing schema** option in the following scenarios:

- ▶ When connecting to a database/user schema you manually created directly on MS SQL Server/Oracle Server.
- ▶ When installing HP Business Service Management in a distributed environment and running the utility on servers subsequent to the first server. In this case, you should have run the wizard on the Data Processing Server first and then on the Gateway servers.

You connect to the databases/user schemas that you created during the installation of the first Data Processing Server. After you have connected to the management database, by specifying the same connection parameters that you set during the installation of the first server, the connection parameters for the other databases appear by default in the appropriate screens. Not all databases appear when running on the Gateway Server.

For information on implementing a distributed deployment of HP Business Service Management, see "Deployment Configurations" on page 123.

Required Information for Setting Database Parameters

Before setting database parameters, you should prepare the information described in the following sections.

Configuring Connection Parameters for MS SQL Server

You need the following information for both creating new databases and connecting to existing ones:

- **Host name.** The name of the machine on which MS SQL Server is installed. If you are connecting to a non-default MS SQL Server instance in dynamic mode, enter the following: <host_name>\<instance_name>

Caution: There is a twenty six (26) character limit for the **Host name** field while running the utility. If using a host name without a domain name is not appropriate in your environment, perform one of these workarounds:

- Use the IP instead of the host name in the **Host name** field.
 - Map the host name to the IP in the Windows Hosts file. Use the host name you mapped in the **Host name** field.
-

- ▶ **Port.** The MS SQL Server's TCP/IP port. HP Business Service Management automatically displays the default port, **1433**.
 - ▶ If you connect to a named instance in static mode, enter the port number.
 - ▶ If you connect to a named instance in dynamic mode, change the port number to **1434**. This port can dynamically listen to the correct database port.
- ▶ **Database name.** The name of the existing database that has been manually created, or the name that you will give your new database (for example, BSM_Management).
- ▶ **User name and Password.** (if you use MS SQL Server authentication) The user name and password of a user with administrative rights on MS SQL Server. The default MS SQL Server administrator user name is **sa**. Note that a password must be supplied.

You can create and connect to a database using Windows authentication instead of MS SQL Server authentication. To do so, you must ensure that the Windows user running the BSM service has the necessary permissions to access the MS SQL Server database. For information on assigning a Windows user to run the BSM service, see "Changing the BSM Service User" on page 455. For information on adding a Windows user to MS SQL Server, see "Using Windows Authentication to Access Microsoft SQL Server Databases" in the *HP Business Service Management Database Guide* PDF.

Note: In Linux environments, Windows authentication is not supported.

Configuring Connection Parameters for Oracle Server

Note: If your Oracle Server is on a Real Application Cluster (Oracle RAC), some of the parameters in this section should be assigned different values. For details, see the section about Support for Oracle Real Application Cluster in the *HP Business Service Management Database Guide* PDF.

Before setting database parameters, ensure that you have created at least one tablespace for each user schema for application data persistency purposes, and that you have set at least one temporary tablespace according to the requirements. For details on creating and sizing the tablespaces for HP Business Service Management user schemas, see "Oracle Server Configuration and Sizing Guidelines" in the *HP Business Service Management Database Guide* PDF.

You need the following information for both creating a new user schema and for connecting to an existing one:

- ▶ **Host name.** The name of the host machine on which Oracle Server is installed.

Caution: There is a twenty six (26) character limit for the **Host name** field while running the utility. If using a host name without a domain name is not appropriate in your environment, perform one of these workarounds:

- ▶ Use the IP instead of the host name in the **Host name** field.
- ▶ Map the host name to the IP in the Windows Hosts file. Use the host name you mapped in the **Host name** field.

-
- ▶ **Port.** The Oracle listener port. HP Business Service Management automatically displays the default port, **1521**.
 - ▶ **SID.** The Oracle instance name that uniquely identifies the Oracle database instance being used by HP Business Service Management.
 - ▶ **Schema name and password.** The name and password of the existing user schema, or the name that you will give the new user schema (for example, BSM_MANAGEMENT).

If you are creating a new user schema, you need the following additional information:

- ▶ **Admin user name and password.** (to connect as an administrator) The name and password of a user with administrative permissions on Oracle Server (for example, a System user).
- ▶ **Default tablespace.** The name of the dedicated default tablespace you created for the user schema.
- ▶ **Temporary tablespace.** The name of the temporary tablespace you assigned to the user schema. The default Oracle temporary tablespace is **temp**.

Note: To create a new user BSM user schema, you must have administrative permissions and CREATE USER, CONNECT, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, UNLIMITED TABLESPACE, CREATE VIEW, and CREATE PROCEDURE privileges on the Oracle Server.

Running the Setup and Database Configuration Utility

You can run the Setup and Database Configuration utility either as part of the HP Business Service Management Setup program or separately from the Setup program. If you run the Setup and Database Configuration utility separately from HP Business Service Management server Setup, note the following important points:

- ▶ If the command prompt window is open on the HP Business Service Management server machine, you must close it before continuing with the Setup and Database Configuration utility.
- ▶ If running this wizard after installation to modify existing configuration and not during initial installation, you must disable HP Business Service Management on the HP Business Service Management server machine before running the Setup and Database Configuration utility (select **Start > Programs > HP Business Service Management > Administration > Disable HP Business Service Management**).
- ▶ Use only English characters when entering database parameters.

To set database parameters and configure server deployment:

- 1 Launch the Setup and Database Configuration utility in one of the following ways:
 - ▶ After completing the server installation stage of HP Business Service Management setup, select to run the Setup and Database Configuration utility as a continuation of the HP Business Service Management Setup program.
 - ▶ **Windows:** On the HP Business Service Management server machine, select **Start > Programs > HP Business Service Management > Administration > Configure HP Business Service Management**. HP Business Service Management launches the Setup and Database Configuration utility.
 - ▶ **Linux:** On the HP Business Service Management server machine, open a terminal command line and launch `/opt/HP/BSM/bin/config-server-wizard.sh`.

2 Follow the on-screen instructions for setting the following databases:

- **Management**
 - **RTSM**
 - **RTSM history**
 - **Business Process Insight**
 - **Event**
-

Note: When running the utility on the Gateway Server, not all databases appear.

3 License. If you are running this utility for the first time, you can select to use the evaluation license or download your new licenses. If this is not the first time you are running this utility, you can select to skip this step or download additional licenses. The license file has a .DAT suffix and must be in a local or network location accessible to the server running the utility.

You can update your licenses after HP Business Service Management is installed in the Licenses Management page of Platform Administration. For details, see "Licenses" in *Platform Administration*.

4 Server Deployment. The recommended workflow is to enter your deployment information in the capacity calculator to determine the scope of your deployment and which applications and features you will be running. You can upload the saved capacity calculator Excel file into this page of the utility. The required fields are automatically populated with the data from the capacity calculator, based on your entries in the Excel sheet. For details, see "Using the Capacity Calculator" on page 83.

- **Users.** The number of logged in users determines whether your user load is **small**, **medium**, or **large**.
- **Model.** The number of configuration items in your model determines whether your model is **small**, **medium**, **large**, or **extra-large**.

- **Metric Data.** The number of monitored applications, transactions, locations, and hosts determines whether your metric data load is **small**, **medium**, or **large**.
- **<List of Applications>**. Select or clear the applications to activate or deactivate for this deployment. Clear those applications you are not using to free memory and processor speed for those applications that you are using.

Note: If you do not enable functionality while running this utility, it is not available to any users. For example, if you do not select Custom Rules (used in OMi and labelled Custom Event Handling in the capacity calculator), users are not able to customize event processing. For details on the application options, see the tooltips in the capacity calculator.

After the installation is complete and you want to change your deployment, you can adjust capacity levels and enable or disable applications and functionality in the Server Deployment page in Platform Administration.

You can also manually enter the information in this page, but it is highly recommended that you use the capacity calculator to determine the scope and capacity of your deployment.

- 5 Login Settings.** Enter passwords for the administrator user ("admin") to access BSM and the JMX console.

Optionally, set an **Access to RTSM password** to secure communication to the Run-time Service Model from Real User Monitor, Business Process Insight, and TransactionVision.

- 6 Firewall Configuration.** If you are running BSM behind a firewall, when running the utility on a Gateway Server, you have the option of configuring the firewall either automatically or manually.

 - ▶ When you select to configure automatically, **only port 383** (the event system default port) is configured on the Gateway Server. You must manually configure the same port when running the utility on the Data Processing Server because the certificate server is hosted there. You may need to open additional ports if a firewall is enabled on this server. For details, see "Port Usage" in *Platform Administration*.
 - ▶ When you select to configure manually, no port configuration is executed and you must manually configure on both the Gateway Server and the Data Processing Server.
- 7** To enable the database connections, you must click **Finish** at the end of the utility.
- 8** If you ran the Setup and Database Configuration utility as part of HP Business Service Management server installation, you must start HP Business Service Management on all BSM servers only after successfully setting the parameters for all the databases. For details, see "Starting and Stopping BSM" on page 447.

If you ran the Setup and Database Configuration utility to add a new Gateway Server or modify the previously defined database types or connection parameters, restart all BSM servers and data collectors after successfully completing the parameter modification process.

Note: If you used this utility to modify any databases on a running BSM deployment, MyBSM and Service Health will no longer contain any pages and components, and OMi perspectives are removed. To restore MyBSM and Service Health pages and components and OMi perspectives:

- Open the following directory: <**Gateway Server root directory**>\conf\uimashup\import. This contains two directories: \loaded, and \toload.
 - Copy the contents of the \loaded directory into the \toload directory. Restart BSM.
-

13

Upgrade Wizard

This chapter includes:

- ▶ Upgrade Wizard Overview on page 181
- ▶ Preparing Information for the Upgrade Wizard on page 182
- ▶ Tracking the Configuration Upgrade Progress on page 183

Upgrade Wizard Overview

The upgrade wizard is run after the post-installation wizard. It replaces the setup and database configuration utility which is run in a regular deployment. The upgrade wizard performs the following tasks:

- ▶ Migrates data from original databases
- ▶ Migrates BAC configurations
- ▶ Guides you through manual procedures necessary for the upgrade process

The upgrade wizard gives you the option of skipping some steps and running them later by restarting the wizard manually. This can be done as many times as is necessary. For example, if you do not have time to complete the data upgrade, you can skip it and complete the rest of the wizard. When you manually restart the wizard, your previous progress is saved. Make sure that you run the entire upgrade wizard from start to finish at least once.

The upgrade wizard runs the database schema verify program on your database schemas to verify that they have been configured properly. For details, see the *HP Business Service Management Database Guide* PDF.

The wizards are located in the HPBSM\bin directory as follows:

Starting Version of BAC/BSM	Upgrade File (OS refers to BSM 9.1x environment)
7.5	Windows: upgrade_wizard_run_from75.bat Linux: upgrade_wizard_run_from75.sh
8.x	Windows: upgrade_wizard_run.bat Linux: upgrade_wizard_run.sh
9.0	Windows: upgrade_wizard_run_from90.bat Linux: upgrade_wizard_run_from90.sh

Preparing Information for the Upgrade Wizard

To speed up the upgrade process, we recommend that you have the following information prepared before starting the upgrade wizard:

- ▶ **Data collectors / components.** Access to all data collectors and components integrated with the original BAC servers.
- ▶ **BAC / BSM Architecture.** Knowledge of BAC 8.x architecture including data collectors / components / servers.
- ▶ **BAC Servers.** Location, credentials, and access to files for all original BAC and new BSM servers.
- ▶ **Database Information.** Locations, credentials, CMDB / RTSM configuration (for example: internal RTSM, external CMDB, both).
 - ▶ **SQL server:** Credentials for a member of the sysadmin group or a user with select permissions for the syslogins system view.
 - ▶ **Oracle server:** Credentials for a user with the DBA or SELECT_CATALOG_ROLE role.

Tracking the Configuration Upgrade Progress

The configuration upgrade step of the upgrade wizard displays the status of the configuration upgraders as they are executed.

The following is an explanation for the meanings of the different statuses:

- ▶ **Failed.** When an upgrader fails, the upgrade process can not continue. Review the log tool and resolve any open issues. For further assistance, contact HP Software Support.
- ▶ **Partially Failed.** This status indicates that the items that failed are not critical to the upgrade process itself. Therefore, the user is asked to decide whether to ignore it and continue with the upgrade or to resolve the issue before continuing. If you decide to continue, you will not be able to rerun the failed upgrader and any data that was not upgraded will be lost. Do not continue unless you understand the implications of each partial failure. For details, see the log tool. For a list of what the partially failed status means for each upgrader, see "Partially Failed Status" on page 183.
- ▶ **Passed.** When an upgrader passes, this does not necessarily mean that there were no errors at all. It may mean that there were minor errors. Users are encouraged to use the log tool and carefully review any errors that occurred during the upgrade.

To view a summary of errors that occurred during the configuration upgrade, run the upgrade log tool located at **<HP Business Service Management server root directory>\tools\logTool\logTool.bat**. This generates a report in the same directory with the name **logTool.txt**.

Partially Failed Status

The following table lists the upgraders and what the partially failed status means for each one.

Upgrader	Meaning of Partially Failed Status
SampleEnrichmentUpgrade	<p>A partially failed status may happen when an unexpected error occurred in the upgrader while trying to upgrade one of the following entities:</p> <ul style="list-style-type: none"> ▶ Metrics configuration in profile database ▶ SiteScope monitor CIs in RTSM ▶ Related CIs in RTSM monitored by SiteScope monitors <p>Some possible reasons for failure are:</p> <ul style="list-style-type: none"> ▶ Database error ▶ CI resolution error ▶ RTSM error ▶ Problems in mapping of measurements to indicators due to missing or corrupted content. <p>When this happens the upgrader will mark the entity as partially failed in the corresponding upgrader log. (i.e sampleEnrich.upgrade.log)</p> <p>If there is at least one entity that was marked as partially failed the final upgrader status will be Partially Failed. In this case the user has the option to stop the upgrade or to instruct the wizard to continue.</p> <p>If the user decides to continue with the upgrade it means that any configuration or data associated with this entity will not be upgraded to the new system.</p> <p>For example, if a monitor was marked as partially failed and the user decided to continue it means that in the upgraded system this monitor and its related data will not exist - HIs/KPIs will not be assigned to CIs which have failed monitors associated with them.</p>
OprContentUpgrader	<p>At least one content pack failed and at least one succeeded.</p> <p>This could happen if you have customized content. We recommend that you continue with the upgrade.</p> <p>In some cases the SiS Upgrader will fail if a required out-of-the-Box-Contentpack conflicted with a custom content. In this case you will have to resolve the conflict manually and upload the OOTB-Contentpacks manually again.</p>

Upgrader	Meaning of Partially Failed Status
RuleTooltipUpgrader	<p>This happens when you have a Service Health rule that does not have a corresponding tooltip.</p> <p>If you decide to continue it means that the rule will not have a tooltip. A new tooltip can be assigned to the rule in repository 9.1x user interface by editing the rule.</p>

Upgrader	Meaning of Partially Failed Status
CustomMapViewNameUpgrader	<p>The upgrade updates two tables, one with data regarding the image set to the view, and one with data of CIs set to the image. If only one table upgrade succeeded and the second failed a partially failed status is returned.</p> <p>If you decide to continue it means that the view will not have an image or the view will have an image but with no CIs on the image. A customer can set new image/CIs in the Custom Image user interface in Admin > Service Health > Custom Image.</p>
BPM Model and RUM Model Upgraders	<p>A partially failed status in the EUM Admin upgraders may happen when an unexpected error occurred in the upgrader while trying to upgrade one of the following entities:</p> <ul style="list-style-type: none"> ➤ BPM profile ➤ RUM Application ➤ RUM End User Group ➤ RUM Page ➤ RUM Transaction ➤ RUM event <p>When this happens the upgrader will mark the entity as partially failed in the corresponding upgrader log.</p> <p>In each EUM Admin upgrader, if there is at least one entity that was marked as partially failed the final upgrader status will be Partially Failed. In this case, you have the option to stop the upgrade or to instruct the wizard to continue.</p> <p>If you decide to continue with the upgrade, it means that any configuration or data associated with this entity will not be upgraded to the new system.</p> <p>For example, if a profile was marked as partially failed and the user decided to continue it means that in the upgraded system this profile and its related data will not exist. Additionally, any other entity that relates to this profile (E.g. Alerts, SLM, report filters, linked CI, etc) will be detached from this profile or removed completely if it cannot exist by its own.</p>

14

Installing Component Setup Files

This chapter includes:

- Overview of Installing Component Setup Files on page 187
- Installing Component Setup Files on page 188

Overview of Installing Component Setup Files

The component setup files are used to install the components used by HP Business Service Management. The component setup files are not installed as part of the basic HP Business Service Management installation. They are located separately in the Web delivery package download area and in the **Data Collectors and Components\components** directory of the HP Business Service Management DVDs and must be installed separately to the HP Business Service Management Downloads page. The component setup files can then be downloaded from HP Business Service Management and used when required. For details on working with the HP Business Service Management Downloads page, see "Downloads Overview" in *Platform Administration*.

You must run all DVDs provided for installation to enable downloading all the HP Business Service Management data collectors and components.

Note: You can install a component by using the component's setup file directly from the network or DVD. For details on installing a component, refer to the individual documentation for the component you want to install. The relevant documentation is available from the Downloads page in HP Business Service Management after the component's setup files are copied to the Downloads page.

Installing Component Setup Files

The procedure for installing component setup files to the Downloads page differs, depending on whether you are installing a Web delivery version or DVD delivery version of HP Business Service Management 9.12.

Installing Component Setup Files Using a Web Delivery Version

Copy the component setup files that you want available in the Downloads page from the appropriate directory in the release download area to the **<BSM root directory>\AppServer\webapps\site.war\admin\install** directory on the HP Business Service Management Gateway Server. If required, create the **admin\install** directory structure.

Installing Component Setup Files Using a DVD Delivery Version

There is a setup utility in the **Data Collectors and Components** directory on the DVD that copies the component setup files from the DVD to the **<BSM root directory>\AppServer\webapps\site.war\admin\install** directory on the HP Business Service Management Gateway Server.

During the setup process, you can choose which data collectors to copy by selecting the relevant checkboxes.

Note: You can install all or some of the component setup files on multiple Gateway Servers, with the files installed on a specific server being available on that server's Downloads page.

To install component setup files to the HP Business Service Management Downloads page:

- 1** Insert the HP Business Service Management DVD into the drive of the HP Business Service Management Gateway Server on which you want to copy the component setup files.
- 2** On the Setup window, click the **Data Collectors and Components Downloads Page Setup** link to open the Data Collector Wizard.
If the Setup window does not appear on your screen, navigate to the **Data Collectors and Components** directory on the DVD and run **copydc.bat**.
- 3** Follow the on-screen instructions to complete the wizard.

15

Uninstalling BSM Servers

This chapter includes:

- Complete Uninstall on page 191

Complete Uninstall

Use the procedure below to completely uninstall HP Business Service Management.

Note: When uninstalling BSM servers completely, the uninstall program removes all BSM servers installed on the server machine.

Uninstalling BSM servers in a Windows environment

To completely uninstall HP Business Service Management servers in a Windows environment:

- 1** On the machine from which you are uninstalling HP Business Service Management, select **Start > Settings > Control Panel > Add/Remove Programs**. Select **HP Business Service Management**.
- 2** Click **Remove**, wait for the HP BSM uninstall script to remove any present updates, and follow the on-screen instructions when prompted.
- 3** If the **Show Updates** check box is selected, all the updates installed over HP BSM are displayed. When BSM is removed, all updates are removed, as well.

- 4 When a Minor-Minor HP BSM Release (9.0X) is removed, any HP BSM Public Patches installed on top of the release are removed, as well.
- 5 Restart the server machine.
- 6 If you are running HP Business Service Management with Microsoft IIS, open the IIS Internet Services Manager and check the following:
 - Under the **Default Web Site**, check that the following virtual directories have been removed and remove them if they still appear:
 - ext
 - HPBAC
 - Jakarta
 - mam_images
 - MercuryAM
 - opr-console
 - Topaz
 - TopazDC
 - Right-click the server machine name in the tree, and select **Properties**. In the Properties dialog box, with **WWW Service** displayed in the Master Properties list, click **Edit**. Select the **ISAPI Filters** tab. If the **jakartaFilter** filter still appears, remove it.

Note: If you plan to uninstall HP Business Service Management and then reinstall it to a different directory on the server machine, there is no need to remove the **jakartaFilter** filter. However, you will need to update the path for the filter. For details, see "Troubleshooting" on page 457.

- 7 Access the Windows Registry Editor by selecting **Start > Run**. Enter **Regedit**

During installation, the value of the Windows Registry key **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservePorts** was updated to include the following port ranges required by BSM: 1098-1099, 8009-8009, 8080-8080, 4444-4444, 8083-8083, 8093-8093.

These ports ranges are not removed from the registry key during uninstall. You should remove the ports from the registry key manually after uninstalling BSM if they are no longer needed by any other application.

Tip: When working with the registry, it is recommended that you back it up before making any changes.

Uninstalling BSM servers in a Linux environment

- 1 Log in to the server as user **root**.
- 2 To access the uninstall program, type:

```
cd /opt/HP/BSM/installation/bin
```

- 3 Run the following script to uninstall in UI mode:

```
./uninstall.sh
```

- 4 The HP Business Service Management uninstall program begins. Follow the on-screen instructions. When the uninstall program is complete, a success message is displayed.
- 5 Click **Finish**.

- 6 Check the **HPBsm_9.10_HPOvInstaller.txt** log file located in the **/tmp** directory for errors. Previous installation files can be found in the **/tmp/HPOvInstaller/HPBsm_9.10** directory.

Note: If you encounter problems during the uninstall procedure, contact HP Software Support.

Part IV

HP Business Service Management Upgrade Information

16

Upgrading BSM with Operations Manager *i* (OMi)

This chapter includes:

- OMi Upgrade Information on page 198
- OMi 8.10 to 9.1x Pre-Upgrade Procedure on page 200
- OMi 8.10 to 9.1x Mid-Upgrade Procedure on page 210
- OMi 8.10 to 9.1x Post-Upgrade Procedure on page 225
- OMi 9.0x to 9.1x Pre-Upgrade Procedure on page 234
- OMi 9.0x to 9.1x Post-Upgrade Procedure on page 239

OMi Upgrade Information

The following items have changed in OMi (Operations Manager *i*) from BAC 8.x to BSM 9.1x.

Topic	OMi 8.10	BSM 9.1x
<p>Connection to HPOM management server.</p>	<p>Connection information is configured in the Infrastructure Settings manager > Operations Management application > HPOM Connection Settings pane.</p>	<p>Connected servers are configured in the Connected Servers manager: Operations Management Administration > Tune Operations Management > Connected Servers.</p> <p>The Connected Servers manager enables you to specify multiple HP Operations Manager servers, external event processing servers, servers connected using BSM Integration Adapter, and other Operations Management (BSM) servers as event forwarding targets.</p> <p>OMi 8.10 HPOM management server connection settings are migrated.</p>
<p>Content pack manager</p>	<p>Content packs must be manually uploaded.</p> <p>Content packs must contain all content that is referenced in a content pack.</p>	<p>Content packs are automatically uploaded during installation, during the migration, and subsequently at every BSM startup.</p> <p>Content packs can contain references to content in other content packs.</p>

Topic	OMi 8.10	BSM 9.1x
Health indicators	Health indicators are part of Operations Management and are only used in Operations Management.	Health indicators have become part of the BSM platform and are used within different BSM applications, including Operations Management. The health indicator user interface has been redesigned.
KPI names and types	KPI names Operations Availability and Operations Performance.	<p>The KPI Operations Availability has been replaced by the KPIs Application Availability, Software Availability, and System Availability.</p> <p>The KPI Operations Performance has been replaced by the KPIs Application Performance, Software Performance, and System Performance.</p> <p>By default the OMi 8.10 KPI assignments to Operations Availability and Operations Performance are replaced by assignments to System Availability and System Performance respectively. For details, see "Alternative KPIs" on page 223.</p>

OMi 8.10 to 9.1x Pre-Upgrade Procedure

Perform the following steps before beginning the BAC 8.x to BSM 9.1x upgrade.

1 Verify the Supported HPOM Versions

Make sure that the version of HPOM that you plan to use with BSM 9.1x is supported. For more information about supported versions, see the BSM 9.1x *Release Notes*.

2 Upgrade HP Operations Smart Plug-ins on the HPOM System - Recommended

HP strongly recommends that you upgrade the HP Operations Smart Plug-ins (SPIs) before starting the OMi upgrade. For more information, see "Upgrading HP Operations Smart Plug-ins (SPIs)" on page 202.

3 Make a Note of Each Modification to the OMi 8.10 Content Packs

Make a note of each modification to the OMi 8.10 content packs in the following situations:

- ▶ You are retaining the SPIs that you have been using with OMi 8.10 but want to upgrade the SPIs to SPI DVD release 2010 at a later point in time.
- ▶ You have already upgraded the SPIs to SPI DVD release 2010.

Alternatively, if you have applied many modifications, consider creating a new content pack that contains all of your OMi 8.10 modifications. For more information about creating content packs, see the *Platform Administration* PDF.

4 Back Up the OMi Configuration Files - Recommended

The configuration files include the content packs, topology synchronization data, and custom icons. For details, see "Backing Up OMi Configuration Files" on page 203.

5 Delete CIs with Short Hostnames

Microsoft Active Directory and Microsoft SQL Server content packs only: Delete all CIs whose name is not the fully qualified domain name. For details, see "Deleting CIs with Short Hostnames" on page 205.

6 Update Empty Host Name Attributes of Host CIs

HP Operations Smart Plug-in for Virtual Infrastructure only: Because the Host Name attribute of host CIs created by the SPI for Virtual Infrastructure is empty, the CIs are not migrated successfully. To correct the problem, create an enrichment rule that copies the value of the Name attribute to Host Name. For details, see "Updating Empty Host Name Attributes of Host CIs" on page 206.

7 Export the OMi Configuration Data - Optional

Export the OMi 8.10 configuration data in the following situations:

- ▶ If you are retaining the SPIs that you have been using with OMi 8.10, use the **ContentManager** command line interface tool to export a snapshot that contains the complete OMi configuration data to a BSM package file.
- ▶ If you upgraded the SPIs to SPI DVD release 2010 and created a custom content pack for your OMi 8.10 content modifications, export that content pack only.

For details, see "Exporting the OMi Configuration Data" on page 207.

8 (Direct Only) Uninstall OMi on all BSM Servers

Uninstall OMi 8.10. For details, see "Uninstalling the OMi 8.10 Installation" on page 208.

9 Continue Upgrading to BSM 9.1x

After having completed the pre-upgrade steps, continue upgrading to BSM 9.1x. For details, see "Upgrade to 9.1x" on page 26.

Upgrading HP Operations Smart Plug-ins (SPIs)

HP strongly recommends that you upgrade the HP Operations Smart Plug-ins (SPIs) to SPI DVD release 2010 or later to take full advantage of the improvements that come with the latest versions. For more information about upgrading SPIs, see the documentation provided with the SPIs. For more information about supported versions, see the support matrix at:

<http://support.openview.hp.com/selfsolve/document/KM323488>

This site requires that you register for an HP Passport and sign in.

For more information about the limitations that arise if you do not upgrade the SPIs, see "Limitations" on page 203.

Limitations

The upgrade does not migrate the following indicators (and their customizations) to version 9.1x. The 9.1x content packs replace these indicators with new indicators of the same name. The new indicators are not compatible and do not work with SPI versions earlier than SPI DVD release 2010:

Indicator	9.1x Content Pack
Ping Availability	Infrastructure Content Pack and some dependent Content Packs
Server Load	Lync Server Content Pack
EJB Timeout Rate	JEE Application Server Content Pack
JMS Server Utilization	JEE Application Server Content Pack
Transaction Timeout Errors	JEE Application Server Content Pack
Transaction Capacity Utilization	JEE Application Server Content Pack
Transaction System Errors	JEE Application Server Content Pack

Backing Up OMi Configuration Files

This task describes how to back up the OMi configuration files. The configuration files include the content packs, topology synchronization data, and custom icons.

Note: Events, Event Browser filters, the configuration for Event Assignments, and Graph Templates, and Graph Assignments are not migrated as part of the product migration.

If you want to use the same filters in the migrated installation, you must make a note of the original filters and recreate them within the Operator and Administrator areas for each user associated with the filter.

To back up the content packs and the topology synchronization rules, complete the following steps:

- 1 From the BAC 8.x Data Processing Server host system, make a copy of all the files in the following directory and subdirectories:

`%TOPAZ_HOME%\conf\opr\`

- 2 Save these files to a safe location, for example:

Windows: `%TEMP%\migration`

Linux: `/tmp/migration`

Staging Only. Copy the files to a safe location on the BSM 9.1x Data Processing Server host system.

Note: The files are copied for backup purposes only. They are not automatically migrated to the new installation. If you have modified any out-of-the-box content packs, you must manually migrate your changes after the upgrade. Also, if you have modified any out-of-the-box topology synchronization packages, you must manually recreate your changes after the upgrade.

To back up the custom icons, complete the following steps:

- 1 From an BAC 8.x Gateway Server host system, make a copy of all the files in the following directory and subdirectories:

`%TOPAZ_HOME%\opr\resources\images\hivalues\`

- 2 Save these files to a safe location, for example:

Windows: `%TEMP%\migration`

Linux: `/tmp/migration`

Staging Only. Copy the files to a safe location on the BSM 9.1x Gateway Server host system.

To be able to recreate the configuration for Event Assignments, complete the following steps:

- 1 Make a note of each Event Assignment rule and each associated filter.
- 2 Recreate these filters and Event Assignment rules in the migrated installation.

To be able to recreate the filters used in the Event Browser, and Closed Event Browser, complete the following steps:

- 1 Make a note of each user and the filter configurations associated with that user.
- 2 Recreate these filters in the migrated installation.

To be able to recreate Graph Templates and Graph Assignments, complete the following step:

- 1 Make a note of each Graph Template and Graph Assignment that has been created. (After migrating from BAC 8.x to 9.1x, when you install content packs 9.1x on BSM 9.1x, new graph templates for all content packs are available in the Content Manager.)
- 2 Recreate your Graph Templates and Graph Assignments in the migrated installation.

Deleting CIs with Short Hostnames

Microsoft Active Directory and Microsoft SQL Server Content Packs only: Delete all CIs whose name is not the fully qualified domain name.

To delete CIs with short hostnames:

- 1 Identify and delete all Active Directory Forest CIs whose **Name** field is not filled with the fully qualified domain name (FQDN).

For example, if two CIs with the names forest1 (FQDN: forest1.com) and forest2.com (FQDN: forest2.com) exist, delete the forest1 CI.

- 2 Delete all Active Directory Domain CIs (recursive) and Active Directory Sites that belong to the deleted Active Directory Forest CI.

In this example, all domains and site CIs for forest1 must be deleted.

- 3 Identify and delete all SQL Server CIs whose name field is not filled with the FQDN.

Updating Empty Host Name Attributes of Host CIs

HP Operations Smart Plug-in for Virtual Infrastructure only: Because the Host Name attribute of host CIs created by the SPI for Virtual Infrastructure is empty, the CIs are not migrated successfully. To correct the problem, create an enrichment rule that copies the value of the Name attribute to Host Name.

To update empty Host Name attributes, complete the following steps:

- 1** In the BAC 8.x Enrichment Manager, create a new, active enrichment rule based on a new TQL:

Select **Admin > Universal CMDB > Modeling > Enrichment Manager**.

To create a new enrichment rule, right-click anywhere in the Enrichment Rules pane and click **New**.

In the enrichment rule wizard, specify a name and description for the rule. Select **Rule is active**. As base TQL type, select **Base the Enrichment on a new TQL**. Close the wizard by clicking **Finish**.

- 2** Drag the CI type **Host** to the editing pane.
- 3** Right-click **Host** in the editing pane and select **Node Properties**.
- 4** Add a new attribute condition by clicking the button with the green plus sign. If necessary, select the new condition, then select **Host Name - (string)** from the **Attribute name:** drop-down list.

Select **Is null** from the **Operator:** drop-down list. (The Value field remains empty.) Click **OK**.

- 5** *Optional:* Calculate the TQL query results.
- 6** In the upper-left corner of the editing pane, click **TQL Mode** and select **Enrichment Mode**.
- 7** Right-click **Host** in the editing pane and select **Update Node**.

- 8** In the **Node Definition** dialog, select the **Host Name** attribute in the **Name** column, then click the **By Attribute** button. The string **Host** appears in the drop-down list next to the **By Attribute** button.

To specify the attribute to be taken, select the **Name** attribute in the drop-down list to the right of the **Host** attribute. Click **OK**.

9 Navigate to Scheduler, select:

Admin > Universal CMDB > Settings > Scheduler

Add a new job by clicking the button with the green plus sign. The **Job Definition** dialog opens where you specify a name and a definition.

To add an action to the job, click the button with the green plus sign under **Actions**. The **Action Definition** dialog opens. Select **Run an Enrichment rule** and click **Next**. Select the enrichment rule that you created in Step 1 and click **Finish**.

- 10 In the **Job Definition** dialog, under **Scheduler**, select **Once** and specify the current time. Click **OK** to save the job definition and close the dialog.
- 11 Wait for the enrichment to finish. Check that the enrichment query created in Step 1 no longer matches any hosts.

For more information about enrichment rules and scheduling, see the *Model Management* section in the BAC online help.

Exporting the OMi Configuration Data

This task describes how to export the OMi configuration data using the Content Manager command line interface.

To export the OMi configuration data, complete the following steps:

- 1 From a BAC 8.x Gateway Server, in a command prompt window, go to the following directory:

```
%TOPAZ_HOME%\opr\bin\
```

- 2 If you are retaining the HPOM Plug-ins (SPIs) that you have been using with your OMi 8.10 installation, export *all* 8.10 content packs. Enter the following command:

```
ContentManager -snapshot -username <administrator account> -password <administrator password> -o <snapshot file name>.xml
```

Where the administrator account must have read and write access to the Content Manager.

- 3 If you collected your modifications to OMi 8.10 content in a custom content pack, export that custom content pack. Enter the following command:

```
ContentManager -username <administrator account> -password  
<administrator password> -e <custom content pack name> -o <custom  
file name>.xml
```

Where the administrator account must have read and write access to the Content Manager.

- 4 Save the exported data output file to a temporary location, for example:

Windows: %TEMP%\migration

Linux: /tmp/migration

If you are following the Staging Mode and the BSM 9.1x Gateway Server host system is already installed and available, copy the exported data output file to a temporary location on the BSM 9.1x Gateway Server host system.

The exported data must be converted to the syntax and model required by the BSM 9.1x version. For details, see "Converting OMi 8.10 Content Packs to 9.1x Model and Syntax" on page 220.

Uninstalling the OMi 8.10 Installation

For more details about uninstalling OMi, see the *HP Operations Manager i Installation and Deployment Guide version 8.10*.

Note: Complete this task only if you are upgrading from BAC 8.x using the direct mode.

To delete the installed OMi components from all the BSM server systems, follow these steps:

- 1 On all Data Processing and Gateway Servers, stop the BSM platform, if it is running:
Start > Programs (or All Programs) > HP Business Availability Center > Administration > Disable Business Availability Center
- 2 In a command prompt window, disable OMi by executing the following command on all the BSM platform systems:

`%TOPAZ_HOME%\bin\opr-configuration.bat -disable`

- 3** Click **Start > Control Panel > Add or Remove Programs**.
- 4** Select **HP Operations Manager i** and click **Change/Remove** to start the HP Software Installer.
- 5** Select **Uninstall** and click **Next**.
- 6** In the Pre-Uninstall Summary, click **Uninstall**.
- 7** Click **OK** when the note about uninstalling the BSM platform appears.

The Installer selects and uninstalls the OMi software components. Each software component and its uninstallation progress are displayed on your screen during the uninstallation operation.

After the uninstallation process is complete, the Uninstall Complete window opens showing you a summary of the uninstallation process.

- 8** In the Uninstall Complete window, click **Done** to close the uninstallation program.

Note: From the View log file link, you can access the uninstallation log file that opens in a web browser. For details on the removed packages, click the **Details** tab.

OMi 8.10 to 9.1x Mid-Upgrade Procedure

Perform this procedure between running the post-installation wizard and the upgrade wizard when upgrading BAC 8.x to BSM 9.1x.

1 Establish Trust Relationship

Establish and verify a trust relationship with HPOM to enable connection and communication between the BSM and HPOM systems. For details, see "Establishing and Verifying a Trust Relationship" on page 212.

2 (Staging Only) Configure HPOM to Forward Events to BSM 9.1x

By default, when using a staging environment to upgrade BSM, only the original OMi 8.10 servers receive events from HPOM. To allow event forwarding to the new staging servers, update the HPOM message forwarding policies as appropriate. As soon as the staging servers are online, both the original OMi 8.10 and the new BSM 9.1x environments receive events from HPOM. Until then only the original servers receive the events.

For details, see "Configuring the HPOM for Windows Forwarding Policy" on page 215 or "Configuring the HPOM for UNIX and HPOM for Linux Forwarding Policy" on page 217.

3 Configure HPOM Event Buffering

During the migration, HPOM continues to attempt sending events to the OMi environment. If the OMi servers cannot be reached, HPOM starts to buffer the events until the servers are online again. Depending on the length of the outage and the number of events, adjust the maximum length of the delivery timeout and the maximum size of the buffer file.

For details, see "Configuring HPOM Event Buffering" on page 219.

4 Convert OMi 8.10 Content Packs to 9.1x Model and Syntax - Optional

Convert the content packs that you exported from your OMi 8.10 installation to the syntax and model required by BSM 9.1x. You only need to complete this step if you exported content as described in "Exporting the OMi Configuration Data" on page 207.

For details, see "Converting OMi 8.10 Content Packs to 9.1x Model and Syntax" on page 220.

5 Restore Custom Icons from OMi 8.10 - Optional

If you have saved copies of OMi 8.10 icons for health indicators, copy the saved OMi 8.10 files to the BSM 9.1x installation. For details, see "Restoring Custom Icons from OMi 8.10" on page 224.

6 Import Security Certificates to JRE Truststore

Secure environments only: To re-enable the trust relationship between the Java Runtime Environment (JRE) and the LDAP server, you must import the LDAP trusted certificate to the JRE truststore. For details, see the *HP Business Service Management Hardening Guide* PDF.

7 Run the BSM 9.1x Upgrade Wizard

Migrated OMi 8.10 content and 9.1x content is uploaded using the create mode. The overwrite mode is not used and the OMi 8.10 content is retained to support the SPI DVD release 2008.1 SPIs.

The upgrade wizard first uploads the content packs for the locale set for the system, followed by English-language content packs that were not uploaded during the first upload phase. For example, if the locale is set to Japanese, Japanese-language content packs will be uploaded first, followed by English-language content packs. This can result in mixed-language content.

Note: If the OprUpgrader component partially fails during the configuration upgrade, check the opr-admin.log file to make sure that the HPOprInf, HPOprJEE, HPOprMss, and HPOprOra content packs are loaded successfully:

Windows: %TOPAZ_HOME%\log\EJBContainer\opr-admin.log

Linux: /opt/HP/BSM/log/EJBContainer/opr-admin.log

If these content packs are loaded successfully, you can click Pass Upgrade and continue with the upgrade. If one of these content packs is not upgraded successfully, you must first correct the problem. Otherwise the subsequent SiSConfigurationEnrichment upgrade fails.

Continue with the main upgrade procedure, step 11 on page 25.

Establishing and Verifying a Trust Relationship

For connection and communication between the BSM and HPOM systems, you must establish a trust relationship between the systems.

Note: The following steps use the ovcert, ovconfchg, and bbcutil command line tools. The tools are located in:

Windows: %OvInstallDir%\bin

Linux: /opt/OV/bin

To establish a trust relationship between BSM and HPOM systems, do the following:

- 1** Ensure that certificates have been set up on the Gateway and Processing Servers. For details, see "Post-Installation Tasks" in the the *HP Business Service Management Deployment Guide* PDF.
- 2** On all BSM Processing Servers, execute the following command:
ovcert -exporttrusted -file BSM_DPS<#>.cer
- 3** On the HPOM management server, execute the following command:
ovcert -exporttrusted -file other.cer
- 4** Copy other.cer from the HPOM management server to all BSM Processing Servers.
- 5** Copy BSM_DPS<#>.cer from the BSM Processing Server to the HPOM management server and all other BSM Processing Servers.
- 6** On all BSM Processing Servers, execute the following commands:
ovcert -importtrusted -file other.cer
and:
ovcert -importtrusted -file other.cer -ovrg server
- 7** On the HPOM management server and on all BSM Processing Servers, execute the following commands:
ovcert -importtrusted -file BSM_DPS<#>.cer
and:
ovcert -importtrusted -file BSM_DPS<#>.cer -ovrg server
- 8** If you have a multi-machine deployment, execute the following command on all Gateway Servers:
setupSecureCommunication <BSM processing server>

If you are not sure whether the agent was installed first, use the command **ovconfchg -edit** to check the **hp.XplConfig.ovconfchg** file. If **sec.cm.client.certificate_server** is set to the HPOM management server, then the agent was not installed first.

- 9 If the agent was installed on the system before the BSM server was installed, execute the following command on all Gateway servers:

ovcert -updatetrusted

- 10 Configure the load balancers and reverse proxies according to the instructions in the the *HP Business Service Management Deployment Guide* PDF depending on your certificate authority and setup. Make sure that the new Data Processing Server certificates are trusted if no central certificate authority is used.

After establishing a trust relationship between the BSM and HPOM systems, check the connection between the two systems.

To check the connection between BSM and HPOM:

- 1 From the HPOM management server, verify that communication to the BSM installation is possible (the return value should be eServiceOk) by executing the following command on the HPOM server:

bbcutil -ping https://<BSM load_balancer, proxy server, or single_gateway_server>

Example of the command result:

```
https://<BSM servername>: status=eServiceOK  
coreID=7c66bf42-d06b-752e-0e93-e82d1644cef8 bbcV=06.10.105  
appN=ovbbccb appV=06.10.105 conn=1 time=1094 ms
```

- 2 From all BSM Processing Server hosts, verify that communication with the HPOM management server host is possible (the return value should be eServiceOk) by executing the following command:

bbcutil -ping https://<HPOM_management_server_hostname>

Example of the command result:

```
https://<HPOM servername>: status=eServiceOK  
coreID=0c43c032-5c94-7535-064a-f7654a86f2d3 bbcV=06.10.070  
appN=ovbbccb appV=06.10.070 conn=7 time=140 ms
```

- 3 On the HPOM management server, add any new BSM Gateway Servers, load balancers, or reverse proxies to the list of target servers for discovery data.

Restart the discovery server processes on the HPOM management server:

- HPOM for Windows:

```
net stop "OvAutoDiscovery Server"
```

```
net start "OvAutoDiscovery Server"
```

- HPOM for UNIX or Linux:

```
ovc -stop opcsvcdisc
```

```
ovc -start opcsvcdisc
```

Configuring the HPOM for Windows Forwarding Policy

To allow event synchronization between HPOM and your two versions of OMi, you must modify the message forwarding policy on each HPOM management server with the node name of the load balancers, NAT device, or reverse proxy, if configured, or one Gateway Server for each OMi installation, as appropriate for your high availability arrangement.

To adapt the message forwarding policy, complete the following steps:

- 1** Start the HPOM for Windows console as follows:

Start > Programs (or All Programs) > HP > HP Operations Manager.

- 2** In the left pane of the HPOM for Windows console, select the following:

Policy management > Server policies grouped by type > Server-based Flexible Management.

- 3** In the right pane of the HPOM for Windows console, double-click the existing policy that you want to edit. The Server-based Flexible Management Editor dialog opens.

- 4 Add another message target manager as shown in the following example policy text:

```
TIMETEMPLATES
# none

RESPMGRCONFIGS
RESPMGRCONFIG DESCRIPTION "Forward all messages to 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 "<First Target Manager>"

MSGTARGETMANAGER
TIMETEMPLATE "$OPC_ALWAYS"
OPCMGR IP 0.0.0.0 "<OMi 8.10 fully qualified host name>"

MSGTARGETMANAGER
TIMETEMPLATE "$OPC_ALWAYS"
OPCMGR IP 0.0.0.0 "<BSM 9.1x fully qualified host name>"
```

Note: This forwards all messages to OMi. If you want to reduce the number of messages to be sent, see “Server-based Flexible Management” in the HPOM documentation and modify the text of the policy, so that only a selected subset of messages is sent to OMi.

- 5 Replace *<fully qualified host name>* in the text with the fully qualified hostname of the Gateway Server system that should receive HPOM messages (for example, HPGwSrv.example.com).

In deployments involving a load balancer, a NAT device, or a reverse proxy, use the fully qualified hostname of the system used to access the Gateway Server system (for example, VirtualSrv.example.com).

For details about load balancing and high availability, see the section “High Availability for HP Business Service Management” in the HP Business Service Management *Deployment Guide*.

- 6 Click **Check Syntax** to check for syntax errors in the new policy text.
- 7 After correcting any syntax errors, click **Save and Close**.
- 8 Redeploy the server-based flexible management policy on the HPOM for Windows management server.

Configuring the HPOM for UNIX and HPOM for Linux Forwarding Policy

To allow event synchronization between HPOM and OMi, you must modify the message forwarding policy on each HPOM management server with the node name of the load balancers, NAT device, or reverse proxy, if configured, or one Gateway Server, as appropriate for your high availability arrangement.

To adapt the message forwarding policy, complete the following steps:

- 1 Change to the work_respmgrs directory as follows:

```
cd /etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs/
```

Note: Policy template files can be found in:

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

- 2 Edit the existing policy to which you want to add the OMi system as a target as follows:

```
vi <policy file name>
```

- 3 Add another message target manager as shown in the following policy text:

```
TIMETEMPLATES
# none

RESPMGRCONFIGS
RESPMGRCONFIG DESCRIPTION "Forward all messages to 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 "<First Target Manager>"

MSGTARGETMANAGER
TIMETEMPLATE "$OPC_ALWAYS"
OPCMGR IP 0.0.0.0 "<OMi 8.10 fully qualified host name>"

MSGTARGETMANAGER
TIMETEMPLATE "$OPC_ALWAYS"
OPCMGR IP 0.0.0.0 "<BSM 9.1x fully qualified host name>"
```

Note: This forwards all messages to OMi. If you want to reduce the number of messages to be sent, see “Server-based Flexible Management” in the HPOM documentation and modify the text of the policy, so that only a selected subset of messages is sent to OMi.

- 4 Replace *<fully qualified host name>* in the text with the fully qualified hostname of the Gateway Server system that should receive HPOM messages (for example, HPGwSrv.example.com).

In deployments involving a load balancer, a NAT device, or a reverse proxy, use the fully qualified hostname of the system used to access the Gateway Server system (for example, VirtualSrv.example.com).

For details about load balancing and high availability, see the section “High Availability for HP Business Service Management” in the HP Business Service Management *Deployment Guide*.

- 5 Enter the following command to check for syntax errors in the new policy text:

```
/opt/OV/bin/OpC/opcmomchk -msgforw <policy file name>
```

- 6 After correcting any syntax errors, copy the policy to the respmgrs directory as follows:

```
cp <policy file name>
/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/
```

- 7 Restart the server processes as follows:

```
/opt/OV/bin/OpC/opcsv -stop
/opt/OV/bin/OpC/opcsv -start
```

Message forwarding from HPOM for UNIX to OMi is now configured and enabled.

Configuring HPOM Event Buffering

This task describes how to adjust the maximum length of the delivery timeout and the maximum size of the buffer file in HPOMs. Depending on the length of the forwarding outage and the number of events, you need to increase the timeout and the buffer size so that HPOM does not discard any unsent events.

To configure HPOM for Windows event buffering, complete the following steps:

- 1 In the console tree, right-click **Operations Manager**, and then click **Configure > Server...** The Server Configuration dialog box appears.
- 2 Click **Namespaces**, and then click **Server-based Flexible Management**.
- 3 Change the value of **Forwarding delivery timeout (in seconds)** (default 1 hour). For example, to set the timeout to 2 days, type **172800**.

- 4** Change the value of **Forwarding queue size maximum (in megabytes)** (default 50 MB). For example, to set the buffer size to 3 GB, type **3072**.
- 5** *Optional:* Change the value of **Forwarding queue size warning threshold (in megabytes)** (default 40 MB). For example, to set the warning threshold to 2.5 GB, type **2560**.
- 6** Click **OK** to save the new values and close the dialog.

To configure HPOM for UNIX or Linux event buffering, complete the following steps:

- 1** Adjust the timeout. For example, to set the timeout to 2 days, type:

```
ovconfchg -ovrg server -ns opc.opcforwm -set \  
REQUEST_TIMEOUT 172800
```

- 2** *Optional:* In HPOM for UNIX or Linux, the buffer size is by default set to 0 (unlimited). To change the buffer size, type

```
ovconfchg -ovrg server -ns opc.opcforwm -set \  
MAX_FILE_BUFFER_SIZE <bytes>
```

- 3** *Optional:* Check the current values of the HTTPS-based forwarding parameters, type:

```
ovconfget -ovrg server opc.opcforwm
```

The command displays only the non-default values.

Converting OMi 8.10 Content Packs to 9.1x Model and Syntax

This task describes how to convert the content packs that you exported from your OMi 8.10 installation in the step "Exporting the OMi Configuration Data" on page 207 to the syntax and model required by the BSM 9.1x version.

The ContentMigration migration tool is located in:

Windows: %TOPAZ_HOME%\opr\bin\ContentMigration.bat

Linux: /opt/HP/BSM/opr/bin/ContentMigration.sh

The ContentMigration migration tool accepts the following options:

ContentMigration *<inputFileName>* *<outputFileName>*
[-A *Availability_KPI_UUID*] [-P *Performance_KPI_UUID*]

For more information about the parameters that the **ContentMigration** command, see the following list:

<inputFileName>

Name of the input file. This must be an OMi Content Pack in XML file format from OMi 8.10.

<outputFileName>

Name of the output file, to which the BSM 9.1x formatted content pack XML file is written.

[-A *<Availability_KPI_UUID>*]

Optional: Specify an alternative availability KPI as the standard availability KPI assignment. For details, see "Alternative KPIs" on page 223.

[-P *<Performance_KPI_UUID>*]

Optional: Specify an alternative performance KPI as the standard availability KPI assignment. For details, see "Alternative KPIs" on page 223.

Note: By default the OMi 8.10 KPI assignments to Availability and Performance are replaced by assignments to System Availability and System Performance respectively. To assign alternative KPIs as the standard availability KPI assignment, see "Alternative KPIs" on page 223.

To convert an OMi 8.10 content pack to the model and syntax required by BSM 9.1x:

- 1** Copy the exported data output file of the content packs that you exported from your OMi 8.10 installation in the step "Exporting the OMi Configuration Data" on page 207. Store the output file in a temporary location on the BSM 9.1x Gateway Server host system that is upgraded first, for example:

Windows: %TEMP%\migration

Linux: \tmp\migration

- 2** On the BSM 9.1x Gateway Server host system, convert the exported content packs:
 - ▶ To convert the exported snapshot of all OMi 8.10 content packs, enter the following command:

Windows: %TOPAZ_HOME%\opr\bin\ContentMigration
<snapshot file name> <output file name>

Linux: /opt/HP/BSM/opr/bin/ContentMigration <snapshot file name> <output file name>

- ▶ To convert the exported custom content pack that contains your OMi 8.10 modifications, enter the following command:

Windows: %TOPAZ_HOME%\opr\bin\ContentMigration <custom file name> <output file name>

Linux: /opt/HP/BSM/opr/bin/ContentMigration <custom file name> <output file name>

Substitute the appropriate file names and specify alternative KPIs, if necessary. See also "Alternative KPIs" on page 223.

- 3** Copy the converted OMi 8.10 content pack *snapshot* to the following location on the BSM 9.1x Gateway Server host system:

Windows: %TOPAZ_HOME%\conf\opr\content\migration

Linux: /opt/HP/BSM/conf/opr/content/migration

The upgrade wizard automatically uploads all converted content packs that reside in that location.

Note: Do not copy the converted OMi 8.10 custom content pack to that location because you must manually upload that content pack *after* the migration. See "Recreating OMi 8.10 Modifications in 9.1x" on page 233 for more information.

- 4** *Optional:* Delete the original, unconverted OMi 8.10 content packs from the following temporary directory on the BSM 9.1x Data Processing Server host system:

Windows: %TEMP%\migration

Linux: /tmp/migration

Alternative KPIs

You can assign alternative KPIs to the default ones. To do this you need to know what KPIs are available and what their `stableId` attributes are in the `SH-DefaultKPIs.xml` file.

To assign alternative KPIs, complete the following steps:

- 1** Open the following file:

Windows: %TOPAZ_HOME%\conf\opr\content\en_US\
SH-DefaultKPIs.xml

Linux: /opt/HP/BSM/conf/opr/content/en_US/SH-DefaultKPIs.xml

- 2** Select an alternative KPI by its `stableId` attribute.

KPIs are contained in XML elements named `<Dimension>`. Select a KPI where the `application` attribute is equal to `dashboard` (`application="dashboard"`).

- 3** Run the `ContentMigration` migration tool and specify the `stableId` attribute of the selected KPI for the `-A` or `-P` parameters.

```
ContentMigration <exported_OMi_8.10_content_pack>.xml  
<converted_BSM_9.1x_content_pack>.xml  
-A <stableId_of_alternative_Availability_KPI>  
-P <stableId_of_alternative_Performance_KPI>
```

Restoring Custom Icons from OMi 8.10

If you want to continue to use the OMi 8.10 icons for health indicators, copy the saved OMi 8.10 files to the BSM 9.1x installation.

- 1 Because some of the icons have changed in 9.1x, from a BSM 9.1x Gateway Server host system, make a backup copy of all the files in the following directory and subdirectories:

Windows: %TOPAZ_HOME%\AppServer\webapps\site.war\images\gui\severities

Linux: /opt/HP/BSM/AppServer/webapps/site.war/images/gui/severities

- 2 Copy the custom icon files that you saved from your OMi 8.10 installation in the step "Backing Up OMi Configuration Files" on page 203 to the following location on the BSM 9.1x Gateway Server host system:

Windows: %TOPAZ_HOME%\AppServer\webapps\site.war\images\gui\severities

Linux: /opt/HP/BSM/AppServer/webapps/site.war/images/gui/severities

OMi 8.10 to 9.1x Post-Upgrade Procedure

Perform this procedure after running the upgrade wizard when upgrading from BAC 8.x to BSM 9.1x.

1 (Staging Only) Configure the HPOM Message Forwarding Policy for the BSM 9.1x Installation Only - Optional

Remove the entry for the obsoleted OMi 8.10 installation from all HPOM message forwarding policies. For details on modifying an HPOM message forwarding policy, see "Configuring the HPOM for Windows Forwarding Policy" on page 215 or "Configuring the HPOM for UNIX and HPOM for Linux Forwarding Policy" on page 217 as appropriate for your HP Operations Manager product.

2 Manage BSM Nodes in HPOM

In HPOM, update the nodes that represent the BSM systems.

For details, see "Managing BSM Nodes in HPOM" on page 227.

3 (Staging Only) Validate Event Synchronization

Validate event synchronization and test the connection between HPOM and OMi. For details, see "Validating Event Synchronization" on page 230.

4 Validate Topology Synchronization

Copy the saved topology synchronization rules to the BSM 9.1x installation. If you have created custom synchronization packages that use out-of-the-box CI types, make sure that your synchronization packages still produce the desired results in BSM 9.1x. For details, see "Validating Topology Synchronization" on page 231.

5 Recreate Your OMi 8.10 Modifications in 9.1x - Optional

If you upgraded the SPIs to the SPI DVD 2010 release *before* the migration, you must manually recreate the modifications that you applied to the OMi 8.10 content in your 9.1x installation. Refer to the notes taken in "Make a Note of Each Modification to the OMi 8.10 Content Packs" on page 200.

Alternatively, if you exported and converted a custom content pack, upload the custom content pack in create mode after the migration. For details, see "Recreating OMi 8.10 Modifications in 9.1x" on page 233.

6 Re-import the 9.1x Content - Optional

If you did *not* upgrade the SPIs to the SPI DVD 2010 release before the migration, but rather decide to switch to the new SPIs after the migration, you must reimport the 9.1x content with overwrite mode. However, the overwrite mode will overwrite *all* of your modifications. You must then manually recreate your OMi 8.10 modifications in the 9.1x content. For details, see "Uploading 9.1x Content in overwrite Mode" on page 233.

7 Complete the Upgrade to BSM 9.1x

After having completed the OMi post-upgrade steps, complete the upgrade to BSM 9.1x. For details, see:

Staging upgrades. "Exit staging mode" on page 30.

Direct upgrades. "Continue with main upgrade procedure" on page 33.

Managing BSM Nodes in HPOM

To enable communication between HPOM and OMi 8.10, the BAC 8.x servers were set up as managed nodes in HPOM (but no HP Operations Agent software installed). After the migration, the managed nodes that represent the BAC 8.x servers are no longer needed in HPOM and you can delete them. For details, see "Deleting BAC 8.x Managed Nodes in HPOM" on page 227. (The BSM 9.1x servers do not need to be added to HPOM to enable communication.)

Do not delete the BAC 8.x managed nodes if the HP Operations Agent software is installed and HPOM monitors the BAC 8.x servers for the purpose of system and performance management:

- ▶ For direct upgrades, if this is the case, you must update the nodes' core IDs in HPOM because the systems have received new certificates. For details, see "(Direct Only) Updating the Core IDs in HPOM for Windows" on page 228 and "(Direct Only) Updating the Core IDs in HPOM for UNIX and HPOM for Linux" on page 229
- ▶ If you are performing a staging upgrade and you want to monitor the new BSM 9.1x systems with HPOM, add the 9.1x systems as new managed nodes to HPOM and install the HP Operations Agent software to these nodes. For details, see the HPOM documentation.

Deleting BAC 8.x Managed Nodes in HPOM

To enable communication between HPOM and OMi 8.10, the BAC 8.x servers were set up as managed nodes in HPOM (but no agent software installed). After the migration, the managed nodes that represent the BAC 8.x servers are no longer needed in HPOM and you can delete them.

Note: Do not delete the BAC 8.x managed nodes if the HP Operations Agent software is installed and HPOM monitors the BAC 8.x servers for the purpose of system and performance management.

To delete the BAC 8.x managed nodes in HPOM for Windows, complete the following steps:

- 1** Open the Configure Nodes dialog, right-click the **Nodes** folder in the console tree and select **Configure > Nodes**.
- 2** Select the nodes that represent the BAC 8.x servers and press the **Delete** key.
- 3** Click **Yes** to confirm that you want to delete the nodes.
- 4** Close the Configure Nodes dialog.

To delete the BAC 8.x managed nodes in HPOM for UNIX or Linux, complete the following step:

On the HPOM for UNIX or Linux management server, use the `opcnode` command line tool to delete the nodes, type:

```
# opcnode -del_node node_name=<node_name> \  
net_type=<network_type>
```

<node_name>: Name of the managed node that you want to remove from the HPOM database.

<network_type>: Type of managed node, for example: Non IP, IP (Network), or External (Node).

The `opcnode` command also ensures that the managed node's assignment to any node groups is removed. For more information about the `opcnode` command and its parameters and options, see the *opcnode(1m)* manual page.

(Direct Only) Updating the Core IDs in HPOM for Windows

The BAC 8.x Data Processing Servers, Gateway Servers, and load balancers still exist as managed nodes in HPOM. However, because these systems may have received new certificates, you must update their core IDs in HPOM.

To update the core ID in HPOM complete the following steps:

- 1** On the BSM 9.1x Processing Servers, Gateway Servers, and load balancers identify the core ID, type:

Windows: `ovcoreid`

Linux: `/opt/OV/bin/ovcoreid`

- 2** On the HPOM for Windows system, start the HPOM for Windows console as follows:
Start > Programs (or All Programs) > HP > HP Operations Manager
- 3** Click **HP Operations Manager Console**.
- 4** Right-click **Nodes** and select **Configure > Nodes**.
The **Configure Managed Nodes** dialog box opens.
- 5** Right-click the managed node that you want to modify in the right pane and select **Properties**.
The **Node Properties** dialog box opens.
- 6** Click **General** to open the **General** tab.
- 7** Click **Advanced Configuration**.
The **Advanced Configuration** dialog box opens.
- 8** Select **Modify Agent ID/Core-ID** and paste the new core ID into the box.
- 9** Click **OK** to save your changes and close all dialog boxes.

(Direct Only) Updating the Core IDs in HPOM for UNIX and HPOM for Linux

The BAC 8.x Data Processing Servers, Gateway Servers, and load balancers still exist as managed nodes in HPOM. However, because these systems may have received new certificates, you must update their core IDs in HPOM. Complete the following steps:

To update the core ID in HPOM complete the following steps:

- 1** On the BSM 9.1x Processing Servers, Gateway Servers, and load balancers identify the core ID, type:
Windows: `ovcoreid`
Linux: `/opt/OV/bin/ovcoreid`
- 2** On the HPOM for UNIX or HPOM for Linux system, type the following command:
`/opt/OV/bin/OpC/utils/opcnode -chg_id node_name=<node_name>
id=<new_id>`

Replace `<node_name>` with the fully qualified domain name of the BSM Processing Server, Gateway Server, and or balancer. Replace `<new_id>` with the output of the `ovcoreid` command.

Validating Event Synchronization

This section provides you with instructions about how to validate event synchronization and test the connection between HPOM and OMi.

To verify message forwarding from HPOM to OMi complete the following steps:

In this section, you check whether the message forwarding policy for sending messages from HPOM to OMi is correctly configured. To do so, complete the following steps:

- 1** Make sure the BSM platform is running.
- 2** Make sure at least one open message interface policy is deployed on your HPOM system. For instructions and details, see the HPOM documentation.
- 3** On the HPOM system, open a command or a shell prompt.
- 4** Create a new message by executing the following command:
 - ▶ On the HPOM for Windows system:
`opcmsg a=App o=Obj msg_text="Hello"`
 - ▶ On the HPOM for UNIX and HPOM for Linux system:
`/opt/OV/bin/OpC/opcmsg a=App o=Obj msg_text="Hello"`

If you have correctly configured the server-based flexible management, the message arrives at the HPOM management server and is forwarded to OMi. You can view the events with the Operations Management Event Browser.

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

To verify the synchronization of HP OMi events with HPOM messages, complete the following steps:

- 1** Make sure the BSM platform is running.
- 2** Log on to the BSM platform management console.
- 3** Click **Applications > Operations Management**.
- 4** In the Event Browser, select an event that has been synchronized in HPOM and OMi earlier.
- 5** In the Event Details pane, click the Edit button of the General tab.
- 6** From the Severity drop-down list, choose another severity (for example, major) and click **Save** to change it to the selected severity.
- 7** In HPOM, verify the severity of this event and make sure it has been set to the new severity value.

Validating Topology Synchronization

If you have modified the out-of-the-box topology synchronization packages, you must manually recreate your changes in the 9.1x topology synchronization packages.

If you have created and saved your own custom topology synchronization packages in OMi 8.10, copy the saved custom packages to the BSM 9.1x installation. If these custom synchronization packages use out-of-the-box CI types, make sure that your synchronization packages still produce the desired results in BSM 9.1x, complete the following steps.

To validate topology synchronization, complete the following steps:

- 1** Copy the custom topology synchronization rules that you saved from your OMi 8.10 installation in the step "Backing Up OMi Configuration Files" on page 203 to the following location on the BSM 9.1x Data Processing Server host system:

Windows: %TOPAZ_HOME%\conf\opr\topology-sync\sync-packages

Linux: /opt/HP/BSM/conf/opr/topology-sync/sync-packages

- 2** On the BSM 9.1x Data Processing Server host system, run basic topology synchronization. Open a command prompt or shell and type:

Windows: %TOPAZ_HOME%\bin\opr-startTopologySync.bat

Linux: /opt/HP/BSM/bin/opr-startTopologySync.sh

- 3** If out-of-the-box CI types have changed in BSM 9.1x, the synchronization process ends with errors. Check the synchronization log file:

Windows: %TOPAZ_HOME%\log\opr-topologysync

Linux: /opt/HP/BSM/log/opr-topologysync

- 4** Enable the data dump option and verify the CI attributes:

- a** Navigate to the HPOM Topology Synchronization settings in the Infrastructure Settings Manager:

Infrastructure Settings > Applications > Operations Management > Operations Management - HPOM Topology Synchronization Settings > Dump data

- b** Change the value of **Dump data** to **true**.

- c** Run the Topology Sync tool with the following command:

Windows: <HPBSM root directory>\bin\opr-startTopologySync.bat

Linux: <HPBSM root directory>/bin/opr-startTopologySync.sh

- d** Check if the file in the following directory contains all expected attributes for the CIs of your synchronization package:

Windows: %TOPAZ_HOME%\opr\tmp\datadump\postenrichment

Linux: /opt/HP/BSM/opr/tmp/datadump/postenrichment

- 5** Use the BSM 9.1x CI Type Manager to find changed CI types, adapt your mapping rules, and run topology synchronization again.

Repeat this process until all mapping errors have been resolved.

For more information about topology synchronization, see the HP Operations Manager i *Extensibility Guide*.

Recreating OMi 8.10 Modifications in 9.1x

If you upgraded the SPIs to SPI DVD release 2010 before the migration, you must manually recreate the modifications that you applied to the OMi 8.10 content in your 9.1x installation. Refer to your notes taken in "Make a Note of Each Modification to the OMi 8.10 Content Packs" on page 200.

Alternatively, if you exported and converted a custom content pack, upload the custom content pack in `create` mode after the migration.

To recreate upload the custom content pack in create mode, complete the following steps:

- 1 Change to the temporary location on the BSM 9.1x Gateway Server host system, where the converted custom content pack resides, for example:

Windows: %TEMP%\migration

Linux: /tmp/migration

- 2 Upload the custom content pack in `create` mode, enter the following command:

```
<HPBSM Install Directory>/opr/bin/ContentManager -username
admin -password admin -i <converted custom content pack>
```

Where the administrator account must have read and write access to the Content Manager.

- 3 Verify the uploaded content pack in the Content Packs Manager.

Uploading 9.1x Content in overwrite Mode

After the migration, if you decide to switch to the SPI DVD release 2010, you can reimport the 9.1x content with `overwrite` mode. However, the `overwrite` mode will overwrite *all* of your modifications. You must then manually recreate your OMi 8.10 modifications in the 9.1x content.

To reimport 9.1x content, complete the following steps:

- 1 Upgrade the HP Operations SPIs to SPI DVD release 2010 as described in the documentation provided with the SPIs.
- 2 Reimport the 9.1x content in `overwrite` mode, enter the following command:

```
<HPBSM Install Directory>/opr/bin/ContentManager -username  
admin -password admin -a -forceReload -f
```

- 3 Manually recreate your OMi 8.10 modifications in the 9.1x content. Refer to the notes taken in "Make a Note of Each Modification to the OMi 8.10 Content Packs" on page 200.

OMi 9.0x to 9.1x Pre-Upgrade Procedure

Perform the following steps before beginning the upgrade to BSM 9.1x from BSM 9.0x with OMi.

1 Back Up OMi Configuration Files

If you have customized the OMi integration with HP Service Manager or any topology synchronization data, back up your customized files before starting the upgrade to BSM 9.1x. For details, see "Backing Up OMi Configuration Files" on page 236.

2 Clean Up Indicators with the Same Name

In BSM 9.0x, it is possible to modify health indicators (HIs) that child configuration item types (CITs) acquire from their parent CITs. When you modify an inherited HI its UUID changes but the name remains the same. Subsequent uploads of content packs in overwrite mode then lead to errors. For details, see "Cleaning Up Indicators With the Same Name" on page 236.

3 Delete TV Content Pack Definitions

You must delete the TV Content Pack and the TVDiag Shared Content Pack definitions before beginning to upgrade to BSM 9.1x. For details, see "Deleting TV Content Pack Definitions" on page 237.

4 Delete Duplicate Downtime Categories

You must delete any duplicate downtime categories before beginning to upgrade to BSM 9.1x. For details, see "Deleting Duplicate Downtime Categories" on page 238.

5 Delete Graph Family Assignments in Blackberry Content Pack

To avoid upload problems after the upgrade, delete the performance graph family assignments in the Content Pack for Blackberry Enterprise Servers before the upgrade. The upload of the 9.1x Blackberry content pack recreates the correct assignments. For details, see "Deleting Graph Family Assignments in Blackberry Content Pack" on page 238.

6 Archive OMi Events

To avoid lengthy database upgrades, it is recommended that you archive your open and closed OMi events before starting the upgrade wizard. You should not keep more than 100,000 events in the database. To archive OMi events, use the archive tool opr-archive-events. For details about opr-archive-events, see the Operations Management online help.

7 Continue upgrading to BSM 9.1x.

After having completed the OMi pre-upgrade steps, continue upgrading to BSM 9.1x. For details, see "Uninstall BSM 9.0x" on page 30.

Backing Up OMi Configuration Files

If you have customized the OMi integration with HP Service Manager or any topology synchronization data, back up your customized files before starting the upgrade to BSM 9.1x.

To back up the integration and the topology synchronization data, complete the following steps:

- 1 From the BSM 9.0x Data Processing Server host system, make a copy of all the files in the following directory and subdirectories:

`%TOPAZ_HOME%\conf\opr\integration`

`%TOPAZ_HOME%\conf\opr\topology-sync`

- 2 Save these files to a safe location on the BSM Data Processing Server host system, for example:

Windows: `%TEMP%\migration`

Linux: `/tmp/migration`

Cleaning Up Indicators With the Same Name

In BSM 9.0x, it is possible to modify health indicators (HIs) that child configuration item types (CITs) inherit from their parent CITs. Modifications include, for example, changing the display name or description. When you modify an inherited HI its UUID changes but the name remains the same. Subsequent uploads of content packs in overwrite mode then lead to errors like the following:

Indicator with id: <uuid>. Cause: Indicator already exists with the same name for this CI type hierarchy. Indicator name: <indicator>.

To prevent upload problems, perform the following steps:

- 1 Enable the BSM server(s) by selecting **Start > Programs > HP Business Service Management > Administration > Enable HP Business Service Management**.
- 2 Before the upgrade, manually merge the changes applied to inherited indicators with the original indicator defined for the parent CIT.

Go to **Admin > Service Health > Repositories**. Select the child CIT and the health indicator that you have modified. Check your changes and then apply them to the HI of the parent CIT.

3 Delete the modified HI.

Alternatively, before the upgrade, make a note of your HI modifications, and then delete the modified HIs. After the upgrade, create new HIs for the child CITs, based on your notes.

4 Disable the BSM server(s) by selecting **Start > Programs > HP Business Service Management > Administration > Disable HP Business Service Management**.

Deleting TV Content Pack Definitions

You must delete the TV Content Pack and the TVDiag Shared Content Pack definitions (if their IDs start with a specific string) before beginning to upgrade to BSM 9.1x. Otherwise the upload fails with the following error in **opr-admin.log**:

A Content Pack Definition with the name [TV_Content_Pack] and a different ID already exists.

To delete TV content pack definitions, complete the following steps:

1 Open the Content Packs Manager:

Admin > Platform > Content Packs

2 In the Content Packs Definitions pane, select TV Content Pack and edit it. If the ID starts with 6f0, delete the content pack definition.

3 In the Content Packs Definitions pane, select TVDiag Shared Content Pack and edit it. If the ID starts with 045, delete the content pack definition.

Deleting Duplicate Downtime Categories

The upgrade may fail if more than one downtime category with the same name exists. You must therefore delete all duplicate downtime categories before beginning the upgrade to BSM 9.1x.

To delete duplicate Downtime Categories, complete the following steps:

- 1 Navigate to the Downtime Behavior manager:

Admin > Operations Management > Tune Operations Management > Downtime Behavior

- 2 Refresh the list of categories.
- 3 If there is more than one entry per category, delete the duplicate categories. Access the Event Schema database using a database administration tool (for example, Microsoft SQL Server Management Studio).
- 4 Open the table DOWNTIME_CONFIG.
- 5 Make sure there is only one line per DT_CATEGORY_ID.
Delete all other rows with that ID or change the ID to another existing Downtime Category.

Deleting Graph Family Assignments in Blackberry Content Pack

The 9.0x Content Pack for Blackberry Enterprise Server generates unique IDs for configuration item type to graph family assignments. Because the IDs are different in each BSM installation, the upload of the new 9.1x Blackberry content pack fails. To avoid upload problems after the upgrade, delete the graph family assignments before the upgrade. The upload of the 9.1x Blackberry content pack recreates the correct assignments.

To delete graph family assignments, complete the following steps:

- 1 Navigate to the Performance Graphs manager:

Admin > Operations Management > Design Operations Content > Performance Graphs

- 2** In the **CI Types** pane, select **ConfigurationItem > Infrastructure Element > Running Software > Application Server > BB Component**.
- 3** In the **Performance Graphs** pane, click the **Delete Item** toolbar button to remove the performance graphs configuration from the selected CI type.

OMi 9.0x to 9.1x Post-Upgrade Procedure

Perform the following steps after running the upgrade wizard when upgrading to BSM 9.1x from BSM 9.0x with OMi.

1 Restore OMi Configuration Customizations

Apply your customizations from the saved OMi configuration files to the BSM 9.1x configuration files. For details, see "Restoring OMi Configuration Customizations" on page 240.

2 Import Security Certificates to JRE Truststore

Secure environments only: To re-enable the trust relationship between the Java Runtime Environment (JRE) and the LDAP server, you must import the LDAP trusted certificate to the JRE truststore. For details, see the *HP Business Service Management Hardening Guide PDF*.

3 Migrate Content from 9.0x to 9.1x

Content is uploaded automatically on the first BSM startup using the create mode. The create mode ignores modified objects in the 9.1x content packs and uploads new and unchanged objects only. If you have also modified the same objects, you can either redo your modifications manually after the migration has finished, or upload the upgrade content packs manually using the overwrite mode. See "Importing Modified Upgrade Content Packs" on page 242 for details.

4 Continue upgrading to BSM 9.1x.

After having completed the OMi post-upgrade steps, continue upgrading to BSM 9.1x. For details, see "Service Health and SLM post-upgrade procedure" on page 32.

Restoring OMi Configuration Customizations

The OMi integration and topology synchronization files have changed with BSM 9.1x. It is therefore recommended that you merge your saved OMi customizations with the BSM 9.1x configuration files rather than replacing them.

- 1 On the BSM 9.1x Data Processing Server host system, make a backup copy of all the files in the following directory and subdirectories:

Windows: %TOPAZ_HOME%\conf\opr

Linux: /opt/HP/BSM/conf/opr

- 2 Merge the OMi integration and topology synchronization files that you saved from your BSM 9.0x installation in the step "Backing Up OMi Configuration Files" on page 236 with the BSM 9.1x configuration files.

The OMi integration and topology synchronization files reside in the following location on the BSM 9.1x Data Processing Server host system

Windows:

`%TOPAZ_HOME%\conf\opr\integration`

`%TOPAZ_HOME%\conf\opr\topology-sync`

Linux:

`/opt/HP/BSM/conf/opr/integration`

`/opt/HP/BSM/conf/opr/topology-sync`

Migrating Content from 9.0x to 9.1x

Content is uploaded automatically on the first BSM startup using the `create` mode. The `create` mode ignores modified objects in the 9.1x content packs and uploads new and unchanged objects only. The HP-modified objects are described in the following file:

`%TOPAZ_HOME%\conf\opr\content\migration\bdm_changes.xml`

`/opt/HP/BSM/conf/opr/content/migration/bdm_changes.xml`

Note: New HI Values are not new objects, but a modification of the Health Indicator, which is a modification of the objects in your content pack.

If you have also modified the same objects, you can either redo your modifications manually after the migration has finished, or upload the upgrade content packs manually using the `overwrite` mode. See "Importing Modified Upgrade Content Packs" on page 242 for details.

The upgrade content pack packages are located in the following directory:

`<HPBSM Install Directory>/conf/opr/content/upgrade/<locale>`

The available upgrade content pack packages are:

- ▶ MM-INF_upgrade.xml — Content Pack for Infrastructure SPI
- ▶ MM-JEE_upgrade.xml — Content Pack for J2EE SPI
- ▶ MM-MSS_upgrade.xml — Content Pack for MS SQL SPI
- ▶ MM-Ora_upgrade.xml — Content Pack for Oracle SPI

Importing Modified Upgrade Content Packs

You can import individual upgrade content packs one by one or all content packs at once. Individual content packs can also be uploaded using the user interface.

To upload *individual* upgrade content packs, complete the following steps:

```
<HPBSM Install Directory>/opr/bin/ContentManager -username admin  
-password admin -f -i <HPBSM Install Directory>/conf/opr/  
content/upgrade/<locale>/<Content Pack to Import>
```

To upload *all* upgrade content packs, complete the following steps:

```
<HPBSM Install Directory>/opr/bin/ContentManager -username admin  
-password admin -a -f -uploadFolder <HPBSM Install  
Directory>/conf/opr/content/upgrade/<locale>
```

17

Platform Upgrade Information

This chapter includes:

- ▶ Recipient Management Upgrade on page 243
- ▶ Downtime Upgrade on page 243
- ▶ User Management Upgrade on page 244
- ▶ Locations Updates on page 244
- ▶ Database Native Partitioning on page 247

Recipient Management Upgrade

In BAC 8.x and below, recipients were assigned time offsets relative to GMT, such as GMT+02.00. From BSM 9.0 and later, recipients are assigned time zones associated with specific cities, such as (GMT+2.00) Europe, Athens. The translation of time offset to time zone is configured in the following file: <HPBSM root directory>\xml\site_xml\timezones.xml.

Downtime Upgrade

In BAC 8.x and below, downtimes were defined with offsets relative to GMT, such as GMT+02.00. From BSM 9.0 and later, downtimes are assigned time zones associated with specific cities, such as (GMT+2.00) Europe, Athens.

Downtimes are upgraded to have the user default time zone unless configured to use a different time zone in the following file: <HPBSM root directory>\dat\downtimeupgrade\downtime_upgrade_timezone.xml.

For example:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<DowntimeUpgradeTimeZone id="Australia/Adelaide"/>
```

User Management Upgrade

After upgrading to BSM 9.1x, users without assigned roles have no access to custom query reports, and cannot see existing favorite filters of other users in the Report Manager.

System Viewers and above are assigned Add and View permissions; and Administrators have Full Control permission to the Custom Query Reports resource, in the User Defined Reports context.

System Viewers and above are assigned View permission; System Modifiers and above are assigned Change and Delete permissions; and Administrators have Full Control permission to the Favorite Filter resource, in the User Defined Reports context.

Locations Updates

There are a number of scenarios in which the BSM 9.1x upgrade will automatically map pre-existing CIs to fit with the new **Locations Manager** model developed for BSM 9.0. For more information, see "Location Manager" in *Platform Administration*.

Note: Geographical location CIs are CIs of type **location** whose name is a geographical location defined by **IP2Location** (IP2Location.com). Logical location CIs are CIs of type **location** whose name is not a geographical location defined by **IP2Location**.

CI Type RUM Location Container

CI of type **RUM Location Container** no longer exist in BSM 9.x. These CIs are automatically converted to CIs of type **location**.

CIs with locations in properties

CIs which had **country**, **state**, or **city** properties contained location data. The BSM 9.1x upgrade creates a new CI of type **location** for each country, state, and city property value. The original CI is then related to the new location CIs.

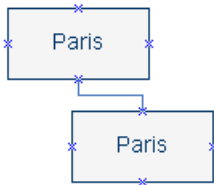
Example: If there was a CI named **Server123** that had the following properties: **country=USA**, **state=Nevada**, **city=Las Vegas**. During the upgrade to BSM 9.1x, three new CIs of type **location** would be created: **USA**, **Nevada**, and **Las Vegas** with appropriate relations indicating their hierarchical relationship. The CI **Server123** would then be related to **Las Vegas**.

Example: If there was a CI of type **location** name **Building1** that had the following properties: **country=USA**, **state=California**, **city=Los Angeles**. During the upgrade to BSM 9.1x, three new CIs of type **location** would be created: **USA**, **California**, and **Los Angeles** with appropriate relations indicating their hierarchical relationship. The CI **Building1** would then be related to **Las Vegas**. Note that in this case the CI **Building1** is not a member of the **IP2Location** list of geographical locations, and thus is a logical location CI.

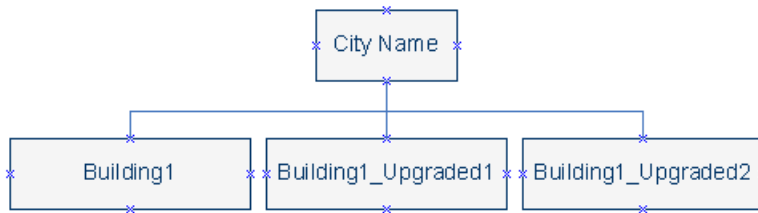
Duplicate CIs

In BAC 8.x, multiple CIs of type location with the same name were valid. In BSM 9.x, location CIs with the same parent can not have the same name. Additionally, locations under World (first level locations) cannot share a name and location type with any other CI. Due to these changes, the following CI's are automatically updated:

Duplicate Geographical CIs. If there is more than one geographical CI with the same location attributes, it is added to the original geographical CI as a child.



Duplicate Logical CIs. The CIs are all linked to the appropriate geographical location CI. Duplicates are appended with the string **Upgradedx**.



Duplicate Locations. Locations under World (first level locations) cannot share a name and location type with any other CI. If CIs that fit this description existed in BAC 8.x, the string **Upgradedx** is appended to the end of the name of the lower level duplicate CIs.

Global Location List Changes

If the attributes of a CI are of a city, state, or country that no longer exists in the **IP2Location** list, logical location CIs are created instead of geographical location CIs.

USA Cities with Unspecified States

If a city located in the USA in 8.x does not have an assigned state, the upgrade will place this CI under the hierarchy USA > Unknown State.

Database Native Partitioning

In BSM 9.0 and later, the only method used by the Partition and Purging Manager to partition historical data (of the profile databases) is the Native Partitioning method.

In an Oracle database, the **Oracle Partitioning** option must be enabled. If the Oracle Partitioning option is not available, the Partition and Purging Manager will not partition or purge data, which may result in major performance issues.

In an SQL database, make sure the **Compatibility Level** database setting is set to reflect the version of SQL server that you are using in each of the BSM 9.1x database schemas. For example if you are using SQL SERVER 2005, the compatibility level should be 90. This will ensure the activation of the native partitioning option.

18

Reports Upgrade Information

This chapter includes:

- Custom Query Builder Upgrade on page 249
- Custom Reports and Favorite Filters on page 251

Custom Query Builder Upgrade

Some of the field names of the alert samples used in the Custom Query Builder were changed.

If a Custom Query Builder was created in BAC 8.x using the `profile_name` field, the following happens during the upgrade:

- 1** If the profile is not linked to any application, an upgraded application will be created with the profile name followed by a "_application" post fix (for example, "myProfile_application").
- 2** If the profile was linked to several applications, same as (1).
- 3** If the profile was linked to a single application, an upgraded application will be created with the application name. If another profile is linked to the same application, the upgraded application will have the postfix ".1" and so on.

In all above cases, under the created application, the upgrade creates a btf with the profile name, an error is logged, and the Custom Query Builder includes the old expression with the `profile_name` field.

A field that is obsolete and was not translated displays in its column the following string: Obsolete Field(s).

Profile Name	Green Threshold	Red Threshold	Red Threshold - Green Threshold
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for CI status alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for event-based alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for event-based alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for event-based alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for event-based alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)
BPM for event-based alerts	Obsolete Field(s)	Obsolete Field(s)	Obsolete Field(s)

Limitations:

- ▶ If a field (for example: dRedThreshold of the trans_t sample), which is obsolete in version 9.1x, was used in the previous version in the Filter box in the Filters dialog box, it is not translated during the upgrade and it is kept as is in the statement. When you generate the report, an exception is issued because of the non-existing field. In such case, open the Filter Builder form, remove the obsolete fields -(that are displayed as blank fields) and regenerate the report.
- ▶ If, in version 8.x, a Custom Report included a Response Time 90th Percentile report, after the upgrade to 9.x, the Custom Report is upgraded but is empty as the Response Time 90th. Percentile report is not supported in 9.x. You should delete this upgraded Custom Report.
- ▶ Favorite Filters and Custom Query Reports created in previous versions using samples that no longer exist in BSM version 9.1x are not upgraded. The samples that are no longer supported are: bla_s_on and bsl_stat_t.

Custom Reports and Favorite Filters

If you selected the Favorite Filters and Custom Report option in the Upgrade Wizard, and the relevant reports have these capabilities, the Favorite Filters that you created for specific reports and the custom reports that you configured in version 8.0 are upgraded to version 9.0. Note that some of the reports have changed names during the upgrade. For details, see "Reports" on page 253.

If you used specific SQL reserved words in Field Formulas or Field Aliases in the Custom Reports or Favorite Filters of the previous version, the queries upgrade might cause problems. The reserved words are as follows:

- SELECT
- WHERE
- FROM
- TOP
- HAVING
- Aliasing with the AS keyword
- OR , AND , NOT
- DISTINCT modifier (only supported for select list items)
- IN
- BETWEEN
- IS NULL
- LIKE
- +, -, *, /, (,)
- =, IS, !=, <>, >, >=, <, <=
- ORDER BY , ASC and DESC

Trend Reports Upgrade

The following measurements are deprecated in BSM 9.1x and are not upgraded. If you had used one of these measurements in the Trend report in version 8.xx the upgrade ignores the measurement and does not display the measurement in the corresponding Trend report in 9.1x:

- For page:
 - main_http_err
 - tot_server_b_sth
 - tot_hits_b_sth
 - http_err_bad_c
 - http_err_ref_c
 - http_err_nfound_c
 - http_err_serr_c
 - tot_dl_b_dth
 - tot_hits_b_dth
 - tot_frstbfr_o_fbth
 - tot_frstbfr_b_fbth
 - tot_hits_o_fbth
 - tot_hits_b_fbth
- For end user group:
 - tot_page_o_lth
 - tot_page_b_lth
 - new_tot_page_hits
 - tot_conn_b_lth
 - tot_conn_o_lth
 - tot_latency_o_lth
 - tot_latency_b_lth
 - tot_unavailable_page_hits

Reports

The upgrade from Business Availability Center 8.0x to BSM 9.0, modifies the names of some of the End User Management reports, creates new reports, and deprecates some of the reports, as shown in the table below.

Report Name 8.0 (A - Z)	Report Name 9.0
Availability Over Time	Metrics Over Time
BPM Transaction Invocation tool in Advanced Analytics	BPM Transaction Invocation
Breakdown Over Time	Transaction Breakdown Over Time
Breakdown Summary	Performance Analysis by Transaction
End Users by Page	End User by Action
Event Count Over Time	Metrics Over Time
Location Analysis	Performance Matrix grouped by Location
Min./Max. Response Time - Group by Group	Performance Status by Application
Min./Max. Response Time - Group by Location	Performance Status by Location
Min./Max. Response Time - Group by Transaction	Performance Status by Transaction
N/A	Action Details
N/A	Action Raw Data
N/A	Action Summary Filtered by Server
N/A	Session Summary
N/A	Page Component Breakdown
N/A	WebTrace By Demand

Report Name 8.0 (A - Z)	Report Name 9.0
N/A	Software Element Over Time
N/A	Software Elements by Transaction
N/A	Location Summary
N/A	Deviation Patterns Report
N/A	Deviation Patterns Details Report
N/A	WebTrace Report
N/A	Hop Report
N/A	Application Health
N/A	Performance Status
N/A	Performance Raw Data
N/A	Abandoned Transactions Summary
N/A	Abandoned Transaction Details Report
Network Analysis	WebTrace/Hop Report
Overall Performance by Profiles	Application Summary BPM as Data Collector
Overall Performance of 3 Worst Locations	Performance Status by Location
Overall Performance of 3 Worst Profiles	Performance Status by Application
Page Over Time	Action Over Time
Page Summary	Action Summary
Pages by Server Summary	Action Summary
Performance Matrix - Group by Group	Application Summary
Performance Matrix - Group by Location	Performance Matrix by Location

Report Name 8.0 (A - Z)	Report Name 9.0
Performance Matrix - Group by Transaction	Performance Matrix by Transaction
Performance of Locations	Performance Status by Location
Performance of Transactions	Performance Status by Transaction
Profile Summary	Application Summary
Profile Summary	Application Summary BPM as Data Collector
Response Time - 90th Percentile - Group by Group	Response Time by Percentile by Transaction
Response Time - 90th Percentile - Group by Location	Response Time by Percentile by Location
Response Time - 90th Percentile - Group by Transaction	Response Time by Percentile by Transaction
Response Time by Percentile - Group by Group	Response Time by Percentile by Transaction
Response Time by Percentile - Group by Location	Response Time by Percentile by Location
Response Time by Percentile - Group by Transaction	Response Time by Percentile by Transaction
Response Time Over Time	Metrics Over Time
Server Summary	Infrastructure Summary
Servers by Page Summary	Infrastructure Elements by Action
Single Profile Summary	N/A (deprecated)
TCP Application over Time	Tiers Over Time
TCP Application Summary	Tiers Summary
Transaction Analysis	Performance Matrix grouped by Transaction

Chapter 18 • Reports Upgrade Information

Report Name 8.0 (A - Z)	Report Name 9.0
Transaction Availability	Performance Analysis by Transaction
Unconfigured End Users by City	N/A (deprecated)
Unconfigured End Users by Country/State	N/A (deprecated)
WebTrace by Location	WebTrace/Hop Report

19

Dashboard and My BSM Upgrade Information

This chapter includes:

- ▶ What's Changed? on page 258
- ▶ Custom Rules on page 261
- ▶ KPI Upgrade on page 262
- ▶ CI Status Alerts Upgrade on page 268
- ▶ SiteScope and EMS KPI Assignment Upgrade on page 270
- ▶ SiteScope KPI Assignments Associated With Custom KPIs on page 275
- ▶ Propagation Rule Upgrade on page 276
- ▶ Repositories Upgrade on page 277
- ▶ View Upgrade and Monitor Removal on page 278
- ▶ SiteScope Monitors Associated with Non-default CIs or Multiple CIs on page 282
- ▶ My BSM Upgrade on page 286

What's Changed?

The following section describes what changed in Dashboard and My BSM, from BAC 8.x to BSM 9.x.

This section includes the following topics:

- ▶ "Dashboard and My BSM were renamed" on page 258
- ▶ "Monitor CIs were removed" on page 258
- ▶ "Health indicators were added and KPIs were modified" on page 259
- ▶ "Additional changes in Service Health 9.x" on page 260
- ▶ "XML adapter is deprecated" on page 261
- ▶ "Limitation in Custom Image" on page 261
- ▶ "Changes in MyBSM 9.x" on page 261

Dashboard and My BSM were renamed

In BSM 9.x, Dashboard is renamed to **Service Health**, and My BSM is called **MyBSM**.

Monitor CIs were removed

In BAC 8.x, each monitored CI had a child CI which was called a **monitor CI**. KPIs which provided information on the monitored CI were assigned to its child CI - the monitor CI.

For example, if you wanted to monitor CPU load on a computer, the computer CI (representing an actual computer) had a monitor CI as its child, and the System KPI monitoring CPU load was assigned to the monitor CI.

In the BSM 9.x topology, the layer of monitor CIs has been removed, and KPIs are now assigned directly to the monitored CIs.

For example, to monitor CPU load on a computer, the relevant KPI is assigned to the computer CI itself.

Note: SiteScope and EMS monitor CIs were not removed in BSM 9.x. For details, see "SiteScope monitor CIs in 9.x" on page 282.

Health indicators were added and KPIs were modified

In BSM 9.x, an additional layer of information was added to the monitored CIs: **health indicators** (HIs).

- ▶ HIs provide fine-grained monitoring of CIs, with far more detail than KPIs. Some HIs provides business metrics, while others monitor aspects of performance and availability. For example, a Windows CI type includes the following HIs: CPU load, memory utilization, and disk space, as well as other HIs that reflect the status of other Windows metrics.
- ▶ KPIs are now higher level indicators than HIs, and they represent a more general aspect of domain health, such as System Performance, System Availability, Application Performance, Application Availability, and so on.

KPIs apply calculation rules to the data provided by HIs to determine CI status; A KPI can be calculated using data from HIs, from other KPIs, or a combination of these.

For an overview of HIs and KPIs in Service Health 9.x, see "Health Indicators, KPIs, and KPI Domains" in *Using Service Health*.

The HI layer of monitoring is associated with a number of areas in Service Health 9.x:

Area in Service Health	Description
Health Indicators component	The Health Indicators component shows HI details for each CI. For details, see "Health Indicator Component Overview" in <i>Using Service Health</i> .
HI assignment mechanism	The HI Assignment mechanism automatically assigns HIs to CIs based on their CI types. For details, see "Indicator Assignments and Propagation" in <i>Using Service Health</i> .

Area in Service Health	Description
HI definitions on CI instances	HI definitions can be modified on individual CI instances using the Service Health Admin > CI Indicators tab. For details, see "Configuring KPIs and Health Indicators" in <i>Using Service Health</i> .
Indicator repository	The Indicator repository contains template definitions for HIs; for details see "Indicator Repository" in <i>Using Service Health</i> .

Additional changes in Service Health 9.x

The following table lists additional changes in Service Health 9.x:

BAC 8.x	BSM 9.x
Console tab	Renamed to Hierarchy
Filters tab	Embedded in the Hierarchy component
360° page with multiple tabs	360° page with Hierarchy component only, with the ability to open other components using CI detail links.
Dashboard Administration > KPIs tab	Renamed to CI Indicators (in Service Health Administration)
Context menus and context menu items in two repositories	Combined into the context menu repository
Business rules and tooltips in two repositories	Tooltips are embedded in the business rules repository
Alerts are administered in a separate application	Alerts are administered within Service Health Administration

XML adapter is deprecated

In BSM 9.x, the XML adapter mechanism is no longer available, and is not supported. If you need to import topology from an external source (XML file), contact HP Support.

Limitation in Custom Image

If you configured 8.x in breakdown mode, and you have a custom image which contains breakdown CIs, in BSM 9.1x these CIs will no longer appear in the custom image for this view.

Changes in MyBSM 9.x

In BAC 8.x, My BSM enabled users to build pages with portlets, in the context of modules. In BSM 9.x, pages are built using **components** that interact with one another.

MyBSM 9.x contains default pages from different applications, and also enables you to create custom pages and to combine different BSM applications and reports to suit your needs. For details, see *Using MyBSM*.

Custom Rules

- **Custom Java rules.** If you created custom Java rules and compiled them to create a new .jar file in pre-9.0 versions of BAC (now BSM), contact HP Professional Services for instructions on modifying and packaging them for BSM 9.x **before** upgrading.

Note that this does not relate to custom rules in the repositories; it is only relevant if you have custom java rule source files.

Note: To compile and build custom .jars, you must have JDK (Java Development Kit) 6 installed. This can be downloaded from <http://www.oracle.com>.

- ▶ **Custom classpath for calculation rules infrastructure setting.** If you created custom rule .jar files and used the **Custom classpath for calculation rules** infrastructure setting to define them in pre-9.0 BAC, contact HP Professional Services for assistance **before** you upgrade.
- ▶ **Text file-based API Rules.** If you created text file-based custom rules using the Rules API, and saved your rules in <**Data Processing Server root directory**>\BLE\rules\groovy\rules\, copy your rules to the same location in your 9.x environment, **before** upgrading.

In addition, edit the text files as follows:

- ▶ Replace lines starting with
import com.mercury.am.platform.processing.ble.calculation with
import com.hp.bsm.platform.ble.calculation.
- ▶ Replace lines starting with
import com.mercury.am.platform.processing.ble.rulesfwk with
import com.hp.am.platform.processing.ble.rulesfwk.
- ▶ Replace lines starting with
import com.mercury.am.platform.processing.ble.groovy.rulefwk with
import com.hp.am.platform.processing.ble.groovy.rulefwk.
- ▶ Replace usage of **RuleTrinityModelAccess** with **RuleBLEModelAccess**.

KPI Upgrade

If your monitored environment contains default KPIs which have not been modified prior to upgrade, they are replaced by the corresponding KPIs and HIs, as defined by the Service Health 9.x pre-defined assignments.

If you modified any KPIs in your pre-upgrade environment, the upgrade handles these KPIs as described in the following section.

This section includes the following topics:

- ▶ "Monitor CIs removed and health indicators added" on page 263
- ▶ "Domain-specific KPIs removed" on page 263
- ▶ "OMi KPIs and rules removed or replaced" on page 264

- "EUM Business rules replaced" on page 264
- "KPIs and HIs on CIs monitored by SiteScope and EMS" on page 265
- "Changes to the SiteScope System KPI" on page 266
- "Custom KPIs in the repositories" on page 266
- "Manual KPI upgrade limitations" on page 267
- "DNode CIs and their created CIs" on page 268
- "EMS Ticketing Integration following upgrade" on page 268

Monitor CIs removed and health indicators added

The two major changes related to KPIs in Service Health 9.x are **monitor removal**, and the addition of **health indicators**.

- As a result of monitor removal, if a customized KPI was assigned to a monitor CI, the upgrade moves this KPI up one level in the hierarchy to the monitored CI (because the monitor CI is removed).
- In addition, a health indicator is assigned to the monitored CI; the status and value of the KPI are calculated based on this HI.
- If you have customized a KPI on a non-monitor CI, the customization is still in effect following upgrade, within the limitations described below.

Note: SiteScope monitors are not removed; for details see "KPIs and HIs on CIs monitored by SiteScope and EMS" on page 265.

Domain-specific KPIs removed

Due to the reorganization of Service Health content that was done in BSM 9.x, the following KPIs are removed (KPI ID appears in parentheses):

User (0), Customer (2), HP System (12), Component Availability (53), Bandwidth (54), and Latency (1077).

These domain-specific KPIs have been replaced with more general KPIs.

OMi KPIs and rules removed or replaced

The following OMi KPIs and rules are removed or replaced following upgrade (IDs appear in parentheses):

BAC 8.x	BSM 9.x
<ul style="list-style-type: none"> ➤ Operations Performance KPI (10002) ➤ Operations Availability KPI (10003) 	These KPIs are removed.
<ul style="list-style-type: none"> ➤ Unresolved Events KPI (10004) ➤ Unassigned Events KPI (10005) 	These KPIs are removed if they were assigned to leaf (monitor) CIs in 8.x.
<ul style="list-style-type: none"> ➤ OprSampleRule (10000) ➤ OprSampleRule (unresolved) (10004) ➤ OprSampleRule (unassigned) (10005) 	The KPIs which used these calculation rules in 8.x are removed.
<ul style="list-style-type: none"> ➤ Convert OprWorstChildGroupRule (10001) ➤ Convert IncidentLifecycleGroupRule (10002) 	These rules are replaced with Worst Child Rule (1).

EUM Business rules replaced

The following EUM business rules are replaced with new rules:

Original 8.x Rule	Replacement 9.x Rule
RUM Application Session Statistics Monitor Availability Rule	Real User Application Sessions Availability
RUM Application Session Statistics Monitor Performance Rule	Real User Application Sessions Performance
RUM Application Session Statistics Monitor Volume Rule	Number of Open Sessions
RUM End User Monitor Availability Rule	Real User Application Sessions Availability
RUM End User Monitor Performance Rule	Real User Application Sessions Performance
RUM End User Monitor Volume Rule	End User Subgroup Open Sessions Rule
RUM End User Session Statistics Monitor Availability Rule	Real User Application Sessions Availability

Original 8.x Rule	Replacement 9.x Rule
RUM End User Session Statistics Monitor Performance Rule	Real User Application Sessions Performance
RUM End User Session Statistics Monitor Volume Rule	Number of Open Sessions
RUM Event Monitor Volume Rule	Sum of Volume
RUM Location Session Statistics Monitor Availability Rule	Real User Application Sessions Availability
RUM Location Session Statistics Monitor Performance Rule	Real User Application Sessions Performance
RUM Location Session Statistics Monitor Volume Rule	Number of Open Sessions
RUM Page Monitor Availability Rule	Real User Transaction Availability
RUM Page Monitor Volume Rule	Real User Number of Transaction Hits
RUM Session Monitor Availability Rule	Real User Application Sessions Availability
RUM Session Monitor Performance Rule	Real User Application Sessions Performance
RUM Session Monitor Volume Rule	Number of Open Sessions
RUM Transaction Monitor Availability Rule	Real User Transaction Availability
RUM Transaction Monitor Performance Rule	Real User Transaction Performance
RUM Transaction Monitor Volume Rule	Real User Number of Transaction Hits
Transaction Availability Rule	Synthetic User Transaction Availability
Transaction Performance Rule	Synthetic User Transaction Performance

KPIs and HIs on CIs monitored by SiteScope and EMS

Unlike other CIs monitored by Service Health, SiteScope and EMS monitor CIs are not removed in BSM 9.x. If a customized KPI is assigned to a SiteScope or EMS monitor CI, an HI is added to the monitor CI, and the KPI is calculated based on this HI.

On CIs monitored by SiteScope, the System Availability KPI is replaced with the Legacy System KPI.

Changes to the SiteScope System KPI

On CIs monitored by SiteScope, the pre-upgrade System KPI is replaced by the Legacy System KPI. If you have collected KPI data over time for this KPI, and you want this data displayed in post-upgrade KPI data over time report and in alerts, perform the following:

Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

- ▶ Select **Foundations > Vertical**.
- ▶ Select **SiteScope**.
- ▶ Locate the SiteScope reports section, and change the **Show Legacy System KPI in reports** to **true**.

Note: Following this procedure, the Legacy System KPI appears on all CIs.

Custom KPIs in the repositories

If you have created a KPI in the pre-upgrade KPI repository, the KPI is copied automatically to the post-upgrade KPI repository. If this KPI was assigned to a monitor CI, the upgrade process adds an HI template to the Indicator Repository.

The HI's name has the format **<KPI name>_Upgraded**. The HI copies its selector and rule from the original KPI, and uses default HI states and icons.

Note: The HI uses the same calculation rule as the original KPI, unless the rule has been replaced.

If a user-defined KPI is assigned to two CITs which have a parent-child relationship (for example Computer and Host), HI types are created in the Indicator Repository for each of the post-upgrade CITs. You should review these HIs and decide if they should be merged into a single HI on the parent CIT, which will then be inherited by its child CITs.

Manual KPI upgrade limitations

The upgrade of manual (customized) KPIs has the following limitations:

BAC 8.x	BSM 9.x limitation
EUM adapter configured to monitor transactions by location	<p>Customized KPIs on the transaction by location monitor CI are no longer supported. For example, if you are monitoring a business transaction from New York, this CI is no longer modeled the same way in BSM 9.x. The CIs are assigned KPIs and HIs using the Service Health 9.x assignment and propagation mechanism.</p> <p>For details on how to set up transaction by location monitoring in Service Health 9.x, refer to "Breakdowns" in <i>Using Service Health</i>.</p>
<p>Manual KPIs on the following CI types (and their descendant CITs):</p> <ul style="list-style-type: none"> ▶ RUM Errors ▶ RUM Information Events ▶ RUM Servers ▶ RUM Event Monitor ▶ RUM Server Monitor 	<p>In the BSM 9.x topology, a number of CITs were removed. As a result, these KPIs are not upgraded.</p>
If you created a KPI calculation rule using the Rules API (Groovy script)	Verify that the rule is still valid for the post-upgrade KPI and CI. In some cases you may need to modify the script to match your post-upgrade environment.
If you created a KPI calculation rule using the Rules API on a monitor CI	The rule script is transferred to the HI on the monitored CI; verify that the rule is still valid for your post-upgrade CI.
If a KPI on a monitor CI is calculated using a sibling rule (based on the values of sibling KPIs)	Verify that the sibling KPIs exist on the post-upgrade monitored CI.

DNode CIs and their created CIs

When you upgrade to BSM 9.x, DNode CIs and their created CIs are not removed; however the DNodes no longer function as node factories. Contact HP Support for instructions on aligning DNode CIs and their created CIs with 9.x concepts (health indicators added, and monitor CIs removed). Note that you may also need to create valid HI and KPI assignments on these CIs.

EMS Ticketing Integration following upgrade

Problem: Following upgrade, the Service Health Number of Open Incidents KPI does not return to its pre-upgrade status and value.

Workaround: Within System Availability Management Administration, manually synchronize the SiteScope HP Service Center monitor with HP Service Manager.

CI Status Alerts Upgrade

Service Health CI status alerts are upgraded as follows:

BAC 8.x	BSM 9.x
An alert was defined on a CIT	<ul style="list-style-type: none"> ▶ If an alert was defined on a CI type which was renamed in 9.x (for example Host > Node), the alert stays on the renamed CIT. ▶ In the BSM 9.x topology, a number of CITs were removed. As a result, alerts on the following CI types (and their descendant CITs) are not upgraded: RUM Errors, RUM Information Events, RUM Servers, RUM Event Monitor, and RUM Server Monitor.
An alert was defined on a monitor CI	The alert is moved to the monitored CI; it is based on the same KPIs as the original alert, which are moved to the monitored CI.

BAC 8.x	BSM 9.x
<p>An alert was defined on a CI</p>	<p>If an alert is defined on a CI in a view which is upgraded to a local impact view, the alert is visible in global views that contain this CI, but it is not displayed in the local impact view.</p> <p>Within a local impact view, alert administration and the alert report are only relevant for alerts defined within the context of the view.</p> <p>Note: A view is upgraded to a local impact view when:</p> <ul style="list-style-type: none"> ▶ The BPM adapter was in breakdown mode. ▶ The view was perspective-based, and used one of the following perspectives: Location Based Monitors Perspective, End User Monitors Perspective, All Monitors Perspective. ▶ The view results contain BPM CIs that had a breakdown topology in the source system (for example BP_GROUP, BP_STEP).
<p>An alert was triggered by a KPI</p>	<p>If an alert was generated by a KPI which no longer exists, the alert will exist after upgrade, but it will not be based on any KPIs.</p>
<p>An alert was triggered by All KPIs</p>	<p>No change following upgrade; if such an alert is defined on a removed monitor CI, it is moved to the parent CI.</p>
<p>EUM adapter was configured to monitor transactions by location</p>	<p>Alerts on the transaction by location monitor CI are removed, because transaction by location is no longer modeled in BSM 9.x.</p>
<p>An alert was defined on a CI based on the SiteScope System KPI</p>	<p>On CIs monitored by SiteScope, the System KPI is replaced by one or more of the following KPIs: System, System Availability, System Performance, Software Availability, Software Performance, Network Performance. A monitor that had the System KPI in 8.x can potentially have any or all of these KPIs in 9.x.</p> <p>Following upgrade, alerts that were defined on SiteScope group or monitor CIs are not changed. However, alerts on other CIs based on the SiteScope System KPI are now based on any of the above replacement KPIs which are assigned to the CI. If any of these KPIs is added later to the CI, it will trigger the alert.</p>

SiteScope and EMS KPI Assignment Upgrade

If you created or edited SiteScope or EMS KPI assignments in Dashboard administration, they are upgraded within Service Health 9.x.

The following KPI assignments are **not** upgraded, and are overwritten by pre-defined BSM 9.x KPIs due to changes in the KPI assignment logic:

- SLM assignments.
- Default Dashboard assignments that have not been modified.
- Dashboard assignments other than SiteScope and EMS.

Each pre-upgrade KPI assignment is upgraded to two assignments: a KPI assignment, and a health indicator assignment, using the following guidelines.

Note: Context menus are copied directly from the old KPI assignments to the new ones.

This section includes the following topics:

- "On which CI types are assignments upgraded?" on page 271
- "How is the assignment condition upgraded?" on page 271
- "Which KPIs and HIs are assigned following upgrade?" on page 272
- "How is the KPI defined in the post-upgrade task?" on page 273
- "How is the HI defined in the post-upgrade task?" on page 273
- "Limitations in the assignment upgrade process" on page 274

On which CI types are assignments upgraded?

Assignments defined on the following CI types (and their descendant CITs) are upgraded:

- EMS Monitor
- SiteScope Measurement
- SiteScope Monitor
- SiteScope Profile Monitor
- SiteScope Web Service Monitor

How is the assignment condition upgraded?

The KPI assignment condition includes a CI type and property conditions which can use attributes. These are upgraded as follows:

Assignment area	Changes in BSM 9.x
CI Type	<p>In BSM 9.x, the names of many CITs were changed; for example Host is replaced with Node. CITs defined in assignment conditions are upgraded for the post-upgrade KPI and HI assignments; for example if an assignment was defined for the Host CIT, its corresponding KPI and HI assignments are defined for the Node CIT.</p> <p>Note: Assignments on the <code>sitescope_webservice_monitor</code> CIT are upgraded to the <code>diagnostics_webservice_monitor</code> CIT. As a result, the upgraded HI assignment on 9.x might become invalid due to an invalid RefProp, for example.</p>
CI Attributes	<p>In BSM 9.x, the names of certain CI attributes were changed. Assignments can contain such attribute names in the property conditions, or as referenced properties. If an assignment used CI attributes, these attributes are upgraded in the new KPI and HI assignments.</p>

Which KPIs and HIs are assigned following upgrade?

The automatic upgrade mechanism is based on the following logic:

- ▶ **KPI assignment.** The post-upgrade KPI assignment uses the same KPI as the pre-upgrade assignment.
- ▶ **HI assignment.** The HI assignment maps an HI to the original KPI, according to the relevant CIT, as described in following table.

For example, if the original assignment placed the System KPI on an EMS Monitor CI, the new HI assignment will place the System EMS Monitor HI to this CI.

Note: This mapping is defined in the file
HPBSM\dat\kes\upgrade\kes_upgrade_configuration.xml.

CI type (or its descendant CIT)	KPI to HI mapping
EMS Monitor	<ul style="list-style-type: none"> ▶ System > System EMS Monitor ▶ Number Of open Incidents > Ticketing EMS Monitor ▶ Software Performance > Software Performance EMS Monitor
SiteScope Measurement	<ul style="list-style-type: none"> ▶ System > LegacySystem ▶ Siebel > Siebel_General ▶ Tasks in error > Siebel_Tasks_in_Error ▶ Sessions > Siebel_Sessions ▶ SAP > SAP_General
SiteScope Monitor	<ul style="list-style-type: none"> ▶ System > LegacySystem
SiteScope Profile Monitor	<ul style="list-style-type: none"> ▶ SiteScope_Availability > SiteScopeHealth
SiteScope Web Service Monitor	<ul style="list-style-type: none"> ▶ (SOA) Performance > Synthetic WS Operation Performance ▶ (SOA) Availability > Synthetic WS Operation Availability

Note: If one of these CITs has an assignment with a KPI which is not on the above list, the upgrade creates an HI in the indicator repository for the CIT, using the following syntax: <Class Name>_<KPI Name>_Auto_Generated. The Class Name is the CIT that appears in the condition of the KPI assignment in 8.x.

The post-upgrade KPI assignment is based on this HI, and the HI assignment places this HI on the relevant CIT.

How is the KPI defined in the post-upgrade task?

Following upgrade, the KPI assignment includes a task, which defines configuration details for the KPI which is assigned when the condition is filled. The post-upgrade KPI configuration is defined as follows:

KPI definition	Defined as...
Business Rule	The default group rule defined in the KPI repository.
Rule Parameters	The default rule parameters in the business rule repository.
Calculated Based On	The post-upgrade KPI is calculated based on KPIs and HIs.
Related Health Indicators	The post-upgrade KPI is calculated based on the HI defined in the HI assignment, which was based on the original KPI assignment. For example, if the original assignment placed the System KPI on an EMS Monitor CI, the new KPI assignment is based on the System EMS Monitor HI.

How is the HI defined in the post-upgrade task?

The post-upgrade HI configuration uses the business rule, rule parameters, selector, and thresholds which were defined for the pre-upgrade KPI.

If the 8.x KPI assignment used referenced properties for the selector or threshold, these are upgraded in the 9.x HI configuration.

Note: The SiteScope WS Operation Performance Rule (1304) on the SiteScope Web Service Monitor CIT in 8.x, is replaced with the Synthetic WS Operation Performance Rule (1306) on the Web Service Operation CIT in 9.x. If a KPI used the original rule, the HI will use the new rule.

Limitations in the assignment upgrade process

- ▶ **SiteScope Monitored CI.** When a SiteScope KPI assignment is upgraded and it assigns HIs and KPIs to a monitor CI, the KPI does **not** propagate from the monitor CI to the parent (monitored) CI. The KPI **does** propagate to the SiteScope group related to the monitor CI.
- ▶ **Stopped Default Assignments.** If you have stopped a default assignment in 8.x, it is not upgraded in 9.x.
- ▶ **Identical Conditions.** If a new default assignment has the same condition as an upgraded custom assignment, the new assignment is stopped, and the upgraded assignment is active.
- ▶ **Default Objectives.** Within the objective area of a KPI assignment in 8.x, you could use the default setting for some parts of the objective (thresholds or operator) and custom values for other parts, within a single KPI.

In BSM 9.x assignments, the thresholds and operator for an HI must be defined either as all default, or all custom. If your 8.x assignment had some KPI thresholds or operator as default and some as custom for a specific KPI, the post-upgrade 9.x HI assignment is invalid. You can edit the assignment and modify the HI objective as needed.

- ▶ **Applicable CITs for Rules.** In 9.x, a list of applicable CI types was added to each of the calculation rules. As a result, an assignment that was valid in 8.x may become invalid in 9.x, if it uses a rule and CI type that do not match.

To fix this, open **Admin > Service Health > Repositories > Business Rules** and edit the relevant rule to be applicable to the CI type, or change the assignment to use a different (applicable) rule.

- **SOA Assignments.** If you have customized an assignment on the `sitescope_webservice_monitor` CIT, this assignment is upgraded to the `diagnostics_webservice_monitor` CIT. As a result, the upgraded HI assignment on 9.x might become invalid due to an invalid RefProp, for example.

SiteScope KPI Assignments Associated With Custom KPIs

If you created a KPI in BAC 8.x or earlier using the **Clone** option in the Dashboard KPI repository (KPI ID 2000 and higher), KPI assignments using this KPI are upgraded. However, since there is no impact from SiteScope monitors to CIs in 9.x, the assignments will not create an impact as they used to. The following section describes two options for handling this within Service Health 9.x.

Note: The following section is also applicable if you used any non-SiteScope KPIs in KPI assignments for SiteScope Monitors.

Use default HIs to calculate the custom KPI

Within the KPI Assignments tab, you can create a KPI assignment which uses default HIs to calculate your custom KPI. The relevant CIs will then have your custom KPI assigned, calculated by the values of default HIs.

Use custom HIs to calculate the custom KPI

- 1 If you have an assignment with a custom KPI, the upgrade creates an HI in the indicator repository, for the CIT defined in the assignment condition, using the syntax `<CIT>_<KPI Name>_Auto_Generated`.

You can use this HI to calculate your KPI, or you can create a new HI in the indicator repository.

- 2 Map the relevant monitor metrics to the custom HI.

Access **Admin > System Availability Management**, and select the **Metrics and Indicators** tab. Manually map the metrics from the monitor to the required indicators on the CI, by selecting the appropriate CIT and the indicators that you want to associate with the monitor. For details, refer to the "Metrics and Indicators Tab" section in *Using SiteScope*.

- 3 If you created a new HI, create a KPI assignment in the KPI Assignments tab which uses this new HI to calculate your custom KPI. The relevant CIs will then have your custom KPI assigned, calculated by the values of your custom HIs.

Propagation Rule Upgrade

The upgrade of propagation rules automatically deals with BDM changes, meaning that CI types which changed from 8.x to 9.x (for example `it_world > configuration_item`) are updated within the propagation rule definitions.

After upgrade, a propagation rule which contains any of the following is not valid:

- A CI type that does not exist.
- A calculation rule that no longer exists.
- A KPI that no longer exists.

Within the Propagation Rules tab, if a propagation rule is invalid after upgrade because its CIT no longer exists, you can create a new rule or clone the rule to replace the invalid one, and delete the invalid rule.

If a propagation rule is invalid because it contains a calculation rule or KPI that no longer exists, you can edit the invalid propagation rule and fix the problem.

Repositories Upgrade

There are a number of areas in the repositories which are effected by the upgrade process, as described in the following section.

This section includes the following topics:

- "Tooltips appended to calculation rules" on page 277
- "Rule class names and rule parameters have been updated" on page 277
- "Applicable CI types defined for calculation rules" on page 278
- "BPI calculation rule IDs are modified" on page 278

Tooltips appended to calculation rules

In previous releases, the tooltip repository in Service Health Administration contained definitions for the tooltip associated with each calculation rule. In BSM 9.x, tooltip definitions are contained within the rule definitions, and each rule template in the business rule repository contains its tooltip definitions. The upgrade attaches the tooltip definition to the rule definition in the rule repository.

If you created a rule and deleted its tooltip definition prior to upgrade, the rule has empty tooltip definitions following the upgrade.

Rule class names and rule parameters have been updated

Each calculation rule belongs to a particular Java class; some of these rule classes were renamed in BSM 9.x. The upgrade renames a number of rule classes, as listed in the following file:

conf\upgraders\9.0.0.0\DPS\ruleClassUpgrade.properties.

Note that this is only done for rules that are not out-of-the-box rules.

In addition, a number of rules were given additional rule parameters in BSM 9.x. For example, rules which calculate KPIs now have rule parameters which define how they are calculated (either based on other KPIs, on HIs, or some combination of these), and which HIs are used in their calculation. The upgrade adds these rule parameters to the relevant rules in the rule repository.

Applicable CI types defined for calculation rules

Within the business rule repository, the upgrade verifies that all calculation rules have at least one applicable CIT. If no applicable CIT is defined for a rule, the upgrade sets the rule to be applicable for the (highest level) **Configuration Item** CIT, so that it can then be applied on all CITs.

BPI calculation rule IDs are modified

Following upgrade, the rule IDs of BPI calculation rules in the business rule repository change from 2000-2010, to 3000-3010. For example, the ID of the BPI Average Duration rule changes from 2000 to 3000; the ID of the BPI Minimum Duration rule changes from 2001 to 3001, and so on.

If you have upgraded from BSM 9.0 to 9.1x, after reloading the repositories (as described in the release notes), perform the following:

- 1 Open the KPI and HI assignment pages, and synch the BPI assignments. This updates the rule IDs on the HIs which use these rules.
- 2 If you have edited an HI using one of these rules, open the HI for editing on the CI Indicators page and select the rule with the updated rule ID.

View Upgrade and Monitor Removal

The upgrade removes monitor CIs from your view definitions, and adds the **monitored_by** attribute to their parent CIs (for example, monitored by RUM or BPM).

View upgrade and monitor removal are done using the settings described in the following sections. You can modify these settings using the file `conf\views_upgrade\bsm_views_upgrade_configuration.properties`.

This section includes the following topics:

- "Links defining monitor CITs for removal" on page 279
- "Removed monitor CITs and their corresponding monitored_by attribute" on page 279
- "Monitor CIs which are not removed" on page 280

- "Views which are not upgraded" on page 280
- "SiteScope monitor CIs in 9.x" on page 282

Links defining monitor CITs for removal

The BSM upgrade process removes monitor CIs that fill the following conditions:

- **monitored_by** (and its descendant links)
- **impact_link** (and its descendant links)

If a monitor CI is attached using a compound link, it is not removed.

Removed monitor CITs and their corresponding monitored_by attribute

The following is a list of monitor CITs which are removed (if their link is monitor_by or Impacted By), and their corresponding **monitored_by** attribute.

For example, if a **bpi_monitor** CI is removed, its parent CI is assigned a monitored_by attribute of **BPI**.

- BPI Monitor > BPI
- BPI Business Process Monitor > BPI
- BPI Business Process Step Monitor > BPI
- BPM Transaction From Location > BPM
- BPM Transaction Monitor > BPM
- BPM Web Service Monitor > BPM
- Diagnostics Probe > Diagnostics
- Diagnostics Web Service Monitor > Diagnostics
- EUM Monitor > BPM,RUM
- OPR Monitor > OM
- RUM Sessions Monitor > RUM
- RUM Event Monitor > RUM

- ▶ RUM Location Monitor > RUM
- ▶ RUM Page Monitor > RUM
- ▶ RUM Server Monitor > RUM
- ▶ RUM Trans Monitor > RUM
- ▶ RUM Transactions Monitor > RUM
- ▶ SiteScope Measurement > SiteScope
- ▶ SiteScope Monitor > SiteScope
- ▶ SiteScope Profile Monitor > SiteScope
- ▶ SOA Monitor > Diagnostics, BPM
- ▶ System Monitor > SiteScope, EMS
- ▶ TV Monitor > TV

Monitor CIs which are not removed

If a monitor CI has more than one parent CI, it is not removed.

The following CITs are not removed:

- ▶ Dynamic Node Monitor
- ▶ EMS Measurement
- ▶ EMS Monitor
- ▶ SAP Alert Monitor
- ▶ SiteScope Measurement
- ▶ SiteScope Monitor
- ▶ SiteScope Profile Monitor

Views which are not upgraded

Only pattern-based and perspective based views are upgraded; template-based views are not upgraded.

If a view contains a subgraph, the subgraph is not upgraded.

Note: We recommend that you review the view definitions that contain monitor CIs or CI types, and replace them with the relevant parent CI type (for example Oracle, Windows, and so on).

In addition, the following views are not upgraded:

- AD_Logical_View
- AD_Physical_View
- CPU_Infrastructure
- End User MonitorsAdmin
- EndUserLocations
- EndUserMonitors
- Exchange_Mail_View
- Exchange_Org_View
- Exchange_Site_View
- Filesystem_Infrastructure
- HACluster_Infrastructure
- Infrastructure_Common
- J2EE_Deployment
- MSSQL_Deployment
- NetworkInterface_Infrastructure
- ORA_Deployment
- RealUserApplications
- RealUserEndUsers
- RealUserLocations
- RealUserMonitors
- RealUserServers

- ▶ Systems_Infrastructure
- ▶ Virtualization_Infrastructure
- ▶ vMA_Infrastructure

SiteScope monitor CIs in 9.x

- ▶ SiteScope monitor CIs have been removed from the **System Hardware Monitoring** and **System Software Monitoring** views. In addition, these views now show CIs monitored by all domains and not only by SiteScope.
- ▶ Monitors have also been removed from the **System Monitors Only** perspective. Any custom views which were build using this perspective will no longer include monitors; they will only show CIs monitored by SiteScope.
- ▶ Monitors are not removed from custom patterns views (views created by users). Since there is no direct impact between monitors and monitored CIs in BSM 9.x, you can remove the monitors from the views themselves. If you do not use monitor CIs for drill downs, Go to Report, or other options, we recommend removing them from the custom views.

SiteScope Monitors Associated with Non-default CIs or Multiple CIs

If you have manually associated SiteScope monitors to CIs of non-default CIT, or multiple CIs in earlier versions of BAC, the upgrade to BSM 9.x may result in two types of configuration issues. This can occur if you created relationships from CIs to monitors either using the Link Monitor to CI option in SiteScope, using UCMDB Administration in BAC, or using the Monitor Deployment Wizard (MDW).

Since SiteScope is not aware of these relationships, the CIs will not have the correct health indicators defined. In addition, a monitor may be connected to more than one CI following manual creation of relationships, and this cannot be handled properly by the CI Resolution process. For details on CI Resolution, refer to "Advanced Event Automation" in *Using Operations Management*.

Two new views have been created in RTSM to help you identify and resolve these problems.

This section includes the following topics:

- "SiteScope Monitors Connected to Multiple CIs" on page 283
- "SiteScope Monitors with Missing Health Indicators" on page 285

SiteScope Monitors Connected to Multiple CIs

In BSM 9.x, each SiteScope monitor can only be associated with a single CI instance. However, you may have manually associated a monitor with more than one CI before upgrading to BSM 9.x. For example, a CPU monitor may be associated by default with a Computer, and manually with a Running Software.

To see if you have any monitors associated with more than one CI, open **RTSM Administration > IT Universe Manager**, and drill down to **Monitors > SiteScope > SiteScope Monitors Connected to Multiple CIs**. If you have monitors associated with multiple CIs, the **SiteScope Monitors Connected to Multiple CIs** view contains these monitors, and their associated CIs. To enable BSM to receive data from a monitor for a CI, you must associate the monitor with a single CI only. The procedure you must follow depends on which CI you want the monitor to link to, as follows:

To create a relationship from a monitor to its default CI:

- 1 Within RTSM, delete the relationships between the monitor and the non-default CIs.
- 2 Within SiteScope, access the monitor's properties page.
 - For SiteScope 10.x, within the **HP BAC Integration Settings** panel, verify that **Include topology data when reporting to BAC** is selected.
 - For SiteScope 11.x, within the **HP Integration Settings** panel, verify that **Report Monitor and Related CI Topology** is selected, and CI Type is not **None**.

To create a relationship from a monitor to a non-default CI:

- 1** Within RTSM, delete the relationships between the monitor and all CIs except the preferred non-default CI.
- 2** Within SiteScope, access the monitor's properties page. In SiteScope 11.x, within the **HP Integration Settings** panel, select the **Report Monitor and Related CI Topology** option. Select the CI type for the monitor, and enter values for the CI type key attributes (they depend on the CI type selected).

This enables you to associate the monitor with a non-default CI, rather than with its default CI.

- 3** To enable BSM to receive health indicator data from a monitor after associating it with a CI of a non-default CIT, perform the following:

If necessary, create new health indicators for the non-default CIT within the Indicator Repository.

Map the indicators that you want to associate with the monitor, to the monitor metrics. This step depends on your version of SiteScope:

- For SiteScope 10.x, access **Admin > System Availability Management**, and select the **Metrics and Indicators** tab. Manually map the metrics from the monitor to the required indicators on the CI, by selecting the appropriate CIT and the indicators that you want to associate with the monitor. For details, refer to the "Metrics and Indicators Tab" section in *Using SiteScope*.
- For SiteScope 11.x, within the monitor's properties page in SiteScope, within the **HP Integration Settings** panel, check the **Report monitor and related CI topology** checkbox. In the **CI Type** dropdown select the relevant CI type, and fill in the details of the CI to which the monitor is linked. In the same panel, under **Indicator Settings**, map metrics of the monitor to the relevant indicators for the CI.

SiteScope Monitors with Missing Health Indicators

In BSM 9.x, each CI type has a default set of health indicators defined in the Indicator Repository, which represents what is monitored on CIs of that CI type. If you have manually associated a monitor with a CI of a non-default CIT, you may need to configure the mappings between the metrics of the monitor, and the indicators.

For example, if you have manually associated a CPU monitor with a Running Software CI (and not with a Computer CI), the Running Software CIT will not have the CPU-related indicators defined, and the Running Software CI will therefore not show CPU data.

There is no automatic way of finding the above associations in BSM. However, such CIs would usually have only the Legacy System HI assigned. In the above example, the Running Software CI will have only the Legacy System HI assigned, but not the CPU Load HI, since CPU Load is defined on the Computer CIT. This is different than a Computer CI associated with another CPU monitor, which would have both HIs assigned.

To enable BSM to receive health indicator data from a monitor after associating it with a CI of a non-default CIT

- 1 If necessary, create new health indicators for the non-default CIT within the Indicator Repository.
- 2 Map the indicators that you want to associate with the monitor, to the monitor metrics. This step depends on your version of SiteScope:
 - For SiteScope 10.x, access **Admin > System Availability Management**, and select the **Metrics and Indicators** tab. Manually map the metrics from the monitor to the required indicators on the CI, by selecting the appropriate CIT and the indicators that you want to associate with the monitor. For details, refer to the "Metrics and Indicators Tab" section in *Using SiteScope*.
 - For SiteScope 11.x, within the monitor's properties page in SiteScope, within the **HP Integration Settings** panel, check the **Report monitor and related CI topology** checkbox. In the **CI Type** dropdown select the relevant CI type, and fill in the details of the CI to which the monitor is linked. In the same panel, under **Indicator Settings**, map metrics of the monitor to the relevant indicators for the CI.

My BSM Upgrade

The MyBSM Legacy page enables users who created pages in My BSM before upgrade, to view these pages in BSM 9.x. You can use the MyBSM Legacy page to view pre-upgrade portlets in read-only mode. For details, see "MyBSM Legacy Page" in *Using MyBSM*.

Note: The MyBSM Legacy page will not be supported in future major releases. Define new pages using the 9.x MyBSM workspace.

The following portlets have been changed or removed:

- ▶ The CMDB portlets are deprecated in BSM 9.x. The UCMDB module and pages are visible, but they do not contain data.
- ▶ The Dashboard Scorecard and Status Snapshot portlets are deprecated in BSM 9.x.
- ▶ The Problem Isolation portlets are deprecated in BSM 9.x.
- ▶ The Filters portlet is now included as part of the Service Health Hierarchy component.
- ▶ The Welcome page is the same as it was in BAC 8.x, and includes deprecated information.

Limitation:

If you created a reports portlet in 8.x and used the default report filter, the filter is not upgraded in the MyBSM Legacy page.

20

Alerts Upgrade Information

In BSM 9.1x, the alert applications have been moved to their own domains: CI Status Alerts to Service Health (formerly Dashboard), SLA Alerts to the Service Level Management application, and EUM alerts (formerly event-based alerts) to the End User Management application.

To define CI Status alerts in version 9.x, see "How to Create a CI Status Alert Scheme and Attach it to a CI" in the *Using Service Health* PDF.

To define your EUM alerts in version 9.x, see "How to Create EUM Alert Schemes" in the *Using End User Management* PDF.

To define SLA alerts in version 9.x, see "How to Define an SLA Alert Scheme" in the *Using Service Level Management* PDF.

This chapter includes:

- ▶ Infrastructure Settings on page 288
- ▶ General Information on page 290
- ▶ CI-Based Alerts on page 290
- ▶ Notification Template Upgrade on page 290
- ▶ Alert Permissions Upgrade on page 291
- ▶ Event-Based Alerts on page 291
- ▶ CI Status and SLA Alerts Upgrade on page 306
- ▶ Upgrade of Downtime for Alerts on page 308

Infrastructure Settings

This section describes upgrade limitations for alert infrastructure settings.

This section includes:

- ▶ "Setting Substitution for Quote in Command Line Parameters" on page 288
- ▶ "Parameters in Default Exe and Default URL Infrastructure Settings" on page 288

Setting Substitution for Quote in Command Line Parameters

The setting **Substitution for quote in command line parameters** under **Foundations - alerting** that was available in version 8.06 is no longer available in version 9.1x. If the value of the parameter was customized in version 8.06, that change will not be available after upgrade. To set it manually after the upgrade, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

- ▶ Select **Foundation**.
- ▶ Select **Alerting**.
- ▶ In the **Foundation - Alerting** table, locate and update the **Command line substitution pairs**.

Parameters in Default Exe and Default URL Infrastructure Settings

Parameters used in the **Default Exe path** and **Default URL** infrastructure settings for alerts triggering defaults in version 8.07, are not upgraded to the new parameters for version 9.1x. To set them manually after the upgrade, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

- ▶ Select **Foundation**.
- ▶ Select **Alerting**.

- In the **Alerting - Triggered alerts** table, locate the **Default Exe path** and **Default URL** settings and update the parameters according to the following table:

BAC 8.07 Parameters	BSM 9.1x Parameters
Profile Name	Entity Name
SubAlerts	Alert XML
Id	Alert ID
Page Name	Transaction Name
User Message	Alert User Description
Group Name	N/A in BSM 9.1x

General Information

Alert samples were changed. For details about the upgrade of the Custom Query Builder, see "Custom Query Builder Upgrade" on page 193.

CI-Based Alerts

CI-based alerts that were defined on End User Management Administration CIs in the old model (in BAC 8.x) are upgraded to be defined on the new corresponding CIs (in BSM 9.1x). For example, an alert defined for a specific Business Process Group is upgraded to be defined on the corresponding business transaction flow.

Notification Template Upgrade

The names of some of the parameters that can be included in a notification template have been changed in BSM 9.1x.

Topics	BAC 8.x	BSM 9.1x
Profile Name (changed - automatically upgraded)	Profile Name	Entity Name
User Message (changed - automatically upgraded)	User Message	Alert User Description
HP BAC URL (changed - automatically upgraded)	HP BAC URL	HP BSM URL
Entity Type attribute was added		
Group Name removed from the Transaction's parameters list		

Alert Permissions Upgrade

The permissions mechanism used for alert users was changed in BSM 9.1x.

- **Alerts - Create dependencies** permissions resource was moved from the **Monitors** context to the **End User Management** context.
- **Alert - Event template** permissions resource was added to the **End User Management** context.
- **Send SNMP trap** permissions resources were moved from the **Monitors** context to the **Platform** context.
- **Run executable file** permissions resources were moved from the **Monitors** context to the **Platform** context.
- **Log to event Viewer** permissions resource was moved from the **Monitors** context to the **Platform** context.

Event-Based Alerts

The table describes the changes that occurred between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles these changes.

Topics	BAC 8.x	BSM 9.x
Event-Based alerts (name was changed)	Event-Based alerts	EUM alerts
Location of the event-based alerts applications	In the Alerts application	In the End User Management application

Topics	BAC 8.x	BSM 9.x
Action parameters (names have changed - automatically upgraded)	Profile Name	Entity Name
	SubAlerts	Alert XML
	Id	Alert ID
	Page Name	Transaction Name
	User Message	Alert User Description
	Group Name	N/A is written in place of the Group Name field. The Group Name parameter used by actions defined for BAC alerts in BAC 8.x is discarded by the upgrade.
Group-by option field names (names have changed - automatically upgraded)		
SNMP trap structure		The SNMP trap structure has changed. For details, see "SNMP Trap Structure Changes" on page 293.
RUM Alert dependencies (automatically upgraded)	RUM alerts assigned to RUM profiles with dependencies.	If the alerts themselves are duplicated as part of the upgrade process, the dependencies are also duplicated. This occurs for each of the applications that were running on the RUM engine.
BPM Alert dependencies	BPM alerts assigned to BPM profiles with dependencies.	These dependencies are automatically upgraded.

SNMP Trap Structure Changes

The following table describes the changes to the SNMP trap structure between BAC 8.x and BSM 9.x.

OID (starts with 1.3.6.1.4.1.5233.)	Variable description (BAC 8.x)	Variable description (BSM 9.x)	Example
4.9	Start of the Subalerts table. Subalerts trigger alerts (listed in Events table)	The ID of the CI related to the alert	Allow the ID of the alert related CI (Application ID in the EUM alert)
4.10	Start of the subalert instance table	The parameters specified in the Grouped By definition of the alert.	Allows Event correlation on the group by parameters between different alert triggers. Example: transaction: tx5
4.11.1.1.2-4.11.1.1.8	Various event parameters (organization, host location, script etc.)	Replaced by 4.11.1.4.1.2.[n].[m]: the actual description of the event	

BPM Alerts

The table describes the changes that occurred between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles these changes.

Topics	BAC 8.x	BSM 9.x
BPM alerts assigned to a BPM profile (automatically upgraded)	BPM alerts assigned to a BPM profile	BPM alerts are changed to BPM Transaction alerts and assigned to the Application CI that corresponds to the application that was defined for the profile.

Topics	BAC 8.x	BSM 9.x
BPM alerts grouped by groups (not supported)	BPM alerts grouped by groups	Group by group is not supported.
	Limit to <group_name> options in the Filters tab of the event-based alerts	Limit to <group_name> options are not supported. The Groupby Business Transaction Flow option was added.
Sub-alert parameters (names changed, XML file structure changed - automatically upgraded)	Sub Alerts parameters	The name of the parameter was changed to 'Alert XML'.
		The structure of the XML file was changed and now contains: <ul style="list-style-type: none"> ➤ General data about the alert (name, ID, severity). ➤ For each trigger, data about the events that triggered the alert (if such events exist). For an example of such an XML file, see "Example of an Alert XML Structure" on page 296.
SNMP structure of event-based alerts (changed - automatically performed)	SNMP structure of the event-based alerts	The SNMP trap structure of the EUM alerts was changed. <ul style="list-style-type: none"> ➤ There is only one trap type: eventAlert ➤ Some of the OIDs and names were changed ➤ Sub alerts/triggers table structure and events table structure changed For details, see "Alerts MIB Varbinds" in <i>Using End User Management</i> .

Topics	BAC 8.x	BSM 9.x
<<Trigger ID>> parameter value was changed (automatically performed)	Value is a number	Value is text
Action parameters with extensions (num, tx_resp, or tx_fail)	<p>Event-based triggers (BPM only). If more than one event triggers an alert, sequential numbers are adjusted to each trigger and event parameter.</p> <p>If more than one triggers' requirements are met, trigger types are adjusted. Trigger types were tx_resp and tx_fail for "Transactions response time" and empty for "Transactions response time relevant to EUM threshold.</p> <p>For example: <<parameter>>1, <<parameter>>1 tx_resp, <<parameter>>2, <<parameter>>2 tx_resp</p> <p>The TriggerTypeMessage parameter is added with the relevant trigger ID.</p>	<p>If more than one trigger and/or event are configured; it is recommended to use the out-of-the-box <<Alert XML>> that contains all the triggered alert information (to access it click the Action tab and select Generate Event, Run executable file, or Access URL) and insert it as an action parameter. For details about its structure see the Example on the next page.</p> <p>TO DO: To use these parameters you must enable the setting and manually upgrade the parameters.</p> <p>For details, see "Action Parameters Manual Upgrade" on page 297.</p>
When BPM adapter was configured to transaction\location mode in the previous version, after the upgrade these views are upgraded into Local Impact Views. The CI Status alerts that were defined for CIs in these views are not copied to the corresponding Local Impact Views and will not be accessible through these views.		

Example of an Alert XML Structure

```

<Alert>
  <Name>Michal</Name>
  <Id>xxx</Id>
  <Severity>Major</Severity>
  <Purpose>Regular Alert</Purpose>
  <UserMessage>N/A</UserMessage>
  <EntityName>Default Client_Snt_Ap1_1</EntityName>
  <EntityId>3fb61099e47ed1b527b48ab2cff636a2</EntityId>
  <Triggers>
    <Trigger>
      <TriggerCause>Response time for 1 out of 1 transactions greater than 0.00
seconds.</TriggerCause>
      <ActualDetails>Response time for 1 out of 1 transactions was greater than 0.00
seconds.</ActualDetails>
      <Events>
        <Event>
          <ActualDetails>Response time was 9.99 seconds.</ActualDetails>
          <Transaction>
            <BTFName />
            <BTFId>701db88f4335742ff454da2216ab4c94</BTFId>
            <Name>tx_10</Name>
            <Time>Tue Dec 14 11:24:34 AM 2010 (GMT +0200)</Time>
            <LocationName>VMAMRND12</LocationName>
            <ScriptName>tx_5_10_15</ScriptName>
            <szBpmAgentName>VMAMRND12</szBpmAgentName>
            <Description />
            <Error>N/A</Error>
            <BPMTriageReportUrl>http://machine
name:80/topaz/rfw/popupAction.do?popUp=true&filter.filters.TIME_PERIOD.timeBarBean.view=pastHo
ur&filter.filters.DATA_COLLECTOR.dataCollector=BPM&autoGenerate=true&reportID=triage_report&filt
er.filters.APPLICATION.selectedIdsInTree=0x3fb61099e47ed1b527b48ab2cff636a2&filter.filters.APPLI
CATION.fromDashboard=true</BPMTriageReportUrl>
            <BPMPerfAnalysisReportUrl>http://machine
name:80/topaz/rfw/popupAction.do?popUp=true&filter.filters.TIME_PERIOD.timeBarBean.view=pastHo
ur&filter.filters.DATA_COLLECTOR.dataCollector=BPM&autoGenerate=true&reportID=performance_su
mmmary_report&filter.filters.APPLICATION.selectedIdsInTree=0x3fb61099e47ed1b527b48ab2cff636a2&
filter.filters.APPLICATION.fromDashboard=true</BPMPerfAnalysisReportUrl>
          </Transaction>
        </Event>
      </Events>
    </Trigger>
  </Triggers>
</Alert>

```


Action Parameters Manual Upgrade

To use the action parameters extensions:

- 1 Change the value of the `settings.enable.legacy.action.parameters` setting in `<HPBAC Gateway Server>\conf\settings\alertengine.xml` to true.

Once the setting is enabled, the parameters are generated with extensions in new format.

- 2 The parameters are not automatically upgraded. Perform the upgrade manually using the tables below.

► BPM event-based triggers - once:

Old parameter	New parameter
[param] tx_resp	[param]_TransactionRespTimeOnce
[param]	[param]_TransactionRespTimeRelativeOnce
[param] tx_fail	[param]_TransactionFailOnce

► BPM event-based triggers - X out of Y:

Old parameter	New parameter
[param]1 tx_resp	[param]_1_TransactionRespTimeXy
[param]1	[param]_1_TransactionRespTimeRelativeXy
[param] tx_fail	[param]_TransactionFailXy

► Over-time BPM and RUM triggers:

Old parameter	New parameter	Description
[param]1	[param]_[trigger id]	For over-time triggers, parameter number extensions

- 3 The **TriggerTypeMessage** parameter is added with the relevant trigger ID. The parameter remains the same. Map its values according to the table Trigger IDs' mapping table.

► **Trigger IDs' mapping table:**

Alert	Trigger	Old ID	New ID
BPM Once	Transaction fail	6	TransactionFailOnce
	Transaction response time	4	TransactionRespTimeOnce
	Transaction response time relative to threshold or EUM threshold	2	TransactionRespTimeRelativeOnce
BPM X out of Y	Transaction fail	16	TransactionFailXy
	Transactions response time	14	TransactionRespTimeXy
	Transactions response time relative to threshold or EUM threshold	12	TransactionRespTimeRelativeXy
BPM Time-based	Availability	27	TransactionAvailability
	Transactions response time	23	TransactionRespTimeOverTime
	Transactions response time relative to threshold or EUM threshold	21	TransactionRespTimeRelativeOverTime
	Average transaction response time	25	TransactionAvgRespTime

Alert	Trigger	Old ID	New ID
RUM Transaction	Transaction availability	111	TransAvailability
	Transaction performance (gross)	113	GrossTransPerformance
	Transaction performance (net)	115	NetTransPerformance
	Transaction performance (server)	117	ServerTransPerformance
	Transaction volume - all	119	TransVolume
	Transaction volume - completed	121	CompletedTransVolume
RUM Server	Server application requests availability	109	RumAppRequestOverTime
	Server network connections availability	110	RumAppNetworkOverTime

RUM Page Alerts

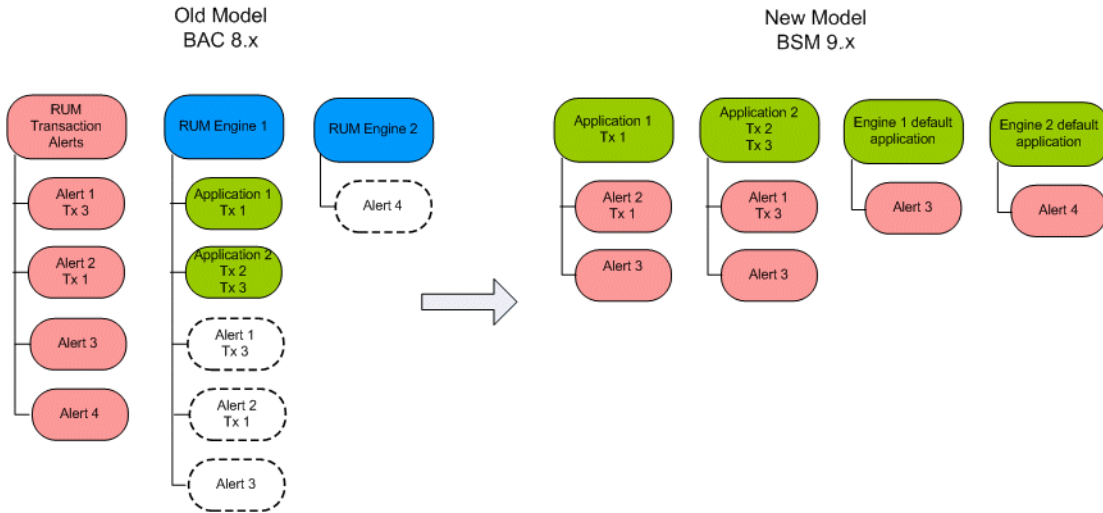
The table describes what was changed between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
RUM Page alerts (type changed - automatically upgraded)	RUM Page alerts	<p>RUM Transaction alerts. The transaction on which the alert is set is the transaction that was created (or mapped to) by the upgrade process for the specific page. For details on the page upgrade process, see "RUM Pages Upgrade" on page 363.</p> <p>Note: A RUM alert configuration at the application level that does not filter a certain transaction will receive more data (samples) that fits its filter (both the pages and transactions). This will cause a difference in the calculation result between the previous version and the new version.</p>
	The RUM Page alerts are defined for a Real User Monitor engine.	The upgrade process assigns the corresponding RUM Transaction alerts to all the RUM applications that are configured in the new model for the specific engine.

Topics	BAC 8.x	BSM 9.x
RUM page alerts (continued)	If an alert was filtered for specific pages.	The upgrade process duplicates the corresponding RUM Transaction alert only to the applications that include these pages. (This is similar to RUM Transaction Alerts. For details, refer to the graphic in "RUM Transaction Alerts" on page 302.)
Trigger criteria	Page Availability	Transaction Availability
	Page Response Time	Transaction Gross Response Time
	Page Server Response Time	Transaction Server Response Time
	Transaction Volume - All	Page
Filters and Group by parameters	Page Name	Transaction ID
	Group by page	Group by transaction
	User Message	Alert User Description
	Page names for RUM Page alerts	Transaction IDs

RUM Transaction Alerts

The following graphic shows the upgrade flow for RUM Transaction alerts defined for a Real User Monitor engine and also for alerts filtered for specific transactions:



The table describes the changes between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
RUM Transaction alerts (changes - automatically upgraded)	RUM Transaction alerts assigned to RUM profiles	Automatically upgraded to RUM Transaction alerts assigned to RUM Application CIs for each of the applications that were running on the RUM engine
	RUM Transaction alert configured with filtering by transaction	Automatically upgraded to alerts assigned to RUM Application CIs for each of the applications that were running on the RUM engine only for the applications that include those transactions

RUM Server Alerts

The table describes the changes between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

	BAC 8.x	BSM 9.x
RUM Server alerts name was changed	RUM Server alerts	RUM Application alerts
RUM Server alerts (changes - automatically upgraded)	RUM Server alerts assigned to RUM profiles	Automatically upgraded to alerts assigned to RUM Application CIs for each of the applications that were running on the specific RUM engine

EUM (Formerly Event-based) Alerts Reports and Favorite Filter Upgrade

The table describes the changes between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
Alert's model (changed - automatically upgraded)		

Topics	BAC 8.x	BSM 9.x
Filtering in reports (changed due to model change - automatically upgraded)	BPM Profile ID	Application ID
	RUM Session ID: ► Filter that was defined on the Default RUM profile .	► Filter displays a list of the applications that were monitored by the specific RUM engine and that had alerts configured for them. Note: A default RUM profile option (hidden by default) can be displayed. It shows the legacy Default RUM profile that was available by default in 8.0 and does no longer exist in 9.0 (unless you select Admin > Platform > Infrastructure Settings > Applications > End User/System Availability Management , and in the End User/System Availability Management - Data table, set the Show legacy data in alert reports option to true). The upgraded Filter might contain a legacy RUM configuration (RUM default profile). In order to be able to view it, set the Show legacy data in alert reports option to true as explained above.

Topics	BAC 8.x	BSM 9.x
Reports	Alert Log report	Alert Log report (report and filter automatically upgraded)
	Alert Count Over Time report	Alert Count Over Time report (report and filter automatically upgraded)
	Alert Count Summary report	Alert Count Summary report (report and filter automatically upgraded)
	Baseline Suggested Alerts Log report	Removed in BSM 9.1x
	Actual vs. Baseline Suggested Alerts report	Removed in BSM 9.1x
	Actual vs. Baseline Suggested Alerts - Detailed report	Removed in BSM 9.1x
Parameters in report's filters (automatically upgraded)	Profile	Configuration Item
	N/A	Recipients Default: All

Troubleshooting and Limitations

This section includes troubleshooting and limitations for the End User Management Administration upgrade of EUM Alerts.

► **Server name field is empty in RUM Server Alerts directly after the upgrade**

A RUM Server Alert is upgraded to an RUM Application Alert. If the alert was filtered by server (Host CI), the upgrade adds the filter to the new alert. If you display the alert immediately after the upgrade and before Real User Monitor has sent any samples for this server, the server name filter field is empty. This is because BSM is trying to match the server ID to all the servers that are linked to the application.

In BAC 8.x, the server CI was not linked to an application and the upgrade process does not create this link. In BSM 9.x, the Real User Monitor engine creates this link when it reports data for the server. Until such data is reported after the upgrade, the server name filter field is empty.

► **CI based alerts on RUM events are not upgraded**

Details of such alerts are logged by the upgrade process so that you can manually reconfigure them in the upgraded system.

CI Status and SLA Alerts Upgrade

The table describes the changes between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
CI Status alerts that were defined on Monitor CIs are automatically moved to monitored CIs (for example, the alert is moved from the BPM Monitor CI to the Business Transaction CI).		
CI Status alerts based on RUM events (not supported - removed during the upgrade)		
KPI identification was changed (automatically upgraded)	KPI Name	KPI Type

Topics	BAC 8.x	BSM 9.x
Action parameters (used for executable actions and for URLs) (automatically upgraded)	Trigger Time	Alert Trigger Time
	Previous Status	Previous Status Name
	Current Status	Current Status Name
	KPI Display Name	<ul style="list-style-type: none"> ▶ KPI Name (for CI Status alerts) ▶ Tracking Period (for SLA alerts)
The KPI Value parameter of CI Status Alerts is automatically upgraded to the Calculation Value parameter.		
When a BPM adapter was configured to transaction\location mode in the previous version, after the upgrade Custom views are upgraded to Local Impact Views. The CI Status alerts that were defined for CIs in these views are not copied to the corresponding Local Impact Views and will not be accessible through these views.		

CI Status Alert Reports and Favorite Filter Upgrade

The table describes the changes between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
End User Monitor View (name was changed - automatically upgraded)	End User Monitor View listed in the report filter's list of views	End User Monitors is listed in the report filter's list of views

Upgrade of Downtime for Alerts

For details, see "Downtime Upgrade" on page 243.

21

SOA, SAP, and Siebel Solutions Upgrade Information

This chapter includes:

- Upgrade Application Management for SOA on page 309
- Upgrade Application Management for SAP and Application Management for Siebel on page 311

Upgrade Application Management for SOA

The table describes what changed between BAC 8.x and BSM 9.x.

Topics	BAC 8.x	BSM 9.x
Operation CI with monitored_by attribute (automatically upgraded)	monitored_by attribute of the Operation CI	Monitored By attribute of the Operation CI
Webservice_operation CI with monitored_by_SiteScope attribute (automatically upgraded)	monitored_by_SiteScope attribute of the Webservice_operation CI	<ul style="list-style-type: none">➤ Monitored By attribute of the Webservice_operation CI➤ The For Sitescope value is added to the attribute
Operation CI with monitored_by_BPM attribute (automatically upgraded)	monitored_by_BPM attribute of the Operation CI	<ul style="list-style-type: none">➤ Monitored By attribute of the Operation CI➤ The For BPM value is added to the attribute

Topics	BAC 8.x	BSM 9.x
Operation CI with monitored_by_Diagnostics attribute (automatically upgraded)	monitored_by_Diagnostics attribute of the Operation CI	<ul style="list-style-type: none"> ▶ Monitored By attribute of the Operation CI ▶ The For Diagnostics value is added to the attribute
Manually specified objectives (automatically upgraded)	Objectives manually specified for the Operations CI	Objectives of the relevant health indicators of the Operation CI
Data from Business Process Monitor and SiteScope monitors		Data sent by the Business Process Monitor and SiteScope monitors affects the same Health Indicators (Synthetic HIs) in Service Health views and SLM.
	The Business Process Monitor and SiteScope monitors are monitoring the same operation.	The assignment of the objectives to the new Health Indicator is random and could come from either the objectives assigned to the operation monitored by Business Process Monitor or by SiteScope.

Upgrade Application Management for SAP and Application Management for Siebel

Several upgraders affect Application Management for SAP and Application Management for Siebel:

Topics	BAC 8.x	BSM 9.x
Business Process Step CIs changed into Business Transaction CIs		The EUM Model upgrader changes Business Process Step CIs into Business Transaction CIs. For details, see "Upgrade - Overview" on page 348.
Host CIs that had Measurement or Monitor child CIs are changed Measurement and Monitor CIs are removed from the model		Host CIs are now Node CIs. Measurement and Monitor CIs are changed into Health Indicators and KPIs attached to the relevant Infrastructure CIs. The Measurement and Monitor CIs are still visible in the System Monitor view.
Relevant KPIs and HIs to the appropriate CIs		The KES upgrader assigns the relevant KPIs and HIs to the appropriate CIs according to the 9.0 defaults.
Manually modified KPIs are upgraded		
Alerts		For details, see "Alerts Upgrade Information" on page 287

Note: The RTSM reconciliation is based on CI names, so if, before the upgrade, you have one or more SAP Enterprise CIs with the same name, it is recommended to delete obsolete SAP Enterprise CIs before you upgrade, as after the upgrade, child CIs of SAP Enterprise CIs with the same names will be connected to their own Siebel Enterprise CIs and to Siebel Enterprise CIs with the same name, creating an incorrect hierarchy. Proceed in the same way for Siebel Enterprise CIs.

22

Service Level Management Upgrade Information

This chapter includes:

- ▶ What's Changed? on page 314
- ▶ What Happens to BSM 8.x SLAs in 9.x? on page 317
- ▶ Converting 8.x SLAs to the BSM 9.x Format on page 318
- ▶ Examples of SLA Conversion on page 322
- ▶ SLA Conversion Settings on page 338

What's Changed?

The following table describes what changed in SLM, in BSM 9.x.

Area in Service Level Management	What's changed?
Monitor CIs removed	<p>In BAC 8.x, each monitored CI had a child CI which was called a monitor CI. KPIs which provided information on the monitored CI were assigned to its child CI - the monitor CI.</p> <p>In the BSM 9.x topology the layer of monitor CIs has been removed, and KPIs are now assigned directly to the monitored CIs.</p> <p>Note: SiteScope and EMS monitor CIs were not removed in BSM 9.x. For details on how to use SLM 9.x with SiteScope and EMS, see "Configuring SLAs Using SiteScope and EMS Data" in <i>Using Service Level Management</i>.</p>
Health Indicators added	<p>In BSM 9.x, an additional layer of information was added to the monitored CIs: health indicators (HIs).</p> <ul style="list-style-type: none"> ▶ HIs provide fine-grained monitoring of CIs, with far more detail than KPIs. Some HIs provides business metrics while others monitor aspects of performance and availability; for example a Windows computer CI might have three HIs: CPU load, memory utilization, and disk space. ▶ KPIs are now higher level indicators than HIs, and they represent a more general aspect of domain health, such as System Performance, System Availability, Application Performance, Application Availability, and so on. <p>For details, see "Indicators for CIs" in <i>Using Service Level Management</i>.</p>
SLA creation	<p>CI-based and service-based SLAs were unified into one wizard. For details, see "Building SLAs with the SLAs Wizard" in <i>Using Service Level Management</i>.</p>

Area in Service Level Management	What's changed?
Location breakdown	<p>In BAC 8., BPM transaction from location was topology based, defined by the source adapter within CMDB. In transaction-location mode, BPM reported a bpm_transaction_from_location CI instance per agent running the transaction.</p> <p>In BSM 9.x, SLAs over BPM data are by default defined as non-breakdown by location.</p> <p>For details on the new BPM topology, see "Business Process Monitor Upgrade" on page 350.</p> <p>To define an SLA with the location granularity, you must configure breakdown as part of the SLA creation. For details, see "Breakdown by Location for BPM CIs" in <i>Using Service Level Management</i>.</p>
Services modeling	<p>Services Modeling is done using the RTSM modeling studio; the SLM services manager user interface is integrated with the RTSM modeling studio user interface.</p>
Alerts administration	<p>Alerts are now administered within SLM, and not in a separate application.</p>
Applicable CIT definitions for calculation rules	<p>In earlier versions of SLM, an infrastructure setting defined the applicable CITs for each of the calculation rules.</p> <p>In BSM 9.x, for non-default rules these definitions are moved from the infrastructure setting to the rule template itself, within the business rule repository. The upgrader takes these definitions from the SLM infrastructure setting, and places them directly on the rule template.</p>
CIs Over Time vs. Target report	<p>The CIs Over Time vs. Target report is deprecated in BSM 9.x. If you were using this report prior to upgrade, it is now replaced with the CIs Over Time report.</p>

Area in Service Level Management	What's changed?
Downtime	<p>The Downtime form in BSM 8.x is replaced in BSM 9.x with the SLA Data Correction Schedule.</p>
	<p>Within the scheduling section, a number of frequency options were deprecated for the Monthly And Yearly definitions. Monthly and Yearly scheduling now support specific dates only, such as day 10 of every month (Monthly), or every January 5th (Yearly).</p> <p>If you have defined downtime in BSM 8.x using the deprecated frequency options (for example using first Sunday of every month, or first Sunday of January), these are not supported following upgrade. Within the SLA Data Corrections tab, define new frequency options as needed.</p>
	<p>BPM downtime definitions in 8.x are read-only in 9.x, and the calculation engine is not affected by them. This limitation is both for ongoing SLAs and re-calculation of SLAs.</p> <p>In order to define downtimes, use the centralized Platform downtime mechanism. For details, see "Downtime Management" in <i>Platform Administration</i>.</p> <p>If the downtime periods occurred in the past, use the SLA data correction mechanism.</p>
Custom calculation rules	<p>If you created custom Java rules or custom rule .jar files in pre-9.0 versions of BAC (now BSM), contact HP Professional Services for instructions on modifying and packaging them for BSM 9.x before upgrading.</p> <p>Note: This does not relate to custom rules in the repositories; it is only relevant if you have custom java rule source files.</p> <p>If you created custom Groovy rule files, see "Custom Rules" on page 261.</p>

Area in Service Level Management	What's changed?
Service offerings	<p>In 9.x, there is no longer an option of private service offerings; all offerings are now global (but the label Global is removed).</p> <p>Private offerings from 8.x are upgraded to regular (global) offerings in 9.x. If you had more than one private offering in 8.x with the same name, after upgrade you will see multiple offerings with the same name. To avoid this, you can rename these offerings before upgrade, or use global offerings instead.</p>
Edited calendars	<p>If you edited the predefined 24x7 or Business Hours Calendars in 8.x, the upgrade overrides your modifications.</p> <p>You must redefine your calendars manually after the upgrade, before you recalculate SLAs.</p>
RUM unconfigured end-user group CIs	<p>When upgrading in stages from BAC 7.x to BSM 9.x (that is, upgrading from BAC 7.x to BAC 8.x and then from BAC 8.x to BSM 9.x), a RUM unconfigured end-user group CI that is included in an SLA in BAC 7.x is no longer included in the upgraded SLA in BSM 9.x.</p>

What Happens to BSM 8.x SLAs in 9.x?

Following the upgrade process, you will not see any changes to your pre-9.x SLAs. Monitor CIs are not removed from these SLAs, and health indicators are not added to CIs. KPIs are still calculated based on sample data, and not based on HIs.

Note: 8.x SLAs will not be supported in future major releases. You can use the SLM conversion action to help you migrate your existing SLAs. For details, see "Converting 8.x SLAs to the BSM 9.x Format" on page 318.

If you make changes to an SLA following upgrade, the SLA is modified as follows:

- ▶ If you add a CI to an SLA, the KPI and HI assignment mechanism assigns KPIs and HIs to the CI. KPIs are calculated for this CI based on HIs, and not based on sample data.
- ▶ If you add a KPI to a CI, you must also assign an HI to that CI. The HI is calculated based on sample data, and the KPI is calculated based on the HI.

If you edit an SLA, the SLA will include CIs with some KPIs based on sample data with sample-based calculation rules (from the original SLA), and other KPIs calculated based on HIs, using group calculation rules (from BSM 9.x).

When you create a new SLA, the SLA uses the BSM 9.x format; the new SLA does not include monitor CIs, and KPIs are calculated based on HIs and not based on sample data.

Note: Hard-sync is not supported for SLAs created before BSM 9.x.

Converting 8.x SLAs to the BSM 9.x Format

Following the upgrade process, your existing SLAs are not changed. However, you have the option of converting each SLA's structure to the BSM 9.x format. This leaves the original SLA intact, and creates a new SLA which is aligned to the BSM 9.x concept as follows:

- ▶ Monitor CIs are removed from the SLA, and replaced with the monitored CIs themselves.
- ▶ Health Indicators are added to monitored CIs, and KPIs are calculated based on these HIs.

Note: The conversion **only** converts the SLA's structure and configuration; the calculation results that have been saved for the original SLA are not converted and not copied. If you delete your original SLA, its saved data is lost.

This section includes the following topics:

- "How to convert an SLA's structure" on page 319
- "How to view a summary of the structural changes" on page 319
- "Monitor CI replacement" on page 320
- "HIs added to replacement CIs" on page 320
- "Exceptions to typical KPI > HI conversion" on page 321

How to convert an SLA's structure

Within SLM Administration, open the Agreements Manager. Select an SLA from 8.x, and click the **Convert SLA** button. (This button is only visible if you have upgraded to BSM 9.x.)

A new SLA is created, with the label (**converted**) appended to the original SLA name.

How to view a summary of the structural changes

Select the converted SLA, and click the **Open SLA Conversion Report** button.

A report opens, listing the differences between the original SLA and the new one. For examples of this report, see the following:

- "Example 4: BPM in Regular Mode (Monitors Only)" on page 328
- "Example 5: SiteScope Group and Monitors Structure" on page 330
- "Example 6: SiteScope Monitors not under SiteScope Group; Replacement CI is not the Parent SLA" on page 333
- "Example 7: SiteScope 8.0 in Host > Monitors Structure" on page 336

Monitor CI replacement

Monitor CIs are replaced by monitored CIs, as defined in the conversion settings. For details, see "SLA Conversion Settings" on page 338.

The following table describes how monitor CIs are converted:

The monitor CI is replaced with...	When...
The monitor's parent CI in the SLA	The parent CI matches the conversion configuration for the monitor (see "SLA Conversion Settings" on page 338).
A related CI from the RTSM	<ul style="list-style-type: none"> ▶ The parent CI is not of the CI type defined by the mapping. ▶ The RTSM has a related CI that matches this replacement CI type, and this CI does not already exist in the SLA.
No replacement; the monitor CI stays in the SLA	<ul style="list-style-type: none"> ▶ The parent CI is not of the CI type defined by the mapping. ▶ The RTSM does not have a related CI that matches this replacement CI type.

The following monitor CIs are **not** removed:

- ▶ EMS monitors
- ▶ SiteScope monitors contained within SiteScope Groups
- ▶ BPM transaction by location monitor CIs, if your 8.0 Source Adapter had breakdown enabled
- ▶ Monitors which are defined in the conversion configuration as not replaced
- ▶ Monitors which are not defined in the conversion configuration

HIs added to replacement CIs

For each KPI assigned to a monitor CI in 8.x, the conversion assigns an HI to the replacement CI in 9.x based on the KPI. The KPI on the replacement CI is then calculated based on this HI.

HI rules, rule parameters, and selectors on the replacement CI are all copied from the KPI on the original monitor CI.

HIs are assigned to the replacement CI based on the KPI > HI mapping, as defined in the conversion settings. For details, see "SLA Conversion Settings" on page 338.

Note the following:

- If you have defined a KPI which has no mapping in the conversion configuration, a custom HI type is created in the indicator repository, and this is assigned to the CI.
- If a SiteScope monitor has been replaced by a monitored CI, HIs are assigned to the replacement CI using the SiteScope dynamic assignment. For details, see "SiteScope Dynamic HI Assignment" in *Using Service Level Management*.
- SLAs from 8.x can be edited in 9.x. If you convert such a hybrid SLA after editing it, the conversion copies HIs from the monitor CI to its replacement CI. KPIs on the replacement CI are based on the copied HIs.

Exceptions to typical KPI > HI conversion

- If multiple monitor CI instances are replaced by one replacement CI, and multiple HI instances of the same HI type should be created on the CI, only one HI instance is created. The HI rule and rule parameter are taken from only one of the HIs.
- If an Outage KPI (or a sibling KPI based on Outage) were defined on the monitor CI, and these KPIs are already defined on the replacement CI, the KPI is not copied from the monitor CI. This will be indicated in the conversion report.
- If a KPI on a monitor CI uses a custom calculation rule created with the Rules API, based on sibling KPIs, this rule is not copied to the KPI on the replacement CI. This will be indicated in the conversion report.
- Service Health (previously called Dashboard) PNR KPI definitions and SLA data correction definitions (previously called downtime) are not copied to the replacement CI. This behavior is identical to the Clone SLA operation.

Examples of SLA Conversion

This section includes the following:

- "Example 1: BPM Transaction by Location; 8.0 System in Breakdown Mode" on page 323
- "Example 2: BPM in Include Locations Mode" on page 325
- "Example 3: BPM in Regular Mode - Monitor CI Replaced with Parent CI" on page 327
- "Example 4: BPM in Regular Mode (Monitors Only)" on page 328
- "Example 5: SiteScope Group and Monitors Structure" on page 330
- "Example 6: SiteScope Monitors not under SiteScope Group; Replacement CI is not the Parent SLA" on page 333
- "Example 7: SiteScope 8.0 in Host > Monitors Structure" on page 336

Example 1: BPM Transaction by Location; 8.0 System in Breakdown Mode

Before conversion, the lowest level of the SLA is BPM Transaction from Location CI type. There are no health indicators, and the KPIs use sample rules:

The screenshot displays the 'BPM Transaction/Location' interface. The top section shows a tree view of CI types, with 'SLM BPM Transaction from Location' highlighted in red. The bottom section shows a table of KPIs with 'Business Rule' highlighted in red.

CI Name	CI Type
BPM Transaction/Location	Service Level Agreement
Service 1	BusinessService
Trade	BusinessTransactionFlow
Checkout	BusinessTransaction
Checkout From New York	SLM BPM Transaction from Location
Checkout From Tokyo	SLM BPM Transaction from Location
Login	BusinessTransaction
Login From New York	SLM BPM Transaction from Location
Login From Tokyo	SLM BPM Transaction from Location
Logout	BusinessTransaction
Logout from New York	SLM BPM Transaction from Location
Logout From Tokyo	SLM BPM Transaction from Location
Search	BusinessTransaction
Search From New York	SLM BPM Transaction from Location
Search From Tokyo	SLM BPM Transaction from Location

KPI Name	Business Rule	KPI ...	Calc...	Rela...
Application Availability	BPM Average Availability	Applic...	N/A	N/A
Application Performance	BPM Percentile	Applic...	N/A	N/A
Application Response Time	BPM Average Response Time	End ...	N/A	N/A

After the SLA conversion, monitors are not replaced because the CIT was BPM Transaction from Location, and the 8.0 Source Adapter was in breakdown mode. KPIs are calculated based on HIs, and HIs are created with the same rules as the original SLA's KPIs.

The converted SLA shows the following in the KPIs tab:

BPM Transaction/Location(converted)

CI Name	CI Type
BPM Transaction/Location(converted)	Service Level Agreement
Service 1	BusinessService
Trade	BusinessTransactionFlow
Checkout	BusinessTransaction
Checkout From New York	SLM BPM Transaction from Location
Checkout From Tokyo	SLM BPM Transaction from Location
Login	BusinessTransaction
Logout	BusinessTransaction
Search	BusinessTransaction

CI Data: Checkout From New York

KPIs Health Indicators Weights

KPI Name	Business Rule	Related Health Indicators
Application Availability	Group Average Value	Synthetic User Transaction Availability
Application Performance	Group Average Value	Synthetic User Transaction Perform...
Application Response Time	Group Average Value	BPM Response Time
Outages	BPM Outage	N/A

The converted SLA shows the following in the HIs tab:

CI Data: Checkout From New York

KPIs Health Indicators Weights

Health Indicator Name	Business Rule	Related KPIs
BPM Response Time	BPM Average Response Time	Application Response Time
Synthetic User Transaction Avai...	BPM Average Availability	Application Availability
Synthetic User Transaction Perf...	BPM Percentile	Application Performance

Example 2: BPM in Include Locations Mode

Before conversion, the lowest level of the SLA is Business Transaction CI type. There are no health indicators, and the KPIs use sample rules:

The screenshot displays the BMC Service Level Management console. The top section shows a tree view of the BPM (Include Locations) structure. The 'BPM (Include Locations)' node is highlighted with a red box. Below it, the 'Service 1' node is expanded to show 'Trade', which is further expanded to show 'Checkout', 'Login', 'Logout', and 'Search'. The 'Checkout' node is highlighted in blue, and its 'BusinessTransaction' CI type is also highlighted with a red box.

CI Name	CI Type
BPM (Include Locations)	Service Level Agreement
Service 1	BusinessService
Trade	BusinessTransactionFlow
Checkout	BusinessTransaction
Login	BusinessTransaction
Logout	BusinessTransaction
Search	BusinessTransaction

The bottom section shows the 'CI Data: Checkout' view. The 'KPIs' tab is selected. The 'Add KPI' button is visible. The table below shows the KPI data for Checkout.

KPI Name	Business Rule	Related Health Indi...
Application Availability	BPM Average Availability	N/A
Application Performance	BPM Percentile	N/A
Application Response Time	BPM Average Response Time	N/A
Outages	BPM Outage	N/A

After conversion, the Business Transaction CIs are not replaced. KPIs are calculated based on HIs, and HIs are created with the same rules as the original SLA's KPIs. The SLA structure is now the out-of-the-box structure for BPM.

The converted SLA shows the following in the KPIs tab:

The screenshot shows the 'BPM (Include Locations)(converted)' SLA configuration. The 'KPIs' tab is selected, displaying a table of KPIs associated with the 'Checkout' CI.

CI Name	CI Type
BPM (Include Locations)(converted)	Service Level Agreement
Service 1	BusinessService
Trade	BusinessTransactionFlow
Checkout	BusinessTransaction
Login	BusinessTransaction
Logout	BusinessTransaction
Search	BusinessTransaction

KPI Name	Business Rule	Related Health Indi...
Application Availability	Group Average Value	Application Availability(...)
Application Performance	Group Average Value	Application Performanc...
Application Response Time	Group Average Value	Application Response T...
Outages	BPM Outage	N/A

The converted SLA shows the following in the HIs tab:

The screenshot shows the 'BPM (Include Locations)(converted)' SLA configuration. The 'Health Indicators' tab is selected, displaying a table of health indicators associated with the 'Checkout' CI.

Health Indicator Name	Business Rule	Related KPIs
BPM Response Time	BPM Average Response Time	Application Response Time
Synthetic User Transaction Avai...	BPM Average Availability	Application Availability
Synthetic User Transaction Perf...	BPM Percentile	Application Performance

Example 3: BPM in Regular Mode - Monitor CI Replaced with Parent CI

This SLA shows BPM monitors in regular mode; the 8.0 SLA was not in transaction/location mode. The monitors are replaced with Business Transaction CIs, which are the 9.x version of BP Step CIs. In this case, the parent CI in the SLA is the Business Transaction, which is the monitored CI.

The original CI shows KPIs with sample rules on the monitor CI, with no HIs:

The screenshot displays the BMC Service Level Management interface. At the top, a tree view shows the hierarchy: 8.05 CS BPM > BPM4Alerts_1 > tx_10 > tx_10 monitor (highlighted with a red box). Below this, a table lists CIs with their types and associated KPIs. The 'tx_10 monitor' CI is highlighted in blue. Below the table, a section titled 'CI Data: tx_10 monitor' shows a 'KPIs' tab (highlighted with a red box) and a table of KPIs.

CI Name	CI Type	KPIs
8.05 CS BPM	Service Level Agreement	Applicatio... Applicatio... O
BPM4Alerts_1	BusinessTransactionFlow	Applicatio... Applicatio... O
tx_10	BusinessTransaction	Applicatio... Applicatio... O
tx_10 monitor	SLM BPM Transaction from Location	Applicatio... Applicatio... Applicatio... O
tx_15	BusinessTransaction	Applicatio... Applicatio... O
tx_15 monitor	SLM BPM Transaction from Location	Applicatio... Applicatio... Applicatio... O

KPI Name	Business Rule	KPI Domain	Calculated Based On	Related Health Inc
Application Availability	BPM Average Availability	Application	N/A	N/A
Application Performance	BPM Percentile	Application	N/A	N/A
Application Response Time	BPM Average Response Time	End User	N/A	N/A
Outages	BPM Outage	Business	N/A	N/A

In the converted SLA, there are no monitor CIs, and there are HIs on the Business Transaction level. This is the typical BSM 9.x out-of-the-box structure for BPM:

CI Name	CI Type	KPIs
8.05 CS BPM(converted)	Service Level Agreement	Application Av... Application Per... Outage
BPMAlerts_1	BusinessTransactionFlow	Application Av... Application Per... Outage
tx_10	BusinessTransaction	Application Av... Application Per... Outage
tx_15	businessTransaction	Application Av... Application Per... Outage

Health Indicator Name	Business Rule	Related KPIs
BPM Response Time	BPM Average Response Time	
Synthetic User Transaction Availability	BPM Average Availability	Application Availability
Synthetic User Transaction Performance	BPM Percentile	Application Performance

Example 4: BPM in Regular Mode (Monitors Only)

This SLA shows BPM monitors in regular mode; the 8.0 SLA was not in transaction/location mode. The monitors are replaced with Business Transaction CIs, which are the 9.x version of BP Step CIs. In this case, the parent CI in the SLA is not the business transaction (the monitored CI), so the business transactions are imported from RTSM into the SLA.

This is the original SLA:

CI Name	CI Type	KPIs
BPM - Regular - Only monitors	Service Level Agreement	Application Availability
tx_10 monitor	SLM BPM Transaction from Location	Application Availability
tx_15 monitor	SLM BPM Transaction from Location	Application Availability

KPI Name	Business Rule	KPI Domain	Calculated Based On	Related Health Indicators
Application Availability	BPM Average Availability	Application	N/A	N/A

The converted SLA shows the following:

CI Name	CI Type	KPIs
BPM - Regular - Only monitors(converted)	Service Level Agreement	Application Availability
tx_10	BusinessTransaction	Application Availability
tx_15	BusinessTransaction	Application Availability

Health Indicator Name	Business Rule	Related KPIs
Synthetic User Transaction Availability	BPM Average Availability	Application Availability

This is the conversion report describing the changes that were made (see "How to view a summary of the structural changes" on page 319):

Conversion Report - BPM - Regular - Only monitors

Original SLA

BPM - Regular - Only monitors
 tx_10 monitor
 tx_15 monitor

Converted SLA

BPM - Regular - Only monitors(converted)
 tx_10
 tx_15

Conversion Info

CI	CI Type	Replacement CI	Replacement CI Type	KPI->HI conversion		Additional Info
				KPI	HI	
tx_10 monitor	SLM BPM Transaction from Location	tx_10 (Monitored CI)	BusinessTransaction	Application Availability	Synthetic User Transaction Availability	None
tx_15 monitor	SLM BPM Transaction from Location	tx_15 (Monitored CI)	BusinessTransaction	Application Availability	Synthetic User Transaction Availability	None

Example 5: SiteScope Group and Monitors Structure

The following SLA shows the typical 8.x SiteScope group and monitor structure:

The screenshot displays the SiteScope interface. The top section shows a tree view of CI Name and CI Type. The CI Name column lists the hierarchy: SiteScope - SiteScope Group, Service 4, CPU SiteScope Group, CPU - Windows1, and CPU - Windows2. The CI Type column lists: Service Level Agreement, BusinessService, SiteScope Group, SiteScope Monitor, and SiteScope Monitor. The 'SiteScope Group' and 'SiteScope Monitor' rows are highlighted with a red box. Below this, the 'CI Data: CPU - Windows1' section is shown, with tabs for KPIs, Health Indicators, and Weights. The KPIs tab is active, showing a table with columns for KPI Name, Business Rule, and Related Health Indicators.

CI Name	CI Type
SiteScope - SiteScope Group	Service Level Agreement
Service 4	BusinessService
CPU SiteScope Group	SiteScope Group
CPU - Windows1	SiteScope Monitor
CPU - Windows2	SiteScope Monitor

KPI Name	Business Rule	Related Health Indicators
System Availability	SiteScope Monitor Rule	N/A
Outages	SiteScope Monitor Outage	N/A

In the converted SLA, monitors are not replaced because this structure is valid on BSM 9. Health indicators are created for each KPI. The System Availability KPI is always mapped to the Legacy System HI in the conversion flow for SiteScope in this hierarchy. The rule for the System Availability KPI is also not replaced in this scenario.

The converted SLA shows the following in the KPIs tab:

SiteScope - SiteScope Group(converted)

Hide KPIs

CI Name	CI Type
SiteScope - SiteScope Group(converted)	Service Level Agreement
Service 4	Business Service
CPU SiteScope Group	SiteScope Group
CPU - Windows1	SiteScope Monitor
CPU - Windows2	SiteScope Monitor

CI Data: CPU - Windows1

KPIs Health Indicators Weights

Add KPI

KPI Name	Business Rule	Related Health Indicators
System Availability	Group Average Value	Legacy System
Outages	SiteScope Monitor Outage	N/A

The converted SLA shows the following in the HIs tab:

CI Data: CPU - Windows1

KPIs Health Indicators Weights

Add KPI

Health Indicator Name	Business Rule	Related KPIs
Legacy System	SiteScope Monitor Rule	System Availability

This is the conversion report describing the changes that were made (see "How to view a summary of the structural changes" on page 319):

Conversion Report - SiteScope - SiteScope Group

Original SLA

SiteScope - SiteScope Group
 Service 4
 CPU SiteScope Group
 CPU - Windows1
 CPU - Windows2

Converted SLA

SiteScope - SiteScope Group(converted)
 Service 4
 CPU SiteScope Group
 CPU - Windows1
 CPU - Windows2

Conversion Info

CI	CI Type	Replacement CI	Replacement CI Type	KPI->HI conversion		Additional Info
				KPI	HI	
CPU - Windows1	SiteScope Monitor	CPU - Windows1 (Not replaced)	SiteScope Monitor	System Availability	Legacy System	None
CPU - Windows2	SiteScope Monitor	CPU - Windows2 (Not replaced)	SiteScope Monitor	System Availability	Legacy System	None

Example 6: SiteScope Monitors not under SiteScope Group; Replacement CI is not the Parent SLA

In the following SLA, **CPU - Windows1** Monitor is monitoring Windows1, and both **CPU - Window2** and **Diskspace - Windows2** are monitoring Windows2.

The screenshot shows the SiteScope interface. The top part displays a hierarchy of CIs (Configuration Items) under the title "SiteScope - Only Monitors". The hierarchy is as follows:

- SiteScope - Only Monitors (Service Level Agreement)
 - Service 5 (Business Service)
 - CPU - Windows1 (SiteScope Monitor)
 - CPU - Windows2 (SiteScope Monitor)
 - Diskspace - Windows2 (SiteScope Monitor)

The bottom part of the screenshot shows the "CI Data: CPU - Windows1" view. It has tabs for "KPIs", "Health Indicators", and "Weights". The "KPIs" tab is active, showing a table of KPIs:

KPI Name	Business Rule	Related Health Indicators
System Availability	SiteScope Monitor Rule	N/A
Outages	SiteScope Monitor Outage	N/A

In the converted SLA, monitors are replaced with the monitored CIs. KPIs using sample rules are replaced with HIs according to the monitor's HI list. The rule for the new HI is also replaced in this flow. For details on the flow's logic, see "Understanding the SiteScope monitor conversion configuration" on page 345.

The converted SLA shows the following in the KPIs tab:

The screenshot shows the 'SiteScope - Only Monitors (converted)' interface. At the top, there are icons for navigation and a 'Hide KPIs' button. Below is a table with two columns: 'CI Name' and 'CI Type'. The table content is as follows:

CI Name	CI Type
SiteScope - Only Monitors (converted)	Service Level Agreement
Service 5	Business Service
Windows1	Windows
Windows2	Windows

Below this table is a section for 'CI Data: Windows2' with tabs for 'KPIs', 'Health Indicators', and 'Weights'. The 'KPIs' tab is active, showing a table with columns: 'KPI Name', 'Business Rule', 'Related Health Indicators', and 'Calculate...'. The table content is:

KPI Name	Business Rule	Related Health Indicators	Calculate...
System Availability	Group Average Value	CPU Load, Disk	HIs
Outages	SiteScope Monitor Out...	N/A	N/A

The converted SLA shows the following in the HIs tab:

The screenshot shows the 'CI Data: Windows2' interface with the 'Health Indicators' tab active. It displays a table with columns: 'Health Indicator Name', 'Business Rule', and 'Related KPIs'. The table content is:

Health Indicator Name	Business Rule	Related KPIs
CPU Load	SiteScope Availability Rule	System Availability
Disk	SiteScope Availability Rule	System Availability

This is the conversion report describing the changes that were made (see "How to view a summary of the structural changes" on page 319):

Conversion Report - SiteScope - Only Monitors

Original SLA

SiteScope - Only Monitors
 Service 5
 CPU - Windows1
 CPU - Windows2
 Diskspace - Windows2

Converted SLA

SiteScope - Only Monitors(converted)
 Service 5
 Windows1
 Windows2

Conversion Info

CI	CI Type	Replacement CI	Replacement CI Type	KPI->HI conversion		Additional Info
				KPI	HI	
CPU - Windows1	SiteScope Monitor	Windows1 (Monitored CI)	Windows	System Availability	CPU Load	None
CPU - Windows2	SiteScope Monitor	Windows2 (Monitored CI)	Windows	System Availability	CPU Load	None
Diskspace - Windows2	SiteScope Monitor	Windows2 (Monitored CI)	Windows	System Availability	Disk	None

Example 7: SiteScope 8.0 in Host > Monitors Structure

In this example, the original SLA structure is **Monitored CI > SiteScope Monitor**.

The screenshot shows the SiteScope - Hardware Monitors interface. At the top, there is a toolbar with icons for navigation and a 'Hide KPIs' button. Below this is a tree view of CI types. The tree structure is as follows:

- SiteScope - Hardware Monitors (Service Level Agreement)
 - Service 3 (BusinessService)
 - Windows1 (Windows)
 - CPU - Windows1 (SiteScope Monitor)
 - Windows2 (Windows)
 - CPU - Windows2 (SiteScope Monitor)
 - Diskspace - Windows2 (SiteScope Monitor)

The 'CPU - Windows2' row is highlighted in blue. Below the tree view, there is a section for 'CI Data: CPU - Windows2' with tabs for 'KPIs', 'Health Indicators', and 'Weights'. The 'KPIs' tab is active, showing a table with the following data:

KPI Name	Business Rule	Related Health Indic...	Calcula...
System Availability	SiteScope Monitor Rule	N/A	N/A
Outages	SiteScope Monitor Outage	N/A	N/A

The converted SLA gives the same result as the previous example. In this example monitors are replaced with the parent CI. The Outage from the monitors are not copied to the parent CI, since the parent CI already has an Outage defined.

The difference between the two examples can be seen in the conversion report, which indicates that the Outage is not copied:

Conversion Report - SiteScope - Hardware Monitors

Original SLA

```
SiteScope - Hardware Monitors
  Service 3
    Windows1
      CPU - Windows1
    Windows2
      CPU - Windows2
      Diskspace - Windows2
```

Converted SLA

```
SiteScope - Hardware Monitors(converted)
  Service 3
    Windows1
    Windows2
```

Conversion Info

CI	CI Type	Replacement CI	Replacement CI Type	KPI->HI conversion		Additional Info
				KPI	HI	
CPU - Windows1	SiteScope Monitor	Windows1 (Parent CI)	Windows	System Availability	CPU Load	Outages (Already exist on parent)
CPU - Windows2	SiteScope Monitor	Windows2 (Parent CI)	Windows	System Availability	CPU Load	Outages (Already exist on parent)
Diskspace - Windows2	SiteScope Monitor	Windows2 (Parent CI)	Windows	System Availability	Disk	Outages (Already exist on parent)

SLA Conversion Settings

You can view SLA conversion settings in the following location: **Admin > Platform > Setup and Maintenance > Infrastructure Settings > Applications > Service Level Management Conversion.**

This section includes the following topics:

- "The conversion settings" on page 338
- "Understanding typical conversion configurations" on page 341
- "Understanding the SiteScope monitor conversion configuration" on page 345

The conversion settings

The following table describes the SLA conversion infrastructure settings. In general you do not need to make any changes to the default settings; however you can modify settings to match your particular environment.

Conversion Setting	Description
Allowed SiteScope monitor CI type as SLA parent	If this CI Type exists in the SLA as the parent CI for a SiteScope monitor or measurement CI, the SiteScope CI is not replaced. Default: SiteScope CI. For an example, see "Example 5: SiteScope Group and Monitors Structure" on page 330.
Candidate CI Types	Defines which CI types are candidates for replacement in the conversion; the CI must also be a leaf CI in the SLA; default is monitor and BP Step (for SLAs where include location is enabled). Change this only if you have created your own custom CI type that is not a sub class of the Monitor CIT.
CI Types support location attribute	The CI types which have a location attribute; default is BPM monitors. Change this only if you have created your own custom CI type that is not a sub class of BPM monitor, and it supports locations.

Conversion Setting	Description
CI Types support selector attribute	The CI types which have a selector, for KPI > HI conversion. Change this only if you have created your own custom CI type that is not a sub class of monitor, and it has selectors.
Conversion configuration	Describes the conversion configuration logic, for details see "Understanding typical conversion configurations" on page 341.
Is verbose logging	Change this for support cases; logs are written to the Gateway machine as follows: log\slm_conversion\ <customer id="">\<source name><="" sla="" td=""/> </customer>
KPIs to ignore	These KPIs are ignores in the KPI > HI conversion; the KPIs are unchanged. The KPI ID is from the SLM KPI repository. Add additional KPIs if you have created KPIs that you want to leave unchanged.
Legacy HI Type	For SiteScope monitor CIs only; this is the HI type that is created for any Legacy KPI type, as specified in the following setting. For an example, see "Example 5: SiteScope Group and Monitors Structure" on page 330. Change this if you want another HI type to be created.
Legacy KPI Type	For SiteScope monitor CIs only; this is the KPI type that is converted to the Legacy HI type, as specified above. For an example, see "Example 5: SiteScope Group and Monitors Structure" on page 330.
Outage Rules by rule id	These rules are handled according to the Outage logic, identified by their rule ID in the SLM rule repository. Add rules here if you have created your own Outage rules, for example using the Rules API.
Outage Rules	These rules are handled according to the Outage logic, identified by their rule class in the SLM rule repository. Add rules here if you have created your own Outage rules using Java (if you have used the Rules API, see above).

Conversion Setting	Description
Outage Rules based on samples, by rule id	<p>These rules are handled according to the Outage logic, identified by their rule ID in the SLM rule repository.</p> <p>Add rules here if you have created your own Outage rules based on samples, using the Rules API.</p>
Outage Rules based on samples	<p>These rules are handled according to the Outage logic, identified by their rule class in the SLM rule repository.</p> <p>Add rules here if you have created your own Outage rules based on samples using Java (if you have used the Rules API, see above).</p>
Rules to ignore	<p>KPIs with these rules are not part of the KPI > HI conversion.</p> <p>Add additional KPIs if you have created rules that you want to leave unchanged.</p>
Sibling rules based on outage	<p>These rules, identified by their class name, represent Outage related rules, and are handled according to the Outage related rules logic.</p> <p>Add rules here if you implemented your own Outage related rules in Java.</p>
Sibling rules not based on outage, by rule id	<p>These rules, identified by their rule ID, represent Sibling rules, and are handled according to the Sibling rules logic.</p> <p>Add rules here if you implemented your own sibling rules using the Rules API.</p>
Sibling rules not based on outage	<p>These rules, identified by their class name, represent Sibling rules, and are handled according to the Sibling rules logic.</p> <p>Add rules here if you implemented your own sibling rules in Java.</p>

Understanding typical conversion configurations

Within the conversion settings there is a setting called **Conversion configuration**. This XML defines the logic of the SLA conversion, for monitor replacement and KPI > HI conversion.

There are two types of configuration: typical, and SiteScope monitors. The following section describes the typical configuration; the configuration for SiteScope monitors is described in "Understanding the SiteScope monitor conversion configuration" on page 345.

Define the candidate CI type and the replacement CI type

The XML contains the following elements:

- **Candidate - ciType**. Mandatory; this string represents the exact CI type for the candidate (CI types that are sub classes of this CI type are not handled, and require a separate configuration).

Validation is done if the candidate passes the preliminary conditions: The CI must be a leaf CI on the SLA, and it must be one of the CI types defined in the **Candidate CI type** setting.

- **Replacement - repType**. Mandatory, options are "self" /"other".

If "self", use the same CI; candidate is not replaced.

If "other", search for a replacement CI, according to the conversion configuration logic.

- **Replacement - Exclude**. Applicable only for "other" replacement type. Optional, default value is false.

If true, the replacement CI type should not match the candidate CI type. (True should be used only when the replacement CI type should be "not one of...".)

If false, the replacement CI type should match the candidate CI type.

- **Replacement - CI type**. Applicable only for "other" type. Multiple entries are allowed; minimum of one entry is required. "OR" condition is applied between entries.

- **name**. Mandatory, string represents the replacement CI type.

- **isDerived**. Mandatory, Boolean.

If true, replacement CI type that is sub classes of the ciType would be accepted too.

If false, only replacement CI type with the exact type of the ciType would be accepted

KPI > HI replacement configuration

This list defines which HI type replaces each KPI type on the replaced CI.

Each <kpiInfo> entry contain the KPI ID as displayed in the KPI repository, and the HI as displayed in the indicator repository. Zero to multiple <kpiInfo> entries are allowed.

Examples of conversion configurations

- 1 In the following example, business transaction CIs are not replaced. There are three mappings of KPIs > HIs for the default KPIs of the CI in include location mode.

```
<candidate ciType="business_transaction">
  <replacement repType="self">
    </replacement>
  <kpiInfo>
    <kpiType>101</kpiType> <!-- Availability KPI -->
    <hiType>58655555-d379-5555-b88e-5992ca393555</hiType> <!-- Synthetic User Transaction Availability -->
  </kpiInfo>
  <kpiInfo>
    <kpiType>106</kpiType> <!-- Performance KPI -->
    <hiType>53333224-2333-332c-b33e-5333ca393b27</hiType> <!-- Synthetic User Transaction Performance -->
  </kpiInfo>
  <kpiInfo>
    <kpiType>103</kpiType> <!-- Response Time -->
    <hiType>88884264-6888-b233-888f-b1345555b33</hiType> <!-- BPM Response Time -->
  </kpiInfo>
</candidate>
```

- 2 In the following example, the tv_tx_monitor CI type is replaced with business_transaction CI, with derived = false. There is no KPI > HI assignment, meaning each KPI instance is e replaced with a Custom HI type that is created during the conversion.

```

<!-- 1. Convert all KPIs defined on tv_tx_monitor CI type to custom HIs on business_transaction CI type -->
<candidate ciType="tv_tx_monitor">
  <replacement repType="other">
    <ciType name="business_transaction" isDerived="false"/>
  </replacement>
</candidate>
<!-- End TV SLA Upgrade -->

```

- 3 In the following example, the business process scope CI is not replaced, and there is no KPI > HI mapping.

```

<candidate ciType="business_process_scope">
  <replacement repType="self"/>
</candidate>

```

- 4 The following example is for the SLM BPM transaction from location CI. This CI type is the BPM transaction from location monitor from pre-9.x versions. It is replaced with the business transaction CIT, with derived= true, meaning it will be replaced with sub classes of business transaction. There are three KPI > HI mappings.

Note: This specific CI type is not replaced if it represents a CI from a specific location (for an example, see "Example 1: BPM Transaction by Location; 8.0 System in Breakdown Mode" on page 323).

For this monitor type, only CIs that are connected in RTSM to the monitor CI with a specific link type (slm_breakdown link type) are considered as replacement CIs from RTSM.

```
<candidate ciType="slm_bpm_tx_from_location" >
  <replacement repType="other">
    <ciType name="business_transaction" isDerived="true"/>
  </replacement>
  <kpiInfo>
    <kpiType>101</kpiType> <!-- Availability KPI -->
    <hiType>58655555-d379-5555-b88e-5992ca393555</hiType> <!-- Synthetic User Transaction Availability -->
  </kpiInfo>
  <kpiInfo>
    <kpiType>106</kpiType> <!-- Performance KPI -->
    <hiType>53333224-2333-332c-b33e-5333ca393b27</hiType> <!-- Synthetic User Transaction Performance -->
  </kpiInfo>
  <kpiInfo>
    <kpiType>103</kpiType> <!-- Response Time -->
    <hiType>88884264-6888-b233-888f-b13455555b33</hiType> <!-- BPM Response Time -->
  </kpiInfo>
</candidate>
```


Understanding the SiteScope monitor conversion configuration

SiteScope monitors have a special conversion flow, as described below. For examples of SiteScope conversions see "Examples of SLA Conversion" on page 322.

The following is the SiteScope monitor conversion flow, with descriptions of its components:

```
<candidate ciType="sitescope_monitor" supportCandidateHiList="true">
  <replacement exclude="false" repType="other">
    <ciType isDerived="true" name="infrastructure_element">
      <linkInfo name="monitored_by" isDerived="false"/>
    </ciType>
  </replacement>
  <rulesMappingInfo>
    <sourceRuleName>com.mercury.am.bac.slm.rules.leaf.impl.rule.sis.SisMonitorRule</sourceRuleName>
    <sampleModeTargetRuleId>3920</sampleModeTargetRuleId>
    <eventModeTargetRuleId>445</eventModeTargetRuleId>
    <hiListAttributeName>health_indicator_list</hiListAttributeName>
    <modeAttributeName>reporting_mode</modeAttributeName>
  </rulesMappingInfo>
</candidate>
```

- ▶ **supportCandidateHiList="true"** in the candidate attribute means that:
 - There is no KPI > HI mapping; HIs are created according to the monitor HI list attribute value, if applicable.
 - If the CIT of the parent in the SLA is SiteScope Group, the monitor is not replaced.
- ▶ The replacement CI type must be from Infrastructure Element and all its sub classes.
- ▶ The replacement CI must be connected to the monitor with a **monitored_by** link.
- ▶ **rulesMappingInfo**. Describes the KPI > HI conversion logic; multiple entries are allowed.

This section is applicable only if:

- ▶ The monitor CI's HI list is not empty. If it is empty this section is not applicable, and each KPI is converted to a Custom HI.
- ▶ The monitor is not replaced with itself (under SiteScope group).
- ▶ The replacement CI is monitored by SiteScope.
- ▶ **sourceRuleName.** This is the full class name of the rule whose related KPI is replaced with HIs, according to HI assignments. Each KPI that has another rule is replaced with a Custom HI type.
- ▶ **sampleModeTargetRuleId.** This is the rule ID that is used for each HI created with the HI assignments, if the mode of the monitor is sample mode (and not events only).
- ▶ **eventModeTargetRuleId.** This is the rule ID that is used for each HI created with the HI assignments, if the mode of the monitor is event mode.
- ▶ **hiListAttributeName.** The attribute that holds the HI list for the monitor.
- ▶ **modeAttributeName.** The attribute that holds the event/sample information. If the value is "Events" (non-case sensitive) the mode of the monitor is event mode; with any other value the mode of the monitor is samples mode.

23

End User Management Upgrade Information

This chapter includes:

- ▶ Upgrade - Overview on page 348
- ▶ Pre Upgrade Actions on page 349
- ▶ Business Process Monitor Upgrade on page 350
- ▶ Real User Monitor Upgrade on page 359
- ▶ EUM Alerts Upgrade on page 373
- ▶ CI Links Upgrade on page 373
- ▶ Views Upgrade on page 373
- ▶ Deleted CIs on page 377
- ▶ Permissions Upgrade on page 379
- ▶ EUM Reports Upgrade on page 380
- ▶ Post Upgrade Actions on page 393

Upgrade - Overview

In BSM 9.x, the End User Management (EUM) model is significantly different from the model in BAC 8.x, requiring many upgrades to data and configurations. The EUM upgraders are included as part of the general BSM upgrade wizards.

The following are some of the major changes to the EUM model in BSM 9.x:

- ▶ Run-time Service Model (RTSM) is used as a single configuration source for BPM and RUM, replacing the profile paradigm. This simplifies administration by being able to use one-time configurations as needed. It enables administrators both to model the end-user services and monitoring needs in a single action, as well as to have a seamless flow into Service Health views without any further configuration.

RTSM is automatically updated by Real User Monitor. Real User Monitor discovery is based on both the servers and running software, and subnet information that it encounters, populating the relevant Configuration Items (CIs) into the model. These CIs are automatically reconciled with CIs discovered by related monitoring tools such as HP Diagnostics. All BSM products share and populate a common data model, improving the consistency and visibility of the dynamic environment on which the transactions flow.

- ▶ The new unified EUM class model includes:
 - ▶ The alignment of the Business Process Monitor and Real User Monitor models, allowing both data sources to report data on the same CI.
 - ▶ A simplified administration to maintain a unique model that can be used by the different BSM applications.
 - ▶ An easier user flow between the different BSM applications using the same model.
- ▶ EUM applications are standardized to the same application data model used across the other BSM products such as HP Diagnostics and Transaction Management. The EUM applications populate this model directly with transactions and dependencies, thereby increasing the consistency of the data model.

- ▶ A new integrated EUM user interface has been introduced, providing the ability to administer both Business Process Monitor and Real User Monitor from a single user interface, thereby streamlining and simplifying configuration.
- ▶ The script repository performance and import capability have been improved. Instead of loading one script at a time, you can import many scripts with a simple drag and drop operation, helping you reuse your existing scripts.
- ▶ Support for distributed monitored applications. One application can now be monitored by multiple Real User Monitor engines, increasing scalability options.
- ▶ Real User Monitor provides an automatic classification of the protocol actions (saving manual configuration overhead) and automatically identifies the back-end tier, for which it reports meaningful information such as performance, availability, and volume.

Pre Upgrade Actions

Before you run the End User Management Administration upgrade, you must perform the following actions:

- ▶ Ensure that all necessary Session Identification configurations do not have empty session ID values. Those with empty session ID values are not upgraded.
- ▶ Check-in all BPM scripts to the Script Repository. The upgrade process does not preserve the checked-out status of scripts.

Business Process Monitor Upgrade

This section describes the major changes to BPM data and configurations that are made as part of the End User Management Administration upgrade.

This section includes the following topics:

- "Model Changes" on page 350
- "Profiles Upgrade" on page 354
- "BPM Agents and Locations Upgrade" on page 356
- "Containers Upgrade" on page 356
- "Transactions Upgrade" on page 357
- "Troubleshooting and Limitations" on page 358

Model Changes

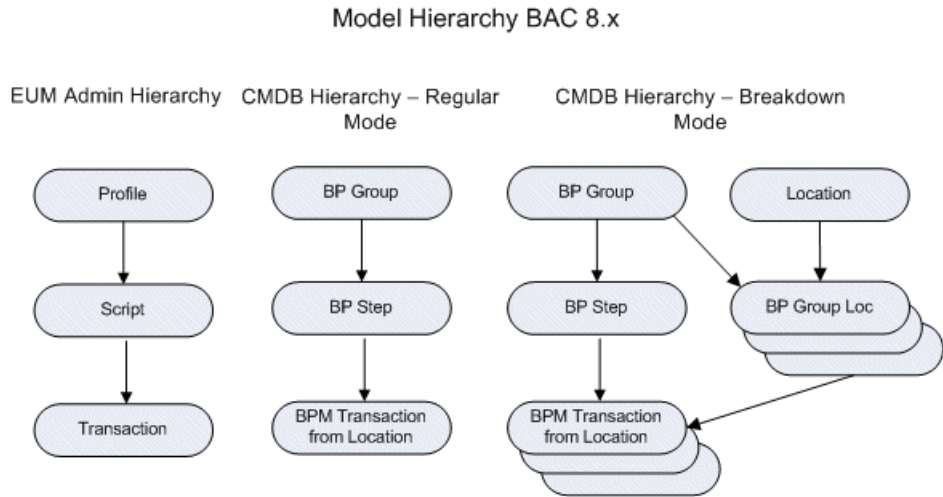
This section describes the major changes to the End User Management Administration model for Business Process Monitor in BSM 9.x.

This section includes the following topics:

- "Schema" on page 351
- "New CI Types" on page 352
- "Application Hierarchy Level" on page 352
- "Scripts" on page 353
- "Location Breakdown" on page 353
- "Location Aware Thresholds" on page 353

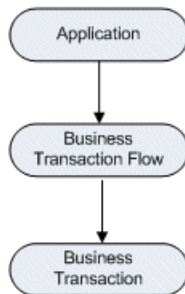
Schema

The following graphic shows the Business Process Monitor hierarchy in End User Management and the corresponding database entries for the BAC 8.x BSM 9.x models:



Model Hierarchy BSM 9.x

EUM Admin and RTSM Hierarchy



New CI Types

The major EUM CI types for Business Process Monitor are replaced by new CI types in BSM 9.x. The following table shows the BAC 8.x CI types and the equivalent new CI types in BSM 9.x:

BAC 8.x CI Type	BSM 9.x CI Type
Business Process Group	Business Transaction Flow
Business Process Step	Business Transaction
BPM Transaction from Location	Removed

Note: After the upgrade old CI types remain in the model, but are obsolete and should not be used.

Application Hierarchy Level

In the new EUM model, applications have been added to the hierarchy as a new level on top of business transaction flows (which have replaced the old BP groups and profiles). Applications can contain multiple business transaction flows and will also include some of the configuration details that were previously saved on the profile level. For details, see "Profiles Upgrade" on page 354.

Note: While in BSM 9.x it is a recommended best practice to create one business transaction flow for a flow that corresponds to one script, the upgrade procedure upgrades each entire profile to one business transaction flow so that it more closely mirrors the BAC 8.x hierarchy.

Scripts

In BSM 9.x, BPM scripts are no longer part of the End User Management Administration tree. Instead, they are displayed as part of a business transaction flow's properties.

Note: In BAC 8.x, script version numbers are in the format x.x.xx, whereas in BSM 9.x they are in the format x.x.x (that is, the third level is a single digit only). A BAC 8.x script version ending in double digits is upgraded to a BSM 9.x script version with the third level reset to 0 and the second level incremented by 1. For example, 1.1.10 is upgraded to 1.2.0.

Location Breakdown

In the EUM BPM model in BSM 9.x, the breakdown mode has been removed. There is now only one Business Transaction that represents the BPM transaction for all the locations that execute it. You can view location breakdown by creating a Local Impact View (LIV). For details on LIV views, see "View Builder Overview" in *Using Service Health*.

The following location breakdown related CI types have been removed:

- ▶ BPM Transaction from Location
- ▶ Business Process Group Location

Location Aware Thresholds

The EUM BPM model is enhanced and now supports location aware thresholds. The model can hold different thresholds for transactions for each location.

If you are upgrading a system that works in breakdown mode, the upgrade process searches for dashboard KPIs on each BP Transaction from Location CI for which you changed the default threshold, and creates location specific thresholds for the corresponding transactions according to these values. This enables location aware thresholds you set in the old system (using Dashboard) to be saved in the upgraded system.

Profiles Upgrade

Profiles are upgraded to both applications and business transaction flows.

This section includes the following topics:

- "Applications" on page 354
- "Business Transaction Flows" on page 355

Applications

For each profile, the upgrade process attempts to locate an existing application to which the profile is connected. If no such application is found, or if more than one such application is found, the upgrade process creates a new parent application with a name that includes the profile name in the format <profile name>_application.

If the upgrade process identifies multiple profiles that are connected to the same application, but that match one of the following conditions, it creates a new application for each profile:

- Profiles stored in different Profile databases.
- Profiles set with different time zones.
- Profiles set with a different value in the **Ignore Outlier values** attribute.

An application set as a profile's parent application in the new model is configured with the following profile details:

- Profile database name
- Profile time zone

Note: A configuration file is used to map time zone offsets (used by the old model) and time zone IDs (used by the new model). The first time zone ID that matches the time zone offset is used. Manually reconfigure the correct time zone for the application after the upgrade has finished.

- Default transaction thresholds and breakdown settings
-

Note:

- When the upgrade process creates a new application for a profile, any existing applications to which the profile is connected are also linked to the upgraded business transaction flow, but these applications are not configured for Business Process Monitor in End User Management Administration (only the newly created application is configured for Business Process Monitor).
 - If the upgrade process uses an existing application for a profile, but determines that the application name is not unique, it renames the application to unique name.
-

Business Transaction Flows

For each profile, the upgrade process creates one corresponding business transaction flow with the same name as the profile. The following list shows the main settings configured for the business transaction flow by the upgrade process:

- Attached scripts and WebTraces
- Scripts order
- BPM agent assignments
- Transaction thresholds and breakdown settings
- Status

BPM Agents and Locations Upgrade

BPM agents are upgraded to the new model without change, but note the following considerations:

- ▶ As all locations are upgraded to a new hierarchical model, the End User Management Administration upgrade links BPM agents to the new, upgraded locations.
- ▶ In BAC 8.x, there is an option to set a group name on a profile's agent assignment. In the new model this option was removed, but new functionality was added that enables you to define custom attributes for each BPM agent.

The upgrade process converts configured group names to a BPM agent custom attribute called **group**. As the old group values were configured for a profile's agent assignment and the new custom attributes are configured for a BPM Agent, there may be cases where multiple values need to be converted to a single value. In such cases, the upgrade process uses the most frequent, non default value among the multiple values as the new, single value.

By replacing the Group property for BPM with custom attributes, the following functionality no longer exists:

- ▶ The group by **Group** and limit to **Group** options in event based alerts.
- ▶ The group by **Group** option in legacy EUM reports.
- ▶ No history is available in reports that use the new custom attributes.

Containers Upgrade

In BAC 8.x, you can place a profile, or a group of profiles, under any hierarchy of containers. In the new model, containers are replaced by CI collections (CiCollection CI type). The upgrade process converts containers to a corresponding hierarchy of CI collections and connects upgraded applications to the relevant CI collection.

If two profiles from different containers are connected to the same application, the upgrade process connects the profiles to the same application, and the application to both new, CI collections.

Note: Top level containers in BAC 8.x (that is, containers defined directly in the EUM Administration tree) are upgraded to BSM 9.x CI collections of the same name, but with a suffix of **-EUM**. For example, a BAC 8.x container called Container1 is upgraded to a BSM 9.x CI collection called Container1-EUM.

Transactions Upgrade

For each transaction, the upgrade process creates a Business Transaction CI.

The following table shows the changes made to transactions during the upgrade:

Description	8.x	9.x
Transaction coloring (for display in EUM reports)	Set for each profile transaction	Set for each transaction in an application
Transaction Availability threshold	Set only in Dashboard, for KPIs relevant to the transaction.	New transaction availability threshold configuration item. Note: The custom threshold values from KPIs are used as the new value for the transaction availability threshold.
Soft deleted transactions	Soft deleted transaction	Business Transaction CI without any BPM configuration. Note: This enables historical data to be displayed in reports.
Hard deleted transaction	Hard deleted transaction	Not upgraded

Troubleshooting and Limitations

This section includes troubleshooting and limitations for the End User Management Administration upgrade of Business Process Monitor.

BP Group Name and Description

In BAC 8.x, for each profile a corresponding BP Group is created in the CMDDB, with the name and description of the Business Process Group CI taken from the profile. You can change these values in the ITU, thereby having 2 different values for the same logical item.

In BSM 9.x, there is only one object (a business transaction flow) that represents the profile. The upgrade process takes the business transaction flow's name and description from the profile data. If you changed the profile's name or description in the ITU, the change is not upgraded and will not exist in the new model.

Checked-out Scripts

BPM scripts that are checked-out of the Script Repository, must be checked-in before the upgrade. The upgrade process does not preserve the checked-out status of scripts.

Profile Time Zone Offsets

A configuration file is used to map time zone offsets (used by the old model) and time zone IDs (used by the new model). The first time zone ID that matches the time zone offset is used. For example, if a profile has a time zone offset of GMT+12 for NZ (New Zealand), the corresponding application is configured by the upgrade process with the time zone for Antarctica, McMurdo, which is the first GMT+12 time zone.

Workaround: Manually reconfigure the correct time zone for the application after the upgrade has finished.

Baseline Configurations

BSM 9.1x does not support baseline configuration for end-user monitors. Baseline configuration for EUM profiles are not upgraded and static transaction thresholds are used for the business transaction flows created for profiles.

Real User Monitor Upgrade

This section describes the major changes to RUM data and configurations that are made as part of the End User Management Administration upgrade.

This section includes the following topics:

- "Model Changes" on page 359
- "RUM Pages Upgrade" on page 363
- "RUM Events Upgrade" on page 363
- "RUM Engine Details Upgrade" on page 364
- "Application Upgrade" on page 365
- "RUM Default Application Upgrade" on page 365
- "RUM End User Group Upgrade" on page 367
- "RUM Locations Upgrade" on page 368
- "RUM Servers Upgrade" on page 368
- "RUM Templates Upgrade" on page 368
- "Troubleshooting and Limitations" on page 369

Model Changes

This section describes the major changes to the End User Management Administration model for Real User Monitor in BSM version 9.x.

This section includes the following topics:

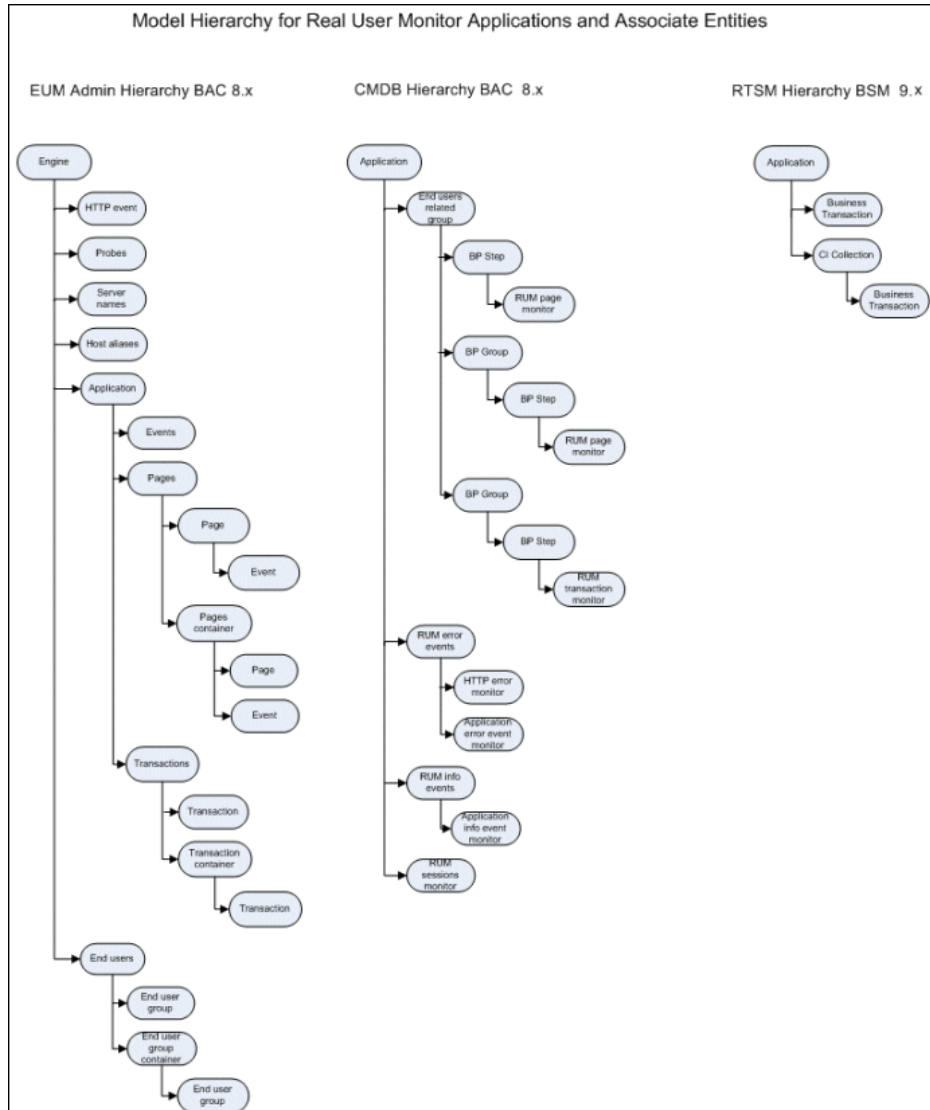
"Schema" on page 360

"New CI Types" on page 362

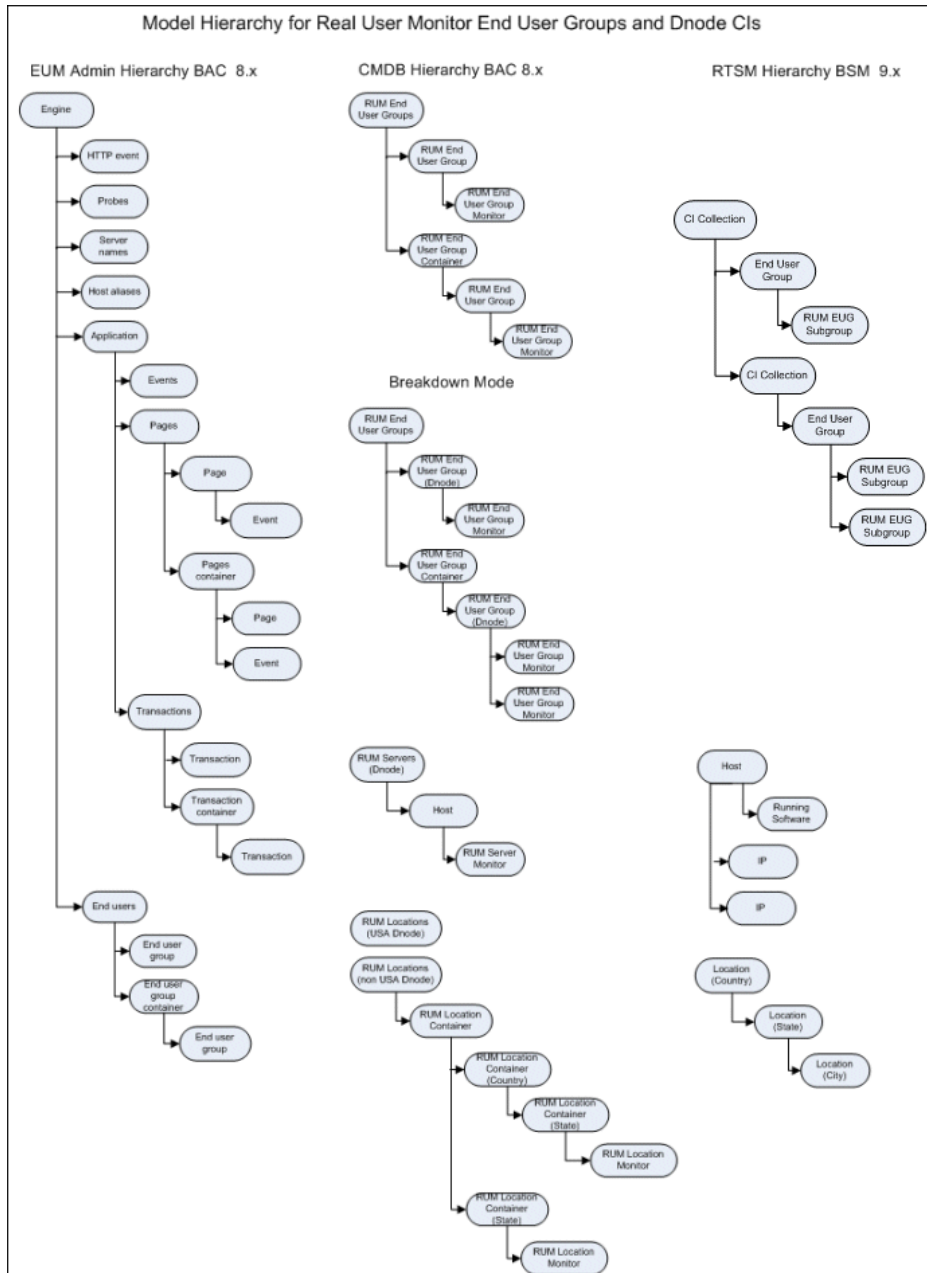
Schema

The following graphics show the Real User Monitor hierarchy in End User Management and the corresponding database entries for both the old (BAC 8.x) and new (BSM 9.x) models.

RUM Application and Associated Entities:



RUM End User Groups and Dnodes:



New CI Types

The major EUM CI types for Real User Monitor are replaced by new CI types in BSM 9.x. The following table shows the old CI types and the equivalent new CI types:

BAC 8.x CI Type	BSM 9.x CI Type
End User Management Application Related Group	CiCollection (only for those CIs that are part of an SLA)
Business Process Step	Business Transaction
RUM Page Monitor	Not used
RUM End User Group	CiCollection
RUM End User Group container	CiCollection
RUM End User Group Monitor	End User Subgroup
RUM Server Monitor	Running Software
Business Process Group	CiCollection
RUM End User Group	End User Group
All RUM events	Not used
All RUM related Dnodes	Not used
RUM Location container	Location

Note: After the upgrade old CI types remain in the model, but are obsolete and should not be used.

RUM Pages Upgrade

In BSM 9.x, RUM pages are managed differently than in BAC 8.x. In BSM version 9.x, RUM pages are managed in a page gallery for each application. The page gallery is a central area for configuring and managing an application's pages and it can contain a hierarchy of page folders. Pages can be attached to RUM transactions and can also be used to filter events.

In BSM 9.x, a page is no longer represented as an independent entity in the RTSM, but is now part of a transaction.

The upgrade process considers the following when upgrading RUM pages:

- ▶ For each application, a page gallery is created and the application's existing pages are placed in the gallery. If the pages were organized in page containers, the containers are converted to a folder hierarchy in the page gallery.
- ▶ Page containers are also added as a CI collection under the application. If a page container has the same name as a transaction container on the same hierarchical level, they are merged in to one CI collection.
- ▶ For each page in an application, the upgrade process checks if it is already included in a single page transaction. If not, a new single page transaction is created for the page. This results in a large number of transactions being created (which replace the 8.x page BP Steps).
- ▶ For pages that are marked for monitoring in 8.x only when they are part of a transaction, the upgrade process will check if they are included in an SLA. If not, it will not create a transaction for them.

RUM Events Upgrade

In BSM 9.x, RUM events are removed from the RTSM model and are considered RUM configuration item only. Also, events are only defined on the application level with the option to filter events by specific pages.

The upgrade process converts all RUM events to application level events. An event that was defined for a page is upgraded to application event with a filter for the specific page. An event that was defined for a page container is upgraded to an application event with a filter for the specific pages included in the container.

RUM Engine Details Upgrade

In BSM 9.x, the RUM engine is not part of the RUM configuration hierarchy as it was in previous versions. You can still view basic RUM engine and probe details in End User Management Administration (for example, names and IP addresses), but you cannot update this data.

The RUM engine and probe details are reported directly to BSM by the RUM engine registration process, and they are displayed in the End User Management Administration Settings tab. In the upgrade process, the relevant details are upgraded from the old system to the new as if they were registered by the RUM engine.

The following configurations (which were previously managed on an engine level, but are now managed on an application level) are moved by the upgrade process to each application monitored by a specific engine:

- ▶ Default page and transaction settings
- ▶ Data reporting settings
- ▶ Session reset settings
- ▶ Global HTTP Error events
- ▶ Host aliases

Note: Although in BAC 8.x the host aliases list was for an engine, and in BSM 9.x it is for an application, the upgrade process duplicates the entire engine host aliases list to each relevant application.

The following configurations are no longer managed in End User Management Administration:

8.x	9.x
Broken link referral settings	Automatically discovered by RUM engine
Server names	Change a server name by renaming the corresponding Node CI

Application Upgrade

If the upgrade process determines that an application name is not unique, it renames the application to a unique name.

RUM Default Application Upgrade

In BSM 9.x there is no default RUM application. You can configure such an application manually if needed. If an engine configured to report data for unconfigured applications is being upgraded to BSM 9.x, a new RUM application is created with the following settings:

Setting	Value
Name	Default Application (on engine1)
IP Range	0.0.0.0—255.255.255.255 and port=80
Type	Web Application
Enable TCP	Off
All snapshot settings	Taken from the old engine's global settings
Host Aliases	Taken from the old engine's settings
Probes	All
Thresholds	Taken from the old engine's general settings
User Name detection	None
Parameter Extraction	None

Setting	Value
Page Discovery Configuration	Use defaults (that is, do not use a file and do not use the page title)
Session Identification	None
Session Reset	Use default (that is, 20 minutes and no URLs)
Session Properties	None
Data Collection - enable clickstream	True
Data Collection - frame unification	False
Sensitive Data	No sensitive data
Statistics Collection	Taken from the old engine's settings
Pages	None
Events	Create HTTP events based on the old engine's HTTP categories

This application is a regular RUM application and can be configured and managed like any other application in End User Management Administration.

Data reported using the old engine's default application ID is upgraded with the newly created application's RTSM ID.

RUM End User Group Upgrade

In BSM 9.x, end-user groups are no longer managed for a specific engine. When upgrading end-user groups, groups with the same names or with overlapping IP ranges are upgraded as follows:

- ▶ As end-user groups may have the same name under different engines, the upgrade process adds the engine name to the upgraded end-user group name (for example, eug1 (engine1)).
- ▶ If there are multiple end-user groups with identical IP range across multiple engines, they are merged into a single end-user group with the following, merged fields:
 - ▶ **Name.** Selected from one of the groups at random.
 - ▶ **Description.** Selected from one of the groups at random, if more than one description exists.
 - ▶ **Status.** If one of the merged end-user groups is active, the status is set to active.
 - ▶ **Monitoring conditions.** Selected from one of the groups at random.
 - ▶ **IP resolution.** Upgraded according to the following priority:
 - ▶ Single IP
 - ▶ CIDR mask (if two different masks exist, the higher one is selected)
 - ▶ RFC
 - ▶ According to ISP
 - ▶ Class C
 - ▶ Class B
 - ▶ Class A
 - ▶ As entered
 - ▶ **Latency.** The lowest value is selected.
 - ▶ **Host name resolution.** If one of the merged end-user groups is set to **true**, the new end-user group is set to **true**.

- ▶ **Physical location.** If only one of the merged end-user groups has a location, that location is used. If more than one group has a location, one of the locations is used at random.
- ▶ If there are end-user groups with intersecting IP ranges (which can occur only when there are more than two engines), the upgrade process upgrades one of the groups at random. For all the other groups a CI is created (without any configuration) so that historical data will still be available for them.

Note: Details of end-user groups that are not upgraded when merged or because of intersecting IP ranges are recorded in the EUM upgrader log file.

RUM Locations Upgrade

In BSM 9.x, all locations discovered by RUM are reported to, and created in, the Location Manager in BSM. Location IDs are used instead of the BAC 8.x location string keys.

RUM Servers Upgrade

Servers detected by RUM are created in BSM 9.x as Nodes and Running Software CIs.

RUM Templates Upgrade

The following table shows the templates used when upgrading template based applications from BAC 8.x to BSM 9.x:

BAC 8.x Template	BSM 9.x Template
Citrix ICA Client	Citrix ICA
File Transfer Protocol	FTP
IMAP	IMAP
LDAP	LDAP

BAC 8.x Template	BSM 9.x Template
Microsoft SQL Database	MS SQL
Microsoft Terminal Server (RDP)	Microsoft Terminal Server (RDP)
MySQL	MySQL
Oracle DB	Oracle DB
Oracle Forms - NCA Over HTTP	Oracle Forms Over HTTP
Oracle Forms - NCA Over TCP	Oracle Forms Over TCP
POP3	POP3
RMI Registry	RMI Registry
SAP GUI	SAP GUI
Siebel 7.x, 8.0	Siebel 8.0
SMTP	SMTP
SSH	SSH
WebSpherePortal5	WebSphere Portal5
WebSpherePortal6	WebSphere Portal6

Troubleshooting and Limitations

This section includes the following troubleshooting and limitations for the End User Management Administration upgrade of Real User Monitor:

- "Container Names" on page 370
- "Page Container Descriptions" on page 370
- "Null Session ID in Session Identification" on page 370
- "Pages with Identical URLs" on page 370
- "Pages do not appear in Dashboard/SLM/CI Alerts" on page 370
- "Deleting an end-user group does not delete included subnets" on page 371
- "End-user group monitor CIs are not upgraded as part of an SLA" on page 371

- ▶ "Data for servers discovered by RUM after the last daily aggregation is not upgraded" on page 371
- ▶ "Multiple capturing groups in regular expressions defined for masking sensitive data are not upgraded" on page 372
- ▶ "Extra CIs are created for some end-user group subnets" on page 372

Container Names

Top level containers in BAC 8.x (that is, containers defined directly in the EUM Administration tree) are upgraded to BSM 9.x CI collections of the same name, but with a suffix of **-EUM**. For example, a BAC 8.x container called Container1 is upgraded to a BSM 9.x CI collection called Container1-EUM.

Page Container Descriptions

Page containers, which can have descriptions, are upgraded to folders in the page gallery, which do not have descriptions. Therefore, page container descriptions are not upgraded.

Null Session ID in Session Identification

In BSM 9.x, you cannot configure session identification with an empty session ID value. Session identification configurations with empty session ID values are not upgraded.

Pages with Identical URLs

If an application includes two pages with identical URLs, only one of the pages is upgraded. If a transaction includes the non upgraded page, it is updated to include the upgraded page instead.

Pages do not appear in Dashboard/SLM/CI Alerts

Pages in BAC 8.x are replaced by transaction in BSM 9.x and therefore no longer appear in Dashboard, SLM, CI Alerts, or other CI oriented applications.

Deleting an end-user group does not delete included subnets

When you delete an end-user group that contains subnets, that was created in an earlier version of BSM and was upgraded to version 9.1x, the included subnets are not deleted.

Workaround: In the upgraded BSM 9.1x system, run the `rum_eug_subnet_change_link` enrichment in RTSM Administration. For details on enrichment, see "Enrichment Manager" in the *RTSM Administration Guide*.

End-user group monitor CIs are not upgraded as part of an SLA

When upgrading in stages from BAC 7.x to BSM 9.x (that is, upgrading from BAC 7.x to BAC 8.x and then from BAC 8.x to BSM 9.x, RUM CIs created by RUM Dnodes (that is, RUM end-user, RUM server, and RUM location monitors) are removed from the model and the following limitations apply to them:

- The CIs will no longer be included in upgraded SLAs.
- CI status alerts defined on these CIs will no longer exist.
- Any Dashboard customization made on these CIs no longer exists.

Data for servers discovered by RUM after the last daily aggregation is not upgraded

When upgrading to BSM 9.x using staging (SDR), any data for servers discovered by RUM since the last daily aggregation included in the Data Transfer tool is not upgraded. For example, if you configure the Data Transfer tool to include data as of 00:30 for a specific date, data for a server discovered by RUM at 02:00 on the same date is not upgraded.

Multiple capturing groups in regular expressions defined for masking sensitive data are not upgraded

When you configure regular expressions (regex) for masking sensitive data for a RUM application, you can include multiple capturing groups (that is, there are multiple places in the regex to mask the data). When such regular expressions are upgraded to BSM 9.x, the multiple capturing groups are not upgraded and either none of the capturing groups, or only the first one, are applied to the upgraded regex.

Solution: Create multiple regular expressions, each with one capturing group only.

Extra CIs are created for some end-user group subnets

If you configured an end-user subgroup in BAC 8.x and either the end-user group name contains a period, or you selected an IP resolution of **Single IP** or **According to ISP**, during the upgrade a new CI is created for the subgroup with the CI name comprising the end-user group name, the name of the RUM engine on which the subgroup is monitored, and the subnet IP range. Historical data for the subnet is upgraded to this new CI.

When the RUM engine is connected to the upgraded BSM 9.x system, it creates another CI for the subnet and new RUM data that is acquired is displayed for this new CI. The new CI's name is either a host name or IP address for Single IP, and an ISP name for According to ISP.

EUM Alerts Upgrade

For details of the changes to EUM alerts that are made as part of the End User Management Administration upgrade, see "Alerts Upgrade Information" on page 287.

CI Links Upgrade

Many CI types used in End User Management are replaced by new CI types in BSM 9.x. The upgrade process moves all the customized links you created on CIs in BAC 8.x to the new CIs created in BSM 9.x. For example, if you linked a Business Process Group to a business service, the upgrade process links the corresponding business transaction flow to the same business service.

Note: Links created on monitor CIs in BAC 8.x are not copied to BSM 9.x.

Views Upgrade

Note: For details on view upgrades in BSM, see "Dashboard and My BSM Upgrade Information" on page 257.

The EUM upgraders upgrade End User Management user defined pattern views and perspectives.

This section includes the following topics:

- "Custom Pattern Views" on page 374
- "Perspective Based Views" on page 375
- "Predefined EUM Views" on page 376
- "Troubleshooting and Limitations" on page 376

Custom Pattern Views

When upgrading custom pattern views, the EUM upgraders do the following:

- For old CI types that have a direct, corresponding new CI type, the upgrade process makes a one to one replacement in all TQLs. For example, all BP Step CIs in a TQL are replaced by Business Transaction CIs.
- TQLs that contains EUM Monitor CI types are upgraded as follows:
 - The parent of the monitor node in the TQL is set with an attribute condition of `monitored_by=BPM` or `monitored_by=RUM`, depending on the monitor type.
 - The monitor CI is removed from the TQL and view definition.

Perspective Based Views

Perspective based views are composed of a perspective (TQL) and specific CI instances. The CI instances may be the instance of a model or CI Collection.

When upgrading perspective based views, the EUM upgraders do the following:

- For Model CI IDs or CI collections that include CI types that have a direct, corresponding new CI type, the upgrade process makes a one to one replacement. For example, a Business Process Step is replaced by a Business Transaction.
- EUM breakdown CIs are replaced by a corresponding CI that is filtered by the location of the original CI. The following table shows the breakdown CIs in BAC 8.x and their corresponding CIs in BSM 9.x:

BAC 8.x CI	BSM 9.x CI (filtered by the location of the original CI)
BP Group from Location	Business Transaction Flow
BPM Transaction from Location	Business Transaction
Location	Application

- Views based on the **Location based monitors** perspective are upgraded to the **End User Monitors** perspective (the Location based monitors perspective is removed in 9.x).
- Any view that was set with breakdown information is set as a Local Impact View (LIV). For details on LIV views, see "View Builder Overview" in *Using Service Health*.

Note: Alerts on CIs in such views are not upgraded to the LIV and therefore, are not accessible through the LIV.

Predefined EUM Views

The following table lists the BAC 8.x predefined EUM views and the BSM 9.x views to which they are upgraded:

BAC 8.x View	BSM 9.x View
End User Location	Deprecated
All RUM Monitors	Deprecated
End User Monitors	End User Monitors
Real User Servers	RUM Servers
Real User Locations	End User Locations
Real User End Users	RUM End Users
Real User Applications	End user Applications

Troubleshooting and Limitations

This section includes troubleshooting and limitations for the End User Management Administration upgrade of Views.

- ▶ Custom Pattern View TQLs that contain only monitor CIs without parents are not upgraded.
- ▶ Custom Pattern View TQLs that contain subgraphs and compound links are not upgraded.
- ▶ Custom Pattern View TQLs that include a node property condition with IDs of EUM CIs that were removed (for example, monitors or `bp_group_from_location`) are not upgraded.
- ▶ Custom pattern views that include breakdown CIs (for example, BPM Transaction from Location) are not upgraded to the new Service Health local impact views that support breakdown in BSM 9.x.

Deleted CIs

As part of the upgrade, CIs of deprecated CI types are deleted, unless they are included in an SLA. The following are the EUM CI types that are deprecated:

- bp_group
- bp_group_location
- bp_step
- bpm_tx_from_location
- end_user_related_group
- rum_end_user_group
- rum_end_user_group_container
- rum_end_user_groups
- rum_end_user_group_monitor
- rum_errors
- rum_app_error_monitor
- rum_http_error_monitor
- rum_info_events
- rum_info_event_monitor
- rum_loc_monitor
- rum_app_session_monitor
- rum_tx_monitor
- rum_page_monitor
- rum_server_monitor
- rum_locations
- rum_servers

After the CIs of the above CI types have been deleted, the upgrade process removes the following CI class definitions.

- bp_group
- bp_group_location
- bp_step
- end_user_related_group
- rum_end_user_group
- rum_end_user_group_container
- rum_end_user_groups
- rum_errors
- rum_info_events
- rum_locations
- rum_servers

Note: A CI class definition is removed only if all its CI instances were deleted.

Permissions Upgrade

In BSM 9.x, permissions are on an application level, except for downtime permissions. Downtime permissions are on a global level so that a user with permissions to create downtime can do so for all applications.

The following table shows the upgraded permissions and roles:

BAC 8.x	BSM 9.x
Permissions	
BPM Profile	BPM configuration for the application created for the profile
RUM Application	RUM configuration for the Application CI
Script Repository Folder	Script Repository folder and all children folders
Profile > Monitor Profile > Transaction	None - obsolete permission
RUM End user RumGeneralSettings	None - obsolete permission
MonitoringFilter MonitoringContainer	None - obsolete permission
All other entity permissions	Unchanged
Roles	
Profile Administrator	BPM Administrator
Profile User	BPM Viewer

EUM Reports Upgrade

This section describes the changes to End User Management reports in BSM 9.x, as well as limitations to upgraded report data.

This section includes the following topics:

- "Changes to End User Management Reports" on page 380
- "Limitations for Upgraded Data in Reports" on page 382
- "Limitations for Reports Using Upgraded Real User Monitor (RUM) Data" on page 386
- "General Limitations" on page 387
- "Reports Mapping" on page 388

Changes to End User Management Reports

The following table lists the major changes to EUM reports that occur after upgrading your system to BSM 9.x.

Functionality	BAC 8.x	BSM 9.x
Filter transactions/locations /groups out of all reports for all users	Exclude entities in Admin > Platform > Profile entity maintenance.	Include entities in the Favorite filter. Include only the items you want to see and save as public. Note: If you add a transaction to an application and want to include it in reports, you must manually add it each relevant filter.
Filter transactions/locations /groups out of reports for specific users	Exclude entities in Admin > End User Management > Reports > Report filters.	Include entities in the Favorite filter. Include only the items you want to see and save as private. Note: If you add a transaction to an application and want to include it in reports, you must manually add it each relevant filter.

Functionality	BAC 8.x	BSM 9.x
Delete transactions/locations /groups permanently from reports	Set in Admin > Platform > Profile entity maintenance.	Delete the relevant CI. Note: If you want to keep historical data (that is, make a soft delete), delete the monitoring configuration in End User Management Administration, but do not delete the CI. If the CI is available, its data can be viewed in reports.
Deleting transaction/location	Still available in reports, but does not exist in EUM configuration.	Still available in reports if only configuration is deleted. Not available in reports if the CI is deleted.
Performance status calculation rule	Based on average of values.	Based on average of statuses. The old rule still exists for backward compatibility and you can configure the system to use it instead of the new rule. For concept details, see "Status Aggregation Rules Overview" in <i>Using End User Management</i> .
BPM threshold changes	Changed retroactively.	Not changed retroactively.
Profile/Application summary data	Calculated from all transactions, including deleted transactions (if not filtered).	Calculated only from existing business transactions. Deleted transactions are not included.
Number of actions and requests displayed in reports	A separate value is displayed for both actions and requests.	A separate value is displayed for both actions and requests, but the number of actions may be a combination of both actions and requests.

For details on upgrading custom reports and changes in report names, see "Reports Upgrade Information" on page 249.

Limitations for Upgraded Data in Reports

The following table lists various limitations to End User Management report data that was upgraded from BAC 8.x, or that was acquired by BSM 9.x while in staging mode during an upgrade to BSM 9.x. (Data acquired after completing an upgrade to BSM 9.x is not affected.)

Report	Description
<p>All reports</p>	<ul style="list-style-type: none"> ▶ Synthetic user (BPM) data may be different as BSM 9.x uses a combination of aggregated and raw data to obtain a more exact picture, whereas BAC 8.x uses either aggregated or raw data (whichever gives most data for the report time period). ▶ Large time frames are rounded to optimize report performance for all reports. In BAC 8.x, this was done only for RUM reports. This means that synthetic user (BPM) report data may vary when you compare BSM 9.x and BAC 8.x reports. ▶ RUM data for transactions, pages, and end-user groups deleted in BAC 8.x are not upgraded. Reports that include these, or related entities, may differ between BAC 8.x and BSM 9.x, even if generated for the same dates and applications. ▶ RUM data for new subnets, locations, and servers that are detected while BSM 9.x is in staging mode do not appear in BSM 9.x End User Management reports. Such entities will only be added to the BSM 9.x production system if they are detected and reported by RUM after moving from staging mode to production mode (and data reported during the staging mode will not be available).
<p>RUM Tier Summary Tiers Over Time RUM Application Infrastructure Summary Application Infrastructure Over Time</p>	<ul style="list-style-type: none"> ▶ The Action Availability percentage may be slightly different than in BAC 8.x due to a different method of calculation. ▶ You cannot filter the report by end-user group or subgroup. If you set such a filter, no data is returned. ▶ Response time breakdown in the Action tab is empty. You can view response time breakdown in the Request-Response tab, which is hidden by default. For details on how to display the Request-Response tab, see "Displaying the Request-Response Tab in Reports" on page 386.

Report	Description
RUM End User Group Summary	<ul style="list-style-type: none"> ▶ You cannot filter the report by server or software element. If you set such a filter, no data is returned. ▶ Response time breakdown in the Action tab is empty. You can view response time breakdown in the Request-Response tab, which is hidden by default. For details on how to display the Request-Response tab, see "Displaying the Request-Response Tab in Reports" on page 386. ▶ Latency information is only available for TCP data.
RUM End User Group Over Time	<ul style="list-style-type: none"> ▶ You cannot filter the report by server or software element. If you set such a filter, no data is returned. ▶ Response time breakdown in the Action tab is empty. You can view response time breakdown in the Request-Response tab, which is hidden by default. For details on how to display the Request-Response tab, see "Displaying the Request-Response Tab in Reports" on page 386.
Application Health	<p>You cannot filter the report by end-user group or subgroup. If you set such a filter, no data is returned in the following components:</p> <ul style="list-style-type: none"> ▶ Load and Availability Over Time ▶ Load and Performance Over Time ▶ End-user group/Server/Location Distribution
Location Summary	<p>All session data is displayed for an unknown location, instead of real locations.</p>
RUM Action Summary	<p>In BSM 9.x, data is grouped by action description instead of by action ID (which was used in BAC 8.x). If an action's description was changed during the report time period, data is displayed for each description separately.</p> <p>Tip: Use the tooltip to display the action's full description to help correlate the data.</p>

Report	Description
Triage	<ul style="list-style-type: none"> ▶ In BSM 9.x, the Triage report uses aggregated data when available, and then uses raw data to complete the report. In BAC 8.x, only raw data is used. This may lead to differences in report data for reports generated in BSM 9.x and BAX 8.x, for the same time period. <p>Tip: Generating the report for a time period of one hour or less uses raw data in both BSM 9.x and BAC 8.x.</p> <ul style="list-style-type: none"> ▶ After upgrading to BSM 9.x, the Transaction by Location component of the Triage report displays an incorrect status for collector health. The correct collector health status is displayed only when you regenerate the report after the relevant BPM machine has been reconnected to, and started communicating with, the upgraded BSM 9.x system.
BPM WebTrace	<p>If an application includes multiple WebTraces to the same host, but for different ports, all the data is displayed for one port only (selected randomly) and for the other ports, no data is displayed. (In BAC 8.x, data is not broken down by port at all.)</p>
RUM Event Summary	<p>In BAC 8.x, when you generate the Event Summary report for a period more than 2 weeks old, only events for undefined pages are included. In BSM 9.x, when you generate the RUM Event Summary report for the same period, all events are included.</p> <p>This means that you will see data for more events in the BSM 9.x RUM Event Summary report than in the BAC 8.x Event Summary report generated for the same dates.</p>

Displaying the Request-Response Tab in Reports

By default, the Request-Response tab is not displayed in End User Management reports in BSM 9.x, but you can configure BSM to display this tab.

To modify the Request-Response tab display setting, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

- ▶ Select **Applications**.
- ▶ Select **End User/System Availability Management**.
- ▶ In the **Display** table, locate the **Display Request tab** entry. Change the value to **true**.

Limitations for Reports Using Upgraded Real User Monitor (RUM) Data

The following table lists various limitations to End User Management reports that use upgraded, raw RUM data that is obtained directly from RUM. Raw data is kept by RUM for a period of two weeks, so these limitations apply to reports generated during, and for the time period of, two weeks after the upgrade.

Report	Description
All reports	<ul style="list-style-type: none"> ▶ You cannot filter a report by multiple subgroups. If you select multiple subgroups in the filter, only one of the selected subgroups (at random) is used. ▶ Historical data on pages with meaningful page names assigned by RUM (on versions earlier than RUM 9.00) is not upgraded. Such pages may be automatically discovered by RUM 9.x, with data being collected for them on an ongoing basis. ▶ Servers for which no IP address is available in BAC 8.x, and end-user groups that were deleted in BAC 8.x, are not included in BSM 9.x reports.
Session Replay Page	Snapshots are not available.

Report	Description
RUM Action Summary	You cannot filter the report by transaction, end-user group or subgroup, event, or location. If you set such a filter, no data is returned.
RUM Transaction Summary	You cannot filter the report by transaction with threshold violation, or by end-user group or subgroup. If you set such a filter, no data is returned.
Application Performance Lifecycle reports	You cannot filter the report by transaction with threshold violation. If you set such a filter, no data is returned.
RUM Session Analyzer	RUM sessions that were open during the time of the upgrade will either not be included in the report at all, or will be included as closed sessions.

General Limitations

This section includes general limitations for End User Management reports.

Comparing BPM Reports Between BAC 8.x and BSM 9.x

When comparing BPM reports between BAC 8.x and BSM 9.x, the time zone for the BSM 9.x user should be set to the same time zone configured for the BSM 9.x server machines.

User Unable to Open the EUM Reports Application Filter

In BSM 9.x, a user who has permission to view EUM reports, but does not have any permissions on RTSM views (that is, he cannot open System health, SLM, or RTSM), is unable to open the EUM reports Application filter.

Workaround: Grant the user view permissions for RTSM views containing the applications to be shown in reports.

Reports Mapping

The following table lists the BAC 8.x End User Management reports and their equivalent report in BSM 9.x:

BAC 8.x Report	BSM 9.x Report	Comments
Status Snapshot	Status Snapshot	
Multi-Profile Summary	<ul style="list-style-type: none"> ▶ No exact replacement, although the BPM Performance Status report includes most of the functionality, apart from alerts information. ▶ Location Performance component functionality is available in the Location Summary report. ▶ Profile Performance functionality is available in the Application Summary report. 	
Single Profile Summary	<p>No exact replacement, although the Application Health report includes most of the functionality. Other reports that include different parts of the functionality are:</p> <ul style="list-style-type: none"> ▶ Performance Analysis ▶ BPM Performance Status ▶ Location Summary ▶ Application Summary ▶ Alert reports 	

BAC 8.x Report	BSM 9.x Report	Comments
Performance Matrix	BPM Performance Over Time	
Triage	Triage	
Triage Raw Data	Triage Raw Data	
Availability Over Time	Metrics Over Time	Select the BPM Availability metric. If you use this frequently, save a favorite filter that includes the application, the metric, and other required filters.
Response Time Over Time	Metrics Over Time	Select the BPM Duration metric. If you use this frequently, save a favorite filter that includes the application, the metric, and other required filters.
Transaction Analysis	BPM Performance Over Time	Group by Transaction.
Error Summary	BPM Error Summary	Outlier information is available only in the BPM Performance Status report.
Location Analysis	BPM Performance Over Time	Group by Location. You can also review location performance in the Location Summary report.

BAC 8.x Report	BSM 9.x Report	Comments
Breakdown Over Time	No exact replacement. The following reports include a Breakdown Over Time component: <ul style="list-style-type: none"> ▶ Performance Analysis ▶ Triage ▶ BPM Performance Over Time 	
Breakdown Summary	Performance Analysis	
Transaction Breakdown Raw Data	Performance Raw Data	The Performance Raw Data report is reached by drilling down from the Performance Analysis report.
Component Breakdown (as a drill down from the Transaction Breakdown Raw Data report)	Page Component Breakdown	The Page Component Breakdown report is reached by drilling down from the Performance Raw Data report.
Min/Max Response Time	BPM Performance Status	
Response Time by Percentile	BPM Response Time by Percentile	
Global Statistics	RUM Global Statistics	
Page Summary	RUM Action Summary	
End Users by Page	RUM End User Group by Action	Available by drilling down from the RUM Action Summary report.
Page Over Time	Action Over Time	Available by drilling down from the RUM Action Summary report.
Event Summary	RUM Event Summary	
Event Analysis	Event Analysis	

BAC 8.x Report	BSM 9.x Report	Comments
Servers by Page Summary	Application Infrastructure by Action	Available by drilling down from the RUM Action Summary report.
Session Analyzer	RUM Session Analyzer	
Transaction Summary	RUM Transaction Summary	
End Users by Transaction	RUM End User Group by Transaction	Available by drilling down from the RUM Transaction Summary report.
Transaction Over Time	Transaction Over Time	Available by drilling down from the RUM Transaction Summary report.
End User Summary	RUM End User Group Summary	
End User Over Time	RUM End User Group Over Time	
Unconfigured End User by Country/State	This functionality exists in the RUM End User Group Summary report.	
End Users by Page	RUM End User Group by Action	
Server Summary	RUM Application Infrastructure Summary	
Server Over Time	Application Infrastructure Over Time	
Pages by Server Summary	This functionality exists in the RUM Action Summary report.	
TCP Poor Requests Summary	TCP Poor Requests Summary	

Chapter 23 • End User Management Upgrade Information

BAC 8.x Report	BSM 9.x Report	Comments
TCP Requests Analyzer	TCP Requests Analyzer	
Event Count Over Time	This functionality exists in the RUM Event Summary report.	
TCP Application Summary	RUM Tier Summary	
TCP Application Over Time	Tiers Over Time	
Network Analysis	BPM WebTrace	
WebTrace by Location	BPM WebTrace	
Page Component Breakdown	BPM Page Component Breakdown on Demand	

Post Upgrade Actions

After you have run the End User Management Administration upgrade, there are a number of different actions you should perform.

This section includes the following topics:

- "Required Actions" on page 393
- "Recommended Actions" on page 395
- "Validations" on page 395

Required Actions

After the upgrade, you must perform the following actions:


- Redirect Business Process Monitor instances to the new BSM Gateway Server. For details, see "Redirecting Business Process Monitor Instances" on page 394.
- For BPM profiles upgraded to applications, manually reconfigure the correct time zones. A configuration file was used to map time zone offsets (used by the old model) and time zone IDs (used by the new model). The first time zone ID that matched the time zone offset was used.
- Copy any user defined RUM templates (that is, templates you created manually for RUM applications) from the **<HPBAC root directory>\conf\rum_templates** directory on the old BAC Gateway Server, to the **<HPBSM root directory>\conf\rum_templates** directory on the new BSM Gateway Server.

Redirecting Business Process Monitor Instances

After you have run the HP Business Service Management upgrade wizard in Staging mode, you must redirect each Business Process Monitor instance to report to the HP Business Service Management Gateway Server.

You can redirect all Business Process Monitor instances simultaneously, using the Business Process Monitor redirect tool, as described below, or you can redirect each Business Process Monitor instance separately by editing each instance within Business Process Monitor Admin. For details on editing a Business Process Monitor instance within Business Process Monitor Admin, see "Instance Page User Interface" in the *Business Process Monitor Administration* PDF. It is recommended that you use the Business Process Monitor redirect tool to redirect your Business Process Monitor instances.

To redirect Business Process Monitors instances using the redirect tool:

- 1** Extract the files within the **<HP Business Service Management server root directory>\tools\RedirectTool.zip** file to a directory on a machine that has access to the Business Process Monitors whose instances you want to redirect.
- 2** In HP Business Service Management, select **Admin > End User Management > Settings > Business Process Monitor Settings > BPM Agents**. The list of Business Process Monitors from your previous BAC system is displayed.
- 3** Select the Business Process Monitor instances you want to redirect and click the **Export Business Process Monitor Agent Information for the Redirect Tool**  button. Save the file to a machine with access to the machine on which the RedirectTool.zip files are located.
- 4** In the **<RedirectTool installation directory>\conf\BPMRedirectTool.properties** file, specify the following parameters:
 - **NEW_BAC_URL**. The URL of the HP Business Service Management Gateway Server.
 - **INPUT_FILE_PATH**. The directory in which you saved the export file. Include the name of the file itself as well. For example:
D:\\Tools\RedirectTool\BPMList.txt
 - **USER**. The user name required to access the Business Process Monitors. (A user name is generally not required.)

- ▶ **PASSWORD.** The password required to access the Business Process Monitors. (A password is generally not required.)
- 5** Run the <RedirectTool installation directory>\RedirectTool.bat file. The Gateway Server URL is updated on all the Business Process Monitor instances. A log file containing information on each updated Business Process Monitor instance is created. If the redirect tool failed to update a Business Process Monitor instance, this information is included in the log file.

Recommended Actions

After the upgrade, it is recommended to perform the following actions, to better utilize the new 9.x model:

- ▶ Unify BPM and RUM locations in the Location Manager. For concept details on the Location Manager, see "Location Manager Overview" in *Platform Administration*. Also, configure geographical coordinates for the locations so that they will appear in the geographical map in the Location Summary report.
- ▶ Create Local Impact Views (LIV) to replace any views that included transaction location breakdown. For details on LIV views, see "View Builder Overview" in *Using Service Health*.

Validations

Verify that the following have been correctly upgraded:

- ▶ Custom reports and favorite filters.
- ▶ Events and page CI alerts (upgraded to event based alerts).
- ▶ End-user groups and their IP ranges.
- ▶ CI status alerts on BPM breakdown CIs.
- ▶ Custom EUM related views (both pattern and perspective based).

24

SiteScope and System Availability Management Upgrade Information

This chapter includes:

- ▶ SiteScope and System Availability Management Upgrader on page 397

SiteScope and System Availability Management Upgrader

The upgrade for SiteScope/System Availability Management is part of the Configuration upgrade stage of the BSM upgrade wizard.

Upgrade Compatibility

When upgrading from BAC to BSM 9.10, you can perform the upgrade with SiteScope version 9.5 or later connected.

However, before redirecting SiteScope to BSM 9.10, you must upgrade to SiteScope 10.10 or later, since versions of SiteScope earlier than 10.10 are not supported by BSM 9.1x.

Troubleshooting - If the Upgrader Fails:

Make sure that the following content packs had been deployed on the environment: **HPOprInf**, **HPOprJEE**, **HPOprMss**, and **HPOprOra**.

What Changed in BSM 9.x

The table describes what changed between the BAC 8.x and BSM 9.x versions, and describes how the upgrade handles the changes.

Topics	BAC 8.x	BSM 9.x
Topology changes		For details, see "Changes to CIs and to Topology" on page 238
Monitors CIs were removed from out-of-the-box views except for the System Monitors view		
A monitor is connected to more than one CI (not supported)		For details, see "SiteScope Monitors Associated with Non-default CIs or Multiple CIs" on page 282.
CI status alerts defined in your pre-upgrade environment		For details, see "CI Status Alerts Upgrade" on page 268.
System Availability Management configuration (automatically upgraded)		The topology reported by SiteScope match the RTSM. The data reported by SiteScope matches the new Health Indicator model.
Customized KPI assignments in SiteScope and EMS integrations (automatically upgraded + manual procedure)		TO DO: For details, see "Manual Procedure" on page 399.

Topics	BAC 8.x	BSM 9.x
Differentiating between the name and the data source of the EMS integration	Only the name of the data source, which also serves as the name of the integration, is saved to the integration.	<p>The name of the EMS integration and the name of the data source can be different.</p> <p>In BSM 9.x, you can separately enter the name and the data source of the integration in the Name and Data Source boxes in the Edit Integration dialog box. During the upgrade, for integrations which are not out-of-the-box (NetScout, HP Service Manager, and HPOM integrations), the name of the integration is copied to the new Data Source field. For details, see "Edit Integration Dialog Box" and "Add Integration Dialog Box" in <i>Solutions and Integrations</i>.</p>
KPIs modified in your pre-upgrade environment		For details, see "KPI Upgrade" on page 262.
KPI assignments associated with Custom KPIs		For details, see "SiteScope KPI Assignments Associated With Custom KPIs" on page 275.

Manual Procedure

Once the upgrade is performed, you must perform the following steps:

- 1** Go to the SiteScope BSM integration preferences and do a redirect to the server on which BSM 9.1x is installed. For details, see "Redirecting SiteScopes" on page 400.
- 2** Restart SiteScope.

- 3 Go to the SiteScope BSM integration preferences (as described in step 2a below), and click **Re-Synchronize** in the **BSM Integration Main Settings** section. The result is that the topology is updated according to the BSM 9.1x class model. For details, see "BSM Integration Preferences Dialog Box" in *Using SiteScope*.

Redirecting SiteScopes

You must ensure that your SiteScopes are pointing to the correct Gateway Server URL so that they can communicate with the BSM 9.1x Gateway Server.

To redirect a SiteScope:

- 1 In BSM 9.1x, select **Admin > System Availability Management** and click the SiteScope whose Gateway Server URL you want to update.
- 2 In SiteScope:
 - a Select **Preferences > Integration Preferences**, double-click **BSM Integration on <SiteScope>**, and in the **BSM Integration Preferences** dialog box, expand the **BSM Integration Main Settings** section.
 - b In the **Business Service Management machine name/IP address** box, enter the name of the HP Business Service Management 9.1x Gateway Server. Click **OK** at the bottom of the Integration Preferences page.

Caution: If you have multiple SiteScopes, you can use the Global Search and Replace wizard to perform the update simultaneously on all your SiteScopes. For details on using Global Search and Replace, see the Using System Availability Management portal in the HP BSM Documentation Library.



- 3 To modify the SiteScope's settings within BSM, select the SiteScope in System Availability Management and click the **Edit SiteScope** button. Under **Distributed Settings**, enter the name of the HP Business Service Management 9.1x Gateway Server in the **Gateway Server name/IP address** box, as well as the user name and password required to access the Gateway Server in the **Gateway Server authentication user name/password** boxes. Click **Submit** at the bottom of the page.

Troubleshooting

If you need to troubleshoot the upgrade procedure, open the following logs in debug mode:

- `<BSM_profile_database_server>\log\upgrade\sampleEnrich.upgrade.log`. This log provides information about the monitors and measurements for which the upgrader failed.
- `<BSM_profile_database_server>\log\EJBContainer\aims.ejb.log`. This log contains advanced information on the process performed on the monitors and measurements in the upgrade flow.

Notes and Limitations

Downtime functionality in SiteScope 10.x or earlier is not supported when connected to BSM 9.x, since a new downtime cannot be created on a SiteScope profile. Previously defined downtimes in BSM 8.x upgraded to BSM 9.x do not affect SiteScope.

Workaround: To enable SiteScope support for the new downtime functionality when using BSM 9.x, upgrade your version of SiteScope to 11.x.

25

Upgrading Business Process Insight

This chapter includes:

- What Changed For BPI From 8.x to 9.x on page 403
- Upgrading BPI Overview on page 405
- Upgrade Notes on page 406
- Tasks to Complete Before Starting the BPI Server Upgrade on page 407
- Upgrading BPI From 8.x to 9.10 on page 410
- Upgrading BPI From 9.10 to 9.12 on page 422

What Changed For BPI From 8.x to 9.x

This section describes what changed in BSI from 8.x to 9.x.

- Terminology changes

The following table lists the BPI terminology changes from 8.x to 9.x:

Terminology in 8.x:	Changed in 9.x to:
➤ Business Process Step ➤ process step	Business Activity
step	Activity
Start Step	Start Activity
End Step	End Activity
active Step	Business Activity
Active step instances	Business Activity instances

Terminology in 8.x:	Changed in 9.x to:
Business Process Monitor CI	Business Process CI
<ul style="list-style-type: none"> ▶ Duration Monitor CI ▶ BPI Value Monitor CI ▶ BPI Custom Monitor CI in BAC Dashboard and My BSM	Business Process Scope CI in BSM Service Health and MyBSM
flowmap in BPI Health page, BAC Dashboard and My BSM	Business Process Diagram in BPI Health page, BSM Service Health, and MyBSM
flow	process

- ▶ Business Process modeling and run time improvements
 - ▶ Process data retention through multiple deployments
 - ▶ Grouping of Business Process data
 - ▶ User interface for Business Process Activity icon customization
 - ▶ Support for per business process permissions
- ▶ BPI / TV integration improvements and drilldowns
 - ▶ Business Transactions related to Business Process Activities regardless of progression rule type
 - ▶ Drill down to specific Business Transaction instance Transaction Tracking report from the Business Process Instance report
 - ▶ Display Business Transactions related to Business Process Activities in the Business Process Diagrams
- ▶ BSM 9.x-related updates
 - ▶ Support for new BSM 9.x Run-Time Service Model (RTSM) model, health indicators (HIs)
 - ▶ Integration with HP Business Service Management licensing and support for Autopass
 - ▶ MyBSM support

- ▶ Late-arriving data sample updates
 - ▶ Database schema creation using scripts and with non-database administrator privileges

Upgrading BPI Overview

You complete the BPI Server upgrade after Business Service Management has been upgraded in production environment mode to 9.12, by installing BPI Server version 9.12 over your existing BPI version 9.10.

There are two upgrade paths for BPI: from 8.x to 9.10 and from 9.10 to 9.12. Upgrades from versions of BPI prior to 8.x are not supported — you must upgrade your BPI system to version 8.x before proceeding with the upgrade process.

Note: If you want to install the same version of BPI to repair your installation, you need to follow the instructions in the "Re-Installing BPI Server Components" chapter of the *Business Process Insight Server Administration Guide* that cover re-installation for the correct version of BPI.

Upgrading BPI After a BSM Direct Upgrade

The BPI Server can only be upgraded after the BSM direct upgrade to 9.12 is completed and BSM is operating in production mode. Upgrading directly refers to installing the new version on the same servers and database schemas as the original version. BPI does not support a staging upgrade method.

- ▶ The BPI 8.x or 9.x system must be shut down before BSM is upgraded by either upgrade method. For more information, see "Tasks to Complete Before Starting the BPI Server Upgrade" on page 407.
- ▶ For details on upgrading BSM for either upgrade method, see "Staging vs. Direct Upgrade" .
- ▶ For instructions on upgrading BPI, see "Upgrading BPI From 8.x to 9.10" on page 410 and "Upgrading BPI From 9.10 to 9.12" on page 422.

Upgrade Notes

Before you start the upgrade process, you need to be aware of the following:

- ▶ Installation defaults.

With the exception of defining the BSM Gateway Server and credential details, all existing settings for your BPI configuration are used as a default for the installation.

- ▶ Following the upgrade to BPI version 9.12, any processes that were being tracked in the Business Impact Engine continue to be tracked and any CIs that you have linked to your Business Process will continue to be monitored.
- ▶ Following the upgrade to BPI version 9.12, all processes in the Modeler remain in the same state (deployed and undeployed) as they were before the upgrade.
- ▶ When you redeploy a new version of a Business Process or Data definition in version 9.12, BPI preserves any existing instances. Subsequent events for both existing and newly created instances are handled by BPI according to the modified definition.

On redeployment you have the following options:

- Replace the existing definition.

This replaces the definition and preserves all existing instances of the definition. Any statistical information collected for the instance is retained.

- Deploy under a different name.

This enables you to deploy the definition using a different name. Any previously deployed version of the definition and instances are left unchanged.

- When upgrading to BPI 9.10, legacy (pre-upgrade) BPI process instance data generated by TransactionVision does not show transaction data before or after the upgrade. However, all new process instances generated by TransactionVision after the upgrade will show transaction data if it is available. If you want to reuse your legacy (8.x) business models that use TransactionVision as a datasource, be sure to perform the post-upgrade procedure "Update the BPI Instance Database if TransactionVision is a Datasource for a Business Model" on page 414.

Tasks to Complete Before Starting the BPI Server Upgrade

Before starting the BPI upgrade, make sure that you have completed the following tasks as appropriate:

- "Check the BPI Database Table Use When Upgrading From BPI" on page 408
- "Copy Changed Component Configuration Files" on page 408
- "Back Up Your System" on page 409
- "Shut Down Your BPI System" on page 409
- "Wait Until the BSM Upgrade to Version 9.12 is Completed and BSM is in a Production Environment Mode" on page 410

1 Check the BPI Database Table Use When Upgrading From BPI

If you have created a database exclusively for your BPI Server data, then you can skip this section.

Note: You are strongly advised to configure a database or database user specifically for BPI to prevent any possibility of table name clashes.

If the database used by the BPI Server is also used for other applications, you need to check the list of table names that are created by the BPI upgrade process. If you have user-defined or application tables that have the same name as the predefined BPI tables, you need to remove them from the BPI schema (database), before starting the upgrade. If you do not, the upgrade process is likely to fail.

The list of schema objects created by the BPI upgrade process is listed in Appendix A, "Database Tables Defined for BPI" in the *Business Process Insight Server Administration Guide*. For schema object changes, see the BSM release notes.

2 Copy Changed Component Configuration Files

Before starting the upgrade process make sure that you copy and save off any files that you have modified while using the existing version of BPI and before starting the upgrade procedure. You can then reapply the changes to the installed files after the upgrade is complete.

Examples of files that you might have changed are configuration files and the SQL script for archiving Active and Deleted instances.

3 Back Up Your System

Before starting the upgrade, you are strongly advised to back up your machine and database. Make sure that you shut down all the BPI components, using the BPI Administration Console, and then close the BPI Administration Console, before backing up your machine and starting the upgrade process. For details on shutting down the BPI components, see "Starting and Stopping the BPI Server Components" in the *Business Process Insight Server Administration Guide*.

4 Shut Down Your BPI System

Shut down all BPI components using the BPI Server Administration Console (see "Stopping the BPI Server Components Using the Administration Console" in the *Business Process Insight Server Administration Guide*).

If the installer detects any of the BPI components still running, the installation is aborted until the components are stopped.

The BPI server must be stopped before all the BSM upgrade activities are started to prevent data loss.

5 Wait Until the BSM Upgrade to Version 9.12 is Completed and BSM is in a Production Environment Mode

Business Process Insight must be upgraded to 9.12 to use with a BSM version 9.12 system. The BPI menus are disabled until you upgrade BPI to version 9.12 and obtain and install a BPI 9.12 license key; see "Licensing" in the *Business Process Insight Server Administration Guide*.

Note: During a Business Availability Center (BAC-8.x) or Business Service Management (BSM-9.x) staged upgrade, there are no BPI components or BPI menus available within BSM version 9.12 until BSM is switched from a staging to production environment mode. Switching the BSM mode from staging to production is a function of the BSM upgrade process. The Modeler, Process Repository and various other BPI components and functionality are disabled during BSM Staged upgrades to protect your BPI data.

You can now continue and upgrade your BPI components as described in "Upgrading BPI From 8.x to 9.10" on page 410 or "Upgrading BPI From 9.10 to 9.12" on page 422.

Upgrading BPI From 8.x to 9.10

Upgrading BPI from 8.x to 9.10 includes the following main tasks:

- "Upgrade Tasks for 8.x to 9.10" on page 411
- "Post Upgrade Tasks for 8.x to 9.10" on page 413
- "Migrating the BPI 9.10 Server Installation To a 64-Bit System" on page 416
- "Troubleshooting and Limitations for an 8.x to 9.10 Upgrade" on page 421

Upgrade Tasks for 8.x to 9.10

Complete the following steps to upgrade any combination of BPI 8.x components to 9.10:

- 1** Make sure that all the BPI Server components are stopped and prerequisites are met as described in "Tasks to Complete Before Starting the BPI Server Upgrade" on page 407.
- 2** From an account with **Administrator** privileges in the Business Service Management interface, download the installation procedure executable for Business Process Insight as follows:
 - a** Access the **Admin > Platform > Setup and Maintenance > Downloads** page.
 - b** Select **Business Process Insight** in the **Category** drop-down list and the appropriate operating system in the **System** drop-down list.

For details on user permissions, see "How to Manage User Permissions" in *Using Business Process Insight*.
 - c** Download the appropriate executable file to a location of your choice and run the setup file for the installation:
 - For Windows: **HPBPI_v9.10_win.exe**
 - For Linux: **HPBPI_v9.10_linux.bin**An installation interface displays, which leads you through the procedures to install your BPI components.
- 3** Click **Next** to start the installation and then follow the instructions presented by the installation interface.
- 4** The installation procedure continues and installs the BPI directories and files. When the installation is complete, click **Done** to exit the installation procedure.

- 5 After BSM 9.10 is in production environment mode, open the BPI Server Administration Console and:
 - ▶ Reconfigure the connection details between BPI 9.10 and the newly installed BSM 9.10 Gateway Server host on the **HP Business Service Management settings** page.
 - ▶ Reconfigure the BPI Repository Schema database in the BPI Server Administration Console on the **<Oracle or MS SQL> Server Access to the Repository Database** page in the **Process Repository** configuration pane.
 - ▶ Reconfigure the security settings for Lightweight single sign-on (LW-SSO) on the BPI Administration Console **Servlet Engine > Security** page so that the BSM 9.10 Gateway Server and BPI 9.10 Server credential information are synchronized. You do this by copying the LW-SSO init string from the BSM Server to the BPI Server Administration Console Security page. Do this as follows:
 - ▶ From the BSM 9.10 user interface, select **Admin > Platform > Users and Permissions > Authentication Management**, click the **Configure** button to open the Authentication Wizard, and select **Single Sign-On**. Select **Lightweight** as the authentication mode. In the Token Creation Key (init String) text box, copy the init string.
 - ▶ From the BPI 9.10 Server Administration Console, select the **Security** option in the Navigator left pane, and paste the init string in the **Single sign-on token creation key (Initstring)** text box.

Note: This token creation key must match between the BSM and BPI servers or the two will not be able to communicate properly.

- 6 Restart the BPI components using the BPI Administration Console or the Windows Services. For details, see "Starting BPI Server Components" in the *Business Process Insight Server Administration Guide*.

You can also verify the installation using the example described in "Verifying Your Installation Using the Integrity Checker" in the *Business Process Insight Server Administration Guide*.

The BPI upgrade is now complete.

You can now complete any relevant post upgrade tasks described in the next section "Post Upgrade Tasks for 8.x to 9.10" on page 413.

Post Upgrade Tasks for 8.x to 9.10

The following sections describe tasks that you might need to complete following the BPI Server upgrade.

If you do not take the actions described in these sections, you might not have a fully operational BPI system.

- "Install the BPI License" on page 413
- "Reinstate Changes to BPI Configuration Files" on page 413
- "Update the BPI Instance Database if TransactionVision is a Datasource for a Business Model" on page 414
- "Compare the 9.10 Servlet Engine Configuration File with the 8.x Configuration File" on page 415

Install the BPI License

BPI Server version 9.10 is a fully licensed product. For licensing information and details about obtaining and installing your license key, see "Licensing" in the *Business Process Insight Server Administration Guide*.

Reinstate Changes to BPI Configuration Files

If you made any changes to configuration files not specifically listed in this chapter, these changes need to be reapplied to the newly installed files.

When you have completed these changes, and completed any other applicable post upgrade tasks described in this section, you can restart the BPI components that you stopped. For details, see "Starting BPI Server Components" in the *Business Process Insight Server Administration Guide*.

Update the BPI Instance Database if TransactionVision is a Datasource for a Business Model

If a pre-upgrade BPI business model uses TransactionVision as a datasource, you need to update the BPI Instance database post-upgrade by deploying the business model using the BPI Modeler.

Following are the basic steps for updating business models that use TransactionVision as a datasource. For details on importing and exporting business models, see “How to Import and Export Definitions” in *Using Business Process Insight*.

Caution: Do not undeploy any parts of the model process, data, or events during this procedure. Doing so may cause a loss of legacy data captured prior to undeployment.

1 In the BPI Modeler, export the business model to a temporary zip file.

- a** Select the business model that uses TransactionVision as a datasource in the Navigator panel under **Process Repository > Processes > <target business model>**.
- b** Click **File > Export Definition** and specify the directory and file name where you want to create the .zip file for the exported business model.
- c** Click **Export** and close the Export Definition dialog when the export is complete.

2 Re-import the business model.

- a** Select **File > Import Definitions**.
- b** Enter or browse for the business model previously exported above and open the file.
- c** Click **Next** to see a summary of definitions and click **Import**.
- d** Close the Import Results dialog when the import is complete.

By re-importing the business model, the Processes, Data, and Events of the model are flagged for update and indicate they require deployment.

3 Deploy the business model - do not undeploy.

This step updates the BPI Instance database without displacing legacy data and without undeploying the business model.

- a** Select the business model in the Navigator panel under **Process Repository > Processes > <target business model>**.
- b** Select **File > Deploy**. Be sure that the radio-button selected in the Deploy dialog panel is set to **Replace the existing definition**.
- c** Click **Deploy**, then close the Deploy dialog when the deploy is complete.

The target business model Processes, Data, and Events should now be in the Deployed (green) state.

4 Repeat steps 1 - 3 for each business model that uses TransactionVision as a datasource.**Compare the 9.10 Servlet Engine Configuration File with the 8.x Configuration File**

Following a BPI upgrade, a new version of the Servlet Engine configuration file (**tomcat-users.xml**) is installed. The original file is left in place and is not modified. This is because you might have made changes to the file which you do not want to be overwritten.

Compare the new file with your existing configuration file and copy the BPI-related changes into the existing file.

The location of the Servlet Engine configuration file is:

bpi-install-dir\nonOV\jakarta-tomcat-5.0.19\conf

The name of the file is the same as the original file, and appended to the file name is a string, which indicates the version of BPI that the file is associated with for example:

tomcat-users.xml.09.10.000

Migrating the BPI 9.10 Server Installation To a 64-Bit System

This section describes how to migrate a BPI Server installation to a 64-bit system, either from a 32-bit system or a 64-bit system.

This section includes:

- "Procedure Overview" on page 416
- "Preparation" on page 417
- "Installation" on page 418
- "Migration" on page 418
- "Start the BPI Product" on page 421

Procedure Overview

It is assumed that the BPI Instance database is to be re-used at its current location. If the BPI Instance database is to be migrated, see step 4 in "Preparation" on page 417 to migrate the database with either the MS SQL Server or Oracle tools.

For the purposes of this procedure, the source and target systems are identified as follows:

- Source BPI Server system name: > <*SourceHostName*>
- Target BPI Server system name: > <*TargetHostName*>
- Source BPI Instance database hostname > <*DBsourceHostName* >

If you are not migrating the BPI Instance database, the source and target BPI Instance database hostnames are to be the same.

- Target BPI Instance database hostname > <*DBtargetHostName*>

Preparation

Complete the following steps to prepare for the migration:

- 1 On *<SourceHostName>*, be sure the BPI Instance database is referenced by its actual name, *<DBsourceHostName >*, and not as **localhost**:
 - a Open the BPI Server Administration Console and navigate to the *<MS SQL or Oracle> Server Access to BPI Instance Database* component.
 - b Check to see if the *<MS SQL or Oracle> Server hostname* in the right panel is *<DBsourceHostName >*.
- 2 If the hostname shown is **localhost**, do the following:
 - a Back up then edit the following files:
 - *<BPI_INSTALLATION_HOME>\HP Business Process Insight\data\conf\bia\masterconfig.properties*
 - *<BPI_INSTALLATION_HOME>\HP Business Process Insight\data\conf\bia\admin.cfg*
 - b Modify references of **localhost** in both files to the appropriate Instance database server name (*<DBsourceHostName>*). The exception being the **local_host=localhost** line near the top of the **admin.cfg** file. Do not modify this line.
- 3 In the *<MS SQL or Oracle> Server Access to BPI Instance Database* component, verify that the appropriate server name is displayed for the BPI Instance database **hostname**.
- 4 If you are migrating the BPI Instance database to a new host, perform that operation here using the appropriate SQL Server or Oracle tools.
Essentially, you are replicating the original BPI Instance database *<DBsourceHostName>* to the desired target host *<DBtargetHostName>*.
If you are not migrating the Instance database to a different location, ignore this step.
- 5 On *<TargetHostName>*, be sure the database service is running.

- 6 On *<SourceHostName>*, be sure:
 - ▶ Database service is running.
 - ▶ BSM is **not** running. Verify using **myStatus.html** by selecting **Start->All Programs->HP Business Service Management->Administration->HP Business Service Management Status**. If BSM is running, disable it.
 - ▶ BPI Server is **not** running — if it is, stop all BPI components through the BPI Administration Console, see “BPI Administration Console” in the *Business Process Insight Server Administration Guide*.
- 7 On *<DBtargetHostName>*, be sure the database service is running.

Installation

Complete the following steps on *<TargetHostName>*:

- 1 Install BSM 9.x (if not already installed).
- 2 Start/Enable BSM. Be sure it is running using **myStatus.html**.
- 3 Install BPI Server 9.x. During installation, note the following:
 - a Do **not** set up the database through the installation wizard - select **No** in the BPI Database Creation Dialog.
 - b Be sure the LWSSO init strings are compatible between BPI and BSM.
 - c Do not launch or start up any BPI components.

Migration

Complete the following steps to perform the migration:

- 1 From the *<SourceHostName>* to the *<TargetHostName>* system, copy the entire file/directory structure under *<BPI_INSTALLATION_HOME>\HP Business Process Insight\data*** from the source to the target. Overwrite directories and files as necessary.
- 2 On *<TargetHostName>*, edit each of the following files (2a, 2b, and 2c).

Be sure the line items identified or tokens listed in these files are correctly set as specified below. Some of these tokens may not be present in the files copied over from the *<SourceHostName>* box, so you might need to add and set them within the file.

- a** Edit `<BPI_INSTALLATION_HOME>\HP Business Process Insight\data\conf\bia\admin.cfg` as follows:
1. Search for `DatabaseMSSQLjdbcUrl` or `DatabaseOraclejdbcUrl` depending on the BPI Instance database type being used.
 2. Be sure that the server identified is the `<DBtargetHostName>` server.
- b** Edit `<BPI_INSTALLATION_HOME>\HP Business Process Insight\data\conf\bia\masterconfig.properties` as follows:
1. Add or modify the following tokens as shown:


```
ESC_BIA_OVIS_MSSQL_HOST=<DBtargetHostName>
BIA_OVIS_MSSQL_HOST=<DBtargetHostName>
BIA_ENGINE_MSSQL_HOST=<DBtargetHostName>
HPBPI_DASHBOARD_HOSTNAME=<TargetHostName>
BAC_SAMPLES_RECALCULATE_DELAY=0
BIA_MAX_GROUP_STATISTICS=100
BIA_INSTALLED_COMPONENTS=eventhandleradaptor,notification,
modelrepos,engine,views,metrics,webservices,adaptorframework,b
acdatasamplesprovider,jmsevenhandleradaptor,modeler
BIA_METRIC_MAX_GROUP_STATISTICS=100
BIA_USE_USERDEF_LOG_VIEWER=true
ESC_HPBPPI_PROCESS_REPOSITORY_MSSQL_HOST=<TargetHostNa
me>
HPBPI_PROCESS_REPOSITORY_MSSQL_DATABASE=<BPI database
name in Process Repository Database>
BIA_OVIS_IMPORTER_HOST=<TargetHostName>
BIA_SMTP_HOST=<TargetHostName>
BIA_METRIC_THRESHOLD_ACTIVE_CHECK_DELAY=300
HPBPI_PROCESS_REPOSITORY_MSSQL_HOST=<TargetHostName>
BIA_OVIS_ORACLE_HOST=<DBtargetHostName>
```

BPI_SERVER_HOSTNAME=<TargetHostName>

ESC_BIA_ENGINE_MSSQL_HOST=<DBtargetHostName>

2. Verify any listed directory paths in this file conform to the appropriate BPI installation locations for <SourceHostName>, <TargetHostName> and <DBtargetHostName>. Be particularly aware of references to “Program Files (x86)” versus “Program Files” for the <TargetHostName>.

c Edit <BPI_INSTALLATION_HOME>\HP Business Process Insight\data/conf/bia/bia-model-repository-db.properties as follows:

1. You may need to modify the specified **DatabaseName** to match the BPI **DatabaseName** on the <TargetHostName>. Be sure that the **hostname** and **Databasename** are correctly listed in this file.

2. Search for the parameter **DatabaseName**=<BPIDataBaseName on TargetHostName> to help identify the items that may need editing in the file.

3 On <TargetHostName>, execute:

<BPI_INSTALLATION_HOME>\HP Business Process Insight\bin\biaadmin applyconfig

4 From the utilities provided by the new 9.x installation on <TargetHostName>, upgrade the reused BPI Instance database located on <DBtargetHostName>. From <TargetHostName>, execute:

a For SQL:

<BPI_INSTALLATION_HOME>\bin\bpidbsetup.bat
-upgradeDatabase -mssql <DBtargetHostName> <databasePort>
 <bpiUser> <bpiUserPassword> <bpiSchema>

b For Oracle:

<BPI_INSTALLATION_HOME>\bin\bpidbsetup.bat
-upgradeDatabase -oracle <DBtargetHostName> <databasePort>
 <bpiUser> <bpiUserPassword> <db_sid>

c Execute **bpidbsetup.bat -help** to see more detailed usage information.

Start the BPI Product

Complete the following steps to start the BPI product:

- 1 On <*TargetHostName*>, start/enable BPI components using the BPI Administration Console.
- 2 Verify the configurations in the Administration Console <*MS SQL or Oracle*> **Server Access to BPI Instance Database** component as described in "Preparation" on page 417.

Troubleshooting and Limitations for an 8.x to 9.10 Upgrade

The following sections describe troubleshooting and limitation information that could occur after completing the BPI upgrade to 9.10.

Upgrading with Large Amounts of Data in the Database

If you have a significant amount of process and business process monitor data in your database, be aware that the upgrade to BPI version 9.10 can take some time.

The amount of time the upgrade takes depends on the database type (Oracle Server, or Microsoft SQL Server), your machine type, and the amount of data. However, with hundreds of thousands of business monitor instances, it could take hours, rather than minutes, for the upgrade to complete.

Servlet Engine and System Restart

Occasionally following a system restart, the Servlet Engine appears not to have started, both within the BPI Server Administration Console and as a Windows Service.

The Servlet Engine service is actually in the processes of starting, but is taking a long time, possibly due to other applications causing delay; for example, the database can take a long time to start when it is very full.

If you think that you are experiencing this problem do the following:

- 1 From the BPI Server Administration Console, click the **Start** button for the Servlet Engine from the **Status** screen.
- 2 Click the **Stop** button for the Servlet Engine as soon as it is enabled.

Your Servlet Engine services are now synchronized and the Servlet Engine is not started.

- 3 Restart the Servlet Engine as normal.

Upgrading BPI From 9.10 to 9.12

Complete the following steps to upgrade BPI 9.10 to 9.12 after the BSM upgrade to 9.12 is completed:

- 1 Make sure that all the BPI Server components are stopped and prerequisites are met as described in "Tasks to Complete Before Starting the BPI Server Upgrade" on page 407.
- 2 From an account with **Administrator** privileges in the Business Service Management interface, download the installation procedure executable for Business Process Insight as follows:

- a Access the **Admin > Platform > Setup and Maintenance > Downloads** page.

- b Select **Business Process Insight** in the **Category** drop-down list and the appropriate operating system in the **System** drop-down list.

For details on user permissions, see "How to Manage User Permissions" in *Using Business Process Insight*.

- c Download the appropriate executable file to a location of your choice and run the setup file for the installation:

- For Windows: **HPBPI_v9.12_win.exe**

- For Linux: **HPBPI_v9.12_linux.bin**

An installation interface displays, which leads you through the procedures to install your BPI components.

- 3 Click **Next** to start the installation and then follow the instructions presented by the installation interface.
- 4 The installation procedure continues and installs the BPI directories and files. When the installation is complete, click **Done** to exit the installation procedure.
- 5 After BSM 9.12 is in production environment mode, open the BPI Server Administration Console and:
 - ▶ Reconfigure the connection details between BPI 9.12 and the newly installed BSM 9.12 Gateway Server host on the **HP Business Service Management settings** page.
 - ▶ Reconfigure the BPI Repository Schema database in the BPI Server Administration Console on the **<Oracle or MS SQL> Server Access to the Repository Database** page in the **Process Repository** configuration pane.
 - ▶ Reconfigure the security settings for Lightweight single sign-on (LW-SSO) on the BPI Administration Console **Servlet Engine > Security** page so that the BSM 9.12 Gateway Server and BPI 9.12 Server credential information are synchronized. You do this by copying the LW-SSO init string from the BSM Server to the BPI Server Administration Console Security page. Do this as follows:
 - ▶ From the BSM 9.12 user interface, select **Admin > Platform > Users and Permissions > Authentication Management**, click the **Configure** button to open the Authentication Wizard, and select **Single Sign-On**. Select **Lightweight** as the authentication mode. In the Token Creation Key (init String) text box, copy the init string.
 - ▶ From the BPI 9.12 Server Administration Console, select the **Security** option in the Navigator left pane, and paste the init string in the **Single sign-on token creation key (Initstring)** text box.

Note: This token creation key must match between the BSM and BPI servers or the two will not be able to communicate properly.

- 6 Restart the BPI components using the BPI Server Administration Console or the Windows Services. For details, see "Starting BPI Server Components" in the *Business Process Insight Server Administration Guide*.

You can also verify the installation using the example described in "Verifying Your Installation Using the Integrity Checker" in the *Business Process Insight Server Administration Guide*.

The BPI upgrade is now complete.

You can now complete any relevant post upgrade tasks described in "Post Upgrade Tasks for 9.10 to 9.12" on page 424.

Post Upgrade Tasks for 9.10 to 9.12

The following sections describe tasks that you might need to complete following the BPI Server upgrade.

If you do not take the actions described in these sections, you might not have a fully operational BPI system.

- "Install the BPI License" on page 424
- "Reinstate Changes to BPI Configuration Files" on page 424
- "Compare the 9.12 Servlet Engine Configuration File with the 9.10 Configuration File" on page 425

Install the BPI License

BPI Server version 9.12 is a fully licensed product. For licensing information and details about obtaining and installing your license key, see "Licensing" in the *Business Process Insight Server Administration Guide*.

Reinstate Changes to BPI Configuration Files

If you made any changes to configuration files not specifically listed in this chapter, these changes need to be reapplied to the newly installed files.

When you have completed these changes, and completed any other applicable post upgrade tasks described in this section, you can restart the BPI components that you stopped. For details, see "Starting BPI Server Components" in the *Business Process Insight Server Administration Guide*.

Compare the 9.12 Servlet Engine Configuration File with the 9.10 Configuration File

Following a BPI upgrade, a new version of the Servlet Engine configuration file (**tomcat-users.xml**) is installed. The original file is left in place and is not modified. This is because you might have made changes to the file which you do not want to be overwritten.

Compare the new file with your existing configuration file and copy the BPI-related changes into the existing file.

The location of the Servlet Engine configuration file is:

***bpi-install-dir*nonOV\jakarta-tomcat-5.0.19\conf**

The name of the file is the same as the original file, and appended to the file name is a string, which indicates the version of BPI that the file is associated with for example:

tomcat-users.xml.09.12.000

26

BAC Integrations Upgrade Information

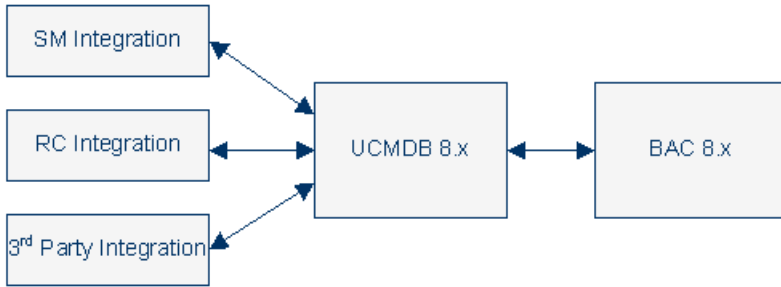
This chapter includes:

- HP Universal CMDB (embedded/external) Upgrade Information on page 427
- Upgrading HP Universal CMDB Integration - Splitting Procedure on page 430
- NNMi Upgrade Information on page 433
- Migrating Modified UCMDB Integration (Federation) Adapters on page 434
- Upgrade of the Integration of HP Operations Orchestration on page 434
- Upgrade EMS Integrations on page 435
- RTSM Upgrade Limitations on page 435

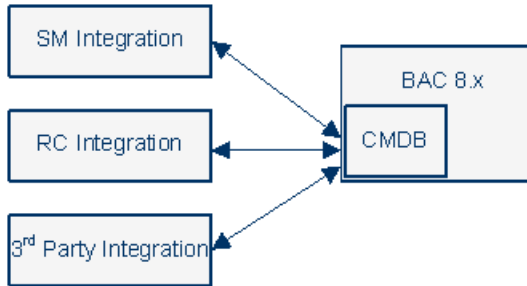
HP Universal CMDB (embedded/external) Upgrade Information

Note: This section is relevant for upgrading integrations in which HP Universal CMDB was being used as a repository for BAC 8.x CI's.

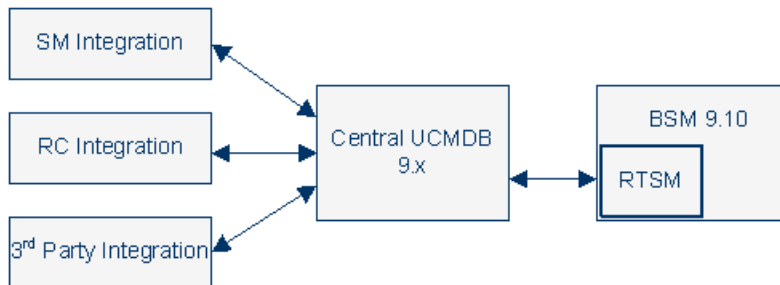
There are a number of different configurations that were possible for integrations between HP Universal CMDB and BAC 8.x. One such configuration was to use an external server for HP Universal CMDB. In this case, you may have configured additional HP and third-party products to integrate with the HP Universal CMDB server, as seen in the example below.



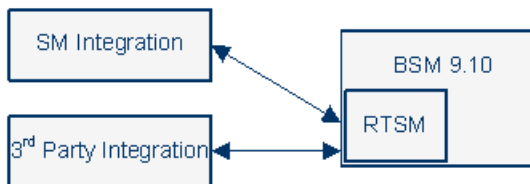
Alternatively, these integrations could also have been configured to communicate directly with the BAC 8.x server via an embedded CMDB.



There are two methods for upgrading HP Universal CMDB and its related integrations. The first method, called **splitting**, involves setting up an external Central UCMDB 9.x server, configuring the HP Universal CMDB integrations to synchronize data with that server, and configuring the Central UCMDB 9.x server to communicate with the embedded RTSM within BSM 9.x.



The second method, called **migrating**, involves reconfiguring any integrations that you had with an external HP Universal CMDB 8.x to communicate with the internal RTSM contained in BSM 9.x. This option is limited in that not every integration can work directly with RTSM (for example Release Control). For more information about RTSM integration recommendations, see the RTSM Best Practices PDF.



Alternatively, if you had an external HP Universal CMDB server with integrations with other products, you can choose to upgrade BSM to 9.x without upgrading HP Universal CMDB or its related integrations. This prevents you from configuring any integrations between BSM and HP Universal CMDB until you upgrade HP Universal CMDB to version 9.x.

RTSM is an embedded version of HP Universal CMDB included in every instance of BSM 9.x. Therefore, if you had an external instance of HP Universal CMDB but did not have any integrations with other products, you no longer need to use an external HP Universal CMDB server. The upgrade will automatically migrate your data from the external server to the embedded RTSM instance.

For more information about working with HP Universal CMDB, see the RTSM Best Practices PDF.

For information about how to upgrade HP Universal CMDB and any integrations associated with it, see "Upgrading HP Universal CMDB Integration - Splitting Procedure" on page 430.

Upgrading HP Universal CMDB Integration - Splitting Procedure

This procedure describes how to migrate HP Universal CMDB and its related integrations to integrate with BSM 9.1x by setting up an external Central UCMDB 9.x server. We recommend performing this procedure in two cases:

- ▶ If you had integrations between other HP products via HP Universal CMDB
- ▶ If your HP Universal CMDB was being used to implement configuration or changes management processes using DDMA, RC, Amber, or other HP or third party products.

For background information about upgrading HP Universal CMDB, see "HP Universal CMDB (embedded/external) Upgrade Information" on page 427.

For more information about working with HP Universal CMDB, see the RTSM Best Practices PDF.

To set up an external Central UCMDB:

- 1** Perform this step only if you are performing a direct BSM upgrade and you did not have an external instance of CMDB in BAC 8.x. Begin the BSM 9.1x direct upgrade procedure, but immediately before uninstalling BAC 8.x, stop all connections and integrations into HP Universal CMDB. Continue with the upgrade process of removing BAC 8.x and upgrading to BSM 9.1x.
- 2** Install new instance of HP Universal CMDB 9.x.
- 3** If you need to preserve other configurations from the original CMDB, create a custom package, export it, and deploy it in the external CMS. For details, see "Package Manager" in the RTSM Administration Guide. Note that deploying custom packages can overwrite critical class model elements in the CMS environment. Therefore, you should only add modified or user type elements and should not add out of the box or factory type elements.
- 4** If you need to preserve credentials and IP ranges from the original CMDB, you can export them from the Data Flow Management under RTSM and then import them into the external CMS. For details see "How to Export and Import Credential and Range" in the RTSM Data Flow Management Guide.
- 5** If you need to preserve the original CMDB IDs of items in the central UCMDB server, perform a one-time synchronization between the central UCMDB server and RTSM. This synchronization is activated from RTSM. This synchronization only transfers data. If there are resources such as views, tqls or enrichments that you want to migrate to the new server, it needs to be exported from RTSM and imported to the central UCMDB manually.

After the synchronization, Central UCMDB will have the synchronized CIs with the original CMDB IDs. The Global IDs in the Central UCMDB will be equal to the internal CMDB IDs.

For information about how to perform this procedure, see "How to Perform Initial Synchronization" in the *RTSM Data Flow Management Guide*.

Note: At this point all configurations and CIs that existed on the external UCMDB are part of RTSM in the upgraded BSM system.

- 6 Move the integrated products from the original server to the Central UCMDB 9.x server.
- 7 If you want to continue synchronizing data between the Central UCMDB and RTSM database embedded in the BSM 9.1x server, set up an ongoing synchronization. Choosing not to synchronize these databases may prevent some integrations from working. For information about how to perform this procedure, see "How to Set Up Integrations between CMS and BSM" in the *RTSM Data Flow Management Guide*.
 - ▶ If you had an integration between BSM and Service Manager relating to alerts, make sure that CIs that are part of this integration are included in on-going synchronization.
 - ▶ If you were integrating Service Manager planned changes and incidents with BSM Service Health, this step is not optional. The integration will not work unless there is an ongoing sync and a delegation of federation is configured. For more details, see "How to Set Up Integrations between CMS and BSM" in *RTSM Data Flow Management Guide*.
 - ▶ You can view BSM KPI's in an external applications by setting up an adapter. If you configured this type of adapter in BAC 8.x, and you have configured a delegation of federation as part of the ongoing topology synchronization between Central CMDB and BSM, the KPI federation adapter must be deployed on the central UCMDB and not on the RTSM. You must manually move this adapter. For details, see below.

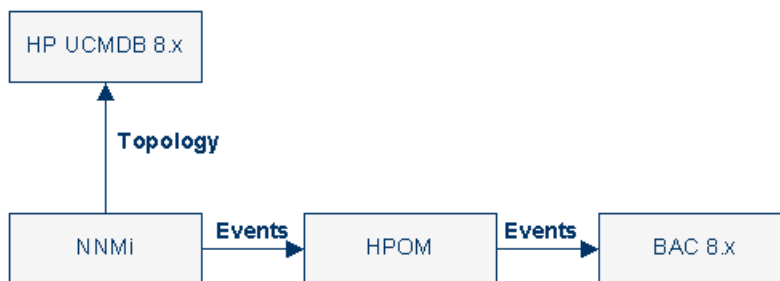
To manually move the adapter used to view KPIs from RTSM to the Central UCMDB server:

- 1 Deploy the following package on the central UCMDB server:
HPBSM\odb\conf\factory_packages\BACKPIsAdapter.zip

- 2 Perform the configurations described in "Set Up an Adapter to View KPIs in an External Application" in the RTSM Developer Reference Guide.

NNMi Upgrade Information

In BAC 8.x, NNMi had the ability to integrate topology information with CMDB, and events with BAC via HPOM and the OMi application as follows:



NNMi 8.x can continue to function with BSM 9.1x without any changes to configuration or functionality. There is a recommended modification that you can perform if you decided to upgrade to NNMi 9.x and you are synchronizing BSM 9.x with HP UCMDB 9.x. In this case, NNMi can integrate both topology and events directly with BSM 9.10 as seen below. Should you choose to perform this modification, it should be done after the BSM 9.1x upgrade is complete.



Migrating Modified UCMDB Integration (Federation) Adapters

Out-of-the-box adapters: All adapters must be compatible with the new BDM model. If you made changes to existing out-of-the-box adapters, you must make the same changes to the adapter files in the new BSM version. That is, do not copy files from version 8.0x and overwrite the files in the new version. Back up the modified adapters before starting the upgrade process and copy the changes once the upgrade is complete.

Custom adapters: Back up the custom adapters before starting the upgrade process and redeploy them in BSM 9.1x. For details, see "Package Manager" in the RTSM Administration Guide.

Upgrade of the Integration of HP Operations Orchestration

The table describes what changed between BAC 8.x and BSM 9.x.

Topics	BAC 8.x	BSM 9.x
Run books assigned to CIs	Run books assigned to CIs	Run books assigned to CIs: The upgrader automatically handles the following changes due to the topology changes in the RTSM: <ul style="list-style-type: none"> ▶ CI Types. For example, Host CI is changed into Node CI. ▶ CI attributes. ▶ The mapping of CI types to runbooks in Admin > Integrations > Operations Orchestration.
BAC-OO integration (not automatically upgraded)	BAC-OO integration	BSM-OO integration TO DO: After the upgrader has run, you must perform the BSM-OO integration. For details on how to reconfigure OO, see "How to Integrate BSM and OO" in <i>Solutions and Integrations</i> .

Upgrade EMS Integrations

The Show Events context menu that opens a console or event log listing the events relevant to the integration and allows you to delete events is not upgraded.

RTSM Upgrade Limitations

- ▶ When upgrading from version 8.0x to version 9.1x, the Data Flow Probe fails to update the server with job results if the Probe's IP address changes (and its identifier remains the same).
- ▶ When upgrading from version 9.0x to version 9.1x, if you have a larger History database, the first server startup may take some time to complete. Do not interrupt the server startup process until you have confirmed that the server is up and running.
- ▶ LDAP server settings are not upgraded during the upgrade process. You must manually reconfigure the LDAP connection configuration after upgrading to 9.1x (user mappings are upgraded).

27

Upgrade Diagnostics

This chapter includes:

- Diagnostics Considerations When Upgrading BAC to 9.1x on page 437

Diagnostics Considerations When Upgrading BAC to 9.1x

If you have Diagnostics integrated with BAC then there are some Diagnostics items to consider when upgrading to BSM 9.1x.

BSM Upgrade and Related Diagnostics Procedures

Follow these general steps in upgrading - when BSM is integrated with Diagnostics.

- 1** Complete the BSM upgrade. Relevant Diagnostics data will be handled during the BSM upgrade process.
- 2** Upgrade Diagnostics Servers (commander/mediators). Note that you can upgrade the agents and collectors to the latest version or leave them at 8.x or 9.x versions or have a mix of both. To get the latest BSM integration features of Diagnostics 9.1x you will need to upgrade agents and collectors to the latest version.
- 3** If you upgraded Diagnostics Servers from 9.0 or 9.01 then you need to remove the certificates used for event channel communication on the Diagnostics commander. That is unless the OM Agent on the Diagnostics Commander is used by another OM sever, then you need to coordinate removing the certificates with other monitoring teams. **If you upgraded your Diagnostics Commander Server from Diagnostics 8.x then you do not need to do this step.**

See the image below for the commands to remove the certificates.

```
C:\ovcert -list
+-----+
| Keystore Content |
+-----+
| Certificates:   |
|   ad2c79b2-9af7-7543-002d-ceeb548960bc (*) |
+-----+
| Trusted Certificates: |
|   CA_6c852d02-9ae6-7543-1d6e-b6fab24428f0 |
+-----+
C:\ovcert -remove ad2c79b2-9af7-7543-002d-ceeb548960bc
C:\ovcert -remove CA_6c852d02-9ae6-7543-1d6e-b6fab24428f0
```

- 4 Then you need to re-register the new version of Diagnostics with the BSM 9.1x servers and the OMi agents. See the *HP Diagnostics Installation and Configuration Guide* chapter on Setting Up Integration Between BSM and Diagnostics, section on "Registering the Diagnostics Server in Business Service Management".
- 5 You can perform a hard sync or wait for the sync to automatically occur. See the *HP Diagnostics Installation and Configuration Guide* chapter on Setting Up Integration Between BSM and Diagnostics, section on "Synchronize CIs Between Diagnostics and Business Service Management".

Troubleshooting the Upgrader for Diagnostics Data

See the following for troubleshooting the upgrade for Diagnostics data:

- The BSM upgrader writes logs relating to Diagnostics data to **log/upgrade/diagupgrade.log**.
- If there are issues with new CIs and HIs not showing up in BSM from Diagnostics make sure that the OMi event channel is set up correctly. See the *HP Diagnostics Installation and Configuration Guide* chapter on Troubleshooting, sections on "OM Agent Troubleshooting", "Configuration of the BSM Gateway Server and Data Processing Server" and "Event Based Health Indicator Status Troubleshooting Flow" for troubleshooting tips.

What's New in the Diagnostics Integration with BSM

When integrating Diagnostics with BSM you will notice the following changes in the Diagnostics integration.

- ▶ The `diagnostics_probe` CI is no longer used and is replaced with more granular application infrastructure CIs representing J2EE and .NET application servers, databases, MQ messaging systems, SAP instances and so on.
- ▶ With Diagnostics 9.1x a new MyBSM Diagnostics Dashboard view is provided in BSM.
- ▶ The Application KPI is no longer used for Diagnostics and is replaced by System and Software KPIs and specific Health Indicators based on Diagnostics metric categories.
- ▶ The Diagnostics view in BAC is replaced by Diagnostics Probe Group and Infrastructure view.

See the *HP Diagnostics User's Guide/Using Diagnostics Online Help* section on Integrations for more information on the Diagnostics and BSM integration.

The BSM upgrade will affect old Diagnostics data and configurations as follows:

- ▶ The old `diagnostics_probe` CI that is no longer used will be deleted from the Run-time Service Model after 40 days.
- ▶ The Application KPI that was associated with the `diagnostics_probe` CI will be deleted at upgrade.
- ▶ Manual modifications on the Application KPI will be lost.

28

Upgrading TransactionVision

This chapter provides information for upgrading TransactionVision to 9.10. For complete upgrading instructions, see "Upgrading TransactionVision" in the *HP TransactionVision Deployment Guide* PDF.

Note: The TransactionVision 9.10 Processing Server and agents can only be used with BSM 9.12.

This chapter includes:

- ▶ Upgrade Compatibility on page 441
- ▶ What Changed for TransactionVision on page 442
- ▶ Upgrading TransactionVision Overview on page 443

Upgrade Compatibility

TransactionVision can be upgraded from 8.0x or 9.0x to 9.10. Upgrades from versions of TransactionVision prior to 8.00 are not supported.

Upgrading TransactionVision After a BSM Direct Upgrade

TransactionVision can only be upgraded after the BSM direct upgrade to 9.12 is completed and BSM is operating in production mode. Upgrading directly refers to installing the new version on the same servers and database schemas as the original version. TransactionVision does not support a staging upgrade method. For details on upgrading BSM in either environment, see "Upgrade Types" on page 19

The TransactionVision system must be shut down before BSM is upgraded in either environment. For complete instructions on upgrading TransactionVision, see "Upgrading TransactionVision" in the *HP TransactionVision Deployment Guide PDF*.

What Changed for TransactionVision

This section describes the major changes to TransactionVision 9.10 and the Transaction Management User Interface within BSM 9.12.

- ▶ Upgrade support for 8.0x and 9.0x to 9.10.
- ▶ Alerting on incomplete and late transactions (including visibility in BSM/Service Health).
- ▶ Better extensibility to support custom event sources.
 - ▶ New Correlation user interface
 - ▶ Server correlation and topology features
 - ▶ Generic event format and API
 - ▶ Event collection from any .NET application using event generation definitions in a points file
- ▶ Report usability improvements in the Transaction Topology, Summary, Tracking and Over Time reports.
 - ▶ Provide quick visualization of metrics, response time thresholds, flow problems and paths in reports and topologies.
 - ▶ Provide enhanced tooltip information for nodes in transaction topologies such as node type, host, application server, and so on.
- ▶ Platform support.
 - ▶ Official WebSphere MQ Agent and Java Agent support for SUSE z/Linux.
 - ▶ Official Java Agent support for TIBCO BusinessWorks and Jetty.
 - ▶ Java Agent support for new versions of JBoss and Tomcat.

- ▶ Improved z/OS Agent performance for CICS and WMQ-CICS.
- ▶ z/OS Agent support for new versions of z/OS.
- ▶ Enhanced tooling support for field engineers.
 - ▶ TransactionVision Java Agent POC/Supportability "Toolkit" and improved POC supportability features.
 - ▶ New Processing Server utility to aid in investigation of correlation issues.
- ▶ Virtualization.
 - ▶ WebSphere MQ and Tuxedo Agent support for VMware ESX Server 4
- ▶ BSM mandates.
 - ▶ Support for Two-way SSL
- ▶ Many enhancements, product improvements, and defect fixes.

Upgrading TransactionVision Overview

There are two upgrade paths for TransactionVision: from 8.0x to 9.10 and from 9.0x to 9.10. Since upgrades from versions of TransactionVision prior to 8.00 are not supported, you must upgrade your TransactionVision system to version 8.0x before proceeding with the upgrade to version 9.10.

BSM-Side and TransactionVision Processing Server-Side Upgrades

Upgrading TransactionVision consists of two parts: BSM-side upgrade and TransactionVision Processing Server-side upgrade.

The BSM side upgrade contains the following TransactionVision components, which are upgraded with the BSM upgrade to 9.12. For BSM upgrading instructions, see "Upgrading to BSM 9.1x - Workflows" on page 19.

- ▶ BSM Management database upgrade, which contains the customer's Processing Server, Analyzer, Communication Links, Filters, Jobs, definitions, and so on, set up by the TransactionVision Administrator.

- ▶ Key performance indicators (KPIs) and health indicators (HIs) upgrade, which are based on the customer's infrastructure configuration items (CIs) collected by TransactionVision and contained in the Run-Time Service Model (RTSM) repository.
- ▶ TransactionVision Profile database upgrade, which contains the Business Transaction CIs, collected and built by TransactionVision.

The TransactionVision Processing Server-side upgrade contains the following components for the TransactionVision upgrade to 9.10:

- ▶ TransactionVision Processing Server
 - ▶ For the 8.0x to 9.10 upgrade, the 9.10 Processing Server is installed over the 8.0x Analyzer.
 - ▶ For the 9.0x to 9.10 upgrade, the 9.0x Processing Server just needs to be upgraded to 9.10.
- ▶ TransactionVision database upgrade

Part V

Post Deployment and Troubleshooting

29

Post-Deployment

This chapter includes:

- ▶ Starting and Stopping BSM on page 447
- ▶ Logging In on page 448
- ▶ Logging Out on page 450
- ▶ Post-Installation Tasks on page 450

Starting and Stopping BSM

After completing HP Business Service Management server installation, restart your computer. It is recommended that you do this as soon as possible. Note that when the machine restarts, you must log in as the same user under which you were logged in prior to restarting the machine.

After successfully installing the 9.12 servers (either together on one machine, or at least one instance of each server type in a distributed deployment) and connecting the server machines to the databases, you launch HP Business Service Management on each server machine.

Note: You can check which HP Business Service Management servers and features are installed on an HP Business Service Management server machine by viewing the [INSTALLED_SERVERS] section of the <HP Business Service Management server root directory>\conf\TopazSetup.ini file. For example, Data_Processing_Server=1 indicates that the Data Processing Server is installed on the machine.

To start or stop HP Business Service Management in Windows:

Select **Start > Programs > HP Business Service Management > Administration > Enable | Disable Business Service Management**. When enabling a distributed environment, first enable the Data Processing Server and then enable the Gateway Server.

To start or stop HP Business Service Management in Linux:

```
/opt/HP/BSM/scripts/run_hpbsm start | stop
```

To start, stop, or restart HP Business Service Management using a daemon script:

```
/etc/init.d/hpbsmd {start| stop | restart}
```

Note: When you stop HP Business Service Management, the HP Business Service Management service is not removed from Microsoft's Services window. The HP Business Service Management service is removed from the Services window only after you uninstall HP Business Service Management.

Logging In

You log in to HP Business Service Management from a client machine's browser using the login page. LW-SSO is HP Business Service Management's default authentication strategy. For details, see "Logging into BSM with LW-SSO" in *Platform Administration*.

You can disable single sign-on authentication completely or you can disable LW-SSO and use another supported authentication strategy. For details on selecting an authentication strategy, see "Set Up the Authentication Strategies" in *Platform Administration*.

Tip: Click the **Help** button on the login page for complete login help.

To access the HP Business Service Management login page and log in for the first time:

- 1** In the Web browser, enter the URL http://<server_name>.<domain_name>/HPBSM where **server_name** and **domain_name** represent the FQDN of the HP Business Service Management server. If there are multiple servers, or if HP Business Service Management is deployed in a distributed architecture, specify the load balancer or Gateway Server URL, as required.

Note: Users running previous versions of HP Business Service Management can still use bookmarks set to access the URL http://<server_name>.<domain_name>/mercuryam and http://<server_name>.<domain_name>/topaz

- 2** Enter the default administrator user (“admin”), and the password specified in the Setup and Database Configuration utility, and click **Log In**. After logging in, the user name appears at the top right.
- 3** (Recommended) Create additional administrative users to enable BSM administrators to access the system. For details on creating users in the HP Business Service Management system, see "User Management" in *Platform Administration*.

Note:

- For login troubleshooting information, see "Troubleshooting and Limitations" in *Platform Administration*.
 - For details on login authentication strategies that can be used in HP Business Service Management, see "Authentication Strategies — Overview" in *Platform Administration*.
 - For details on accessing HP Business Service Management securely, see the *HP Business Service Management Hardening Guide* PDF.
-

Logging Out

When you have completed your session, it is recommended that you log out of the Web site to prevent unauthorized entry.

To log out:

Click **Logout** at the top of the page.

Post-Installation Tasks

This section contains the following post-installation tasks:

- ▶ "Disable Firewall between BSM Servers" on page 450
- ▶ "Establish trust between BSM servers" on page 450
- ▶ "Configure Gateway Server Certificates" on page 452
- ▶ "Modify the product_name_enum" on page 453
- ▶ "Check Installation Log Files" on page 454

Disable Firewall between BSM Servers

Disable any firewalls that exist between BSM Gateway and Data Processing Server servers. By default, Windows Server 2003 SP1 and later versions include such a firewall. It must be manually disabled.

Establish trust between BSM servers

If you have more than one BSM Data Processing server, you need to establish trust to enable communication between the servers.

For each additional Data Processing Server, complete the following configuration appropriate for your environment:

- 1 If you have a central certificate authority, make sure that the CA root certificate was already imported into the OV certificate repository on all BSM Data Processing Servers using the following command:

```
ovcert - importtrusted -file c:\ca_root.pem
```

ovcert -importtrusted -file c:\ca_root.pem -ovrg server

- 2** From the primary Data Processing Server, export the trusted certificates using the following command:

ovcert -exporttrusted -file <file with certificate>

- 3** Copy the exported trusted certificates to the new Data Processing Server and install the certificates on new Data Processing Server using the following commands:

ovcert -importtrusted -file <file with certificate>

ovcert -importtrusted -file <file with certificate> -ovrg server

- 4** On new Data Processing Servers, export certificates using the command:

ovcert -exporttrusted -file <file with certificate>

- 5** Copy this file to all your existing Data Processing Servers and import using the following commands:

ovcert -importtrusted -file <file with certificate>

ovcert -importtrusted -file <file with certificate> -ovrg server

- 6** If you have an integration with HPOM (Windows or Unix) follow the procedure "How to Establish a Trust Relationship between BSM and External Servers" in *Solutions and Integrations* for every Data Processing server.

- 7** Update trusted certificates using the **ovcert -updatetrusted** command on following servers:

- All Gateway servers
- All HP Diagnostics servers
- All SiteScope servers
- All Integration Adapter servers

Configure Gateway Server Certificates

Operations Management and other HP BTO Software applications use certificates that enable to clients and servers to identify themselves and communicate securely with each other. The Data Processing Server can issue the required certificates to other servers in your environment, acting as a certificate authority.

If you have a one-machine deployment, the installation configures the certificates that you need. You do not need to configure Gateway Server certificates.

However, if you have a distributed deployment, after you install your BSM servers, you must make sure that every Gateway Server requests certificates from the Data Processing Server. You must then make sure that the Data Processing Server grants each certificate request.

Note: If BSM is required to issue certificates, for example, for an Integration Adapter, then the Gateway Servers must be configured to forward all incoming requests to the Data Processing Server. The primary Data Processing Server (the first server that you have configured) must be specified in the Operations Management Infrastructure Settings: **Applications > Operations Management > Certificate Server Settings > Certificate Server IP Address.**

To request certificates for Gateway Servers:

- 1 On each Gateway Server, open a command prompt, and then type the appropriate command depending on your operating system:

windows: `cd %TOPAZ_HOME%/bin`

linux: `cd /opt/HP/BSM/bin`

- 2 Start the following command:

setup-secure-communication

- 3 The command prompts you for the DNS name of the Data Processing Server. Type this name, and then press ENTER.

To grant certificate requests:

- 1 On the Data Processing Server, open a command prompt, and then type the appropriate command depending on your operating system:

windows: `cd %TOPAZ_HOME%/bin`

linux: `cd /opt/HP/BSM/bin`

- 2 Start the following command:

setup-secure-communication

- 3 The command checks for pending certificate requests. For each pending certificate request, the command shows details of the request. For example:

**INFO: Secure communication request from:
gateway1.example.com**

Press **G** to grant each request in turn. After you grant a certificate request, the command sends certificates to the Gateway Server, and then verifies that secure communication is possible.

Modify the product_name_enum

If you are planning to use Operations Manager *i*, perform the following steps:

- a Go to **Admin > RTSM Administration > Modeling > CI Type Manager**.
- b From the CI Types list select **System Type Manager**.
- c Select **product_name_enum** and click **Edit**.
- d Type **lync_server** and click **Add**.
- e Click **OK**.

Check Installation Log Files

You can see the installation log file by clicking the **View log file** link at the bottom of the installer window.

In a Windows environment, this log file, along with additional log files for separate installation packages, is located in the `%temp%\..\HPOvInstaller\HPBsm_9.10` directory.

In a Linux environment, the logs files are located in the `/tmp/HPOvInstaller/HPBsm_9.10` directory.

The installer log file name is in the following format:

HPBsm_<VERSION>_<DATE>_HPOvInstallerLog.html or
HPBsm_<VERSION>_<DATE>_HPOvInstallerLog.txt (for example,
HPBsm_9.10_2010.10.21_13_34_HPOvInstallerLog.html).

Individual installation package log file names are in the following format:

Package_<PACKAGE_TYPE>_HPBSM_<PACKAGE_NAME>_install.log (for
example, Package_msi_HPBSM_BPiPkg_install.log).

30

Changing BSM Service Users

This chapter includes:

- ▶ Changing the BSM Service User on page 455

Changing the BSM Service User

The BSM service, which runs all BSM services and processes, is installed when you run the Setup and Database Configuration utility. By default, this service runs under the local system user. However, you may need to assign a different user to run the service (for example, if you use NTLM authentication).

The user you assign to run the service must have the following permissions:

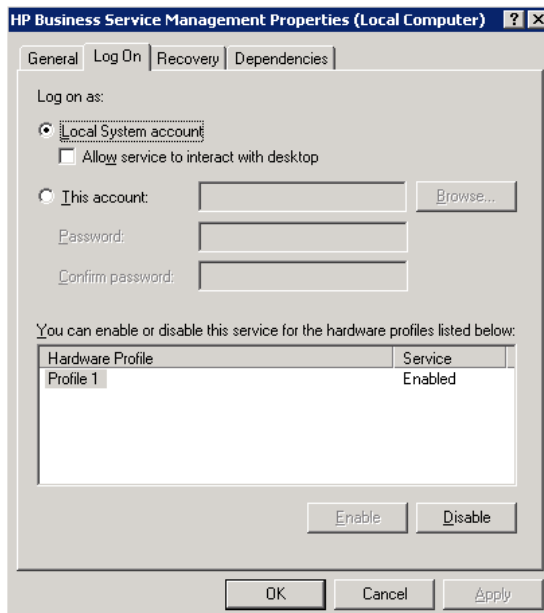
- ▶ Sufficient database permissions (as defined by the database administrator)
- ▶ Sufficient network permissions
- ▶ Administrator permissions on the local server

Note: When the BSM service is installed, it is installed as a manual service. When you enable BSM for the first time, it becomes an automatic service.

To change the BSM service user:

- 1** Disable BSM (**Start > Programs > HP Business Service Management > Administration > Disable HP Business Service Management**).

- 2 In Microsoft's Services window, double-click **HP Business Service Management**. The HP Business Service Management Properties (Local Computer) dialog box opens.
- 3 Click the **Log On** tab.



- 4 Select **This account** and browse to choose another user from the list of valid users on the machine.
- 5 Enter the selected user's Windows password and confirm this password.
- 6 Click **Apply** to save your settings and **OK** to close the dialog box.
- 7 Enable BSM (**Start > Programs > HP Business Service Management > Administration > Enable HP Business Service Management**).

Note: This procedure must be repeated if BSM is uninstalled or upgraded.

31

Troubleshooting

This chapter includes:

- Troubleshooting Resources on page 457
- Troubleshooting the Upgrade Process on page 458
- Installation and Connectivity Troubleshooting on page 465

Troubleshooting Resources

- **Installation log files.** For details, see "Check Installation Log Files" on page 454.
- **Upgrade log tool.** To view a summary of errors that occurred during the configuration upgrade portion of the upgrade wizard, run the upgrade log tool located at **<HP Business Service Management server root directory>\tools\logTool\logTool.bat**. This generates a report in the same directory with the name **logTool.txt**.
- **HP Software Self-solve knowledge base.** For additional troubleshooting information, see the HP Software Self-solve knowledge base (<http://www.hp.com/go/hpsoftwaresupport>).
- **BSM Tools.** You can use BSM tools to assist in troubleshooting the HP Business Service Management environment. You access the tools from **<HP Business Service Management server root directory>\tools** directory. Most of the tools should only be used in coordination with HP personnel. The Database Schema Verification utility (dbverify) and Data Marking utility should be used according to documented instructions.

- **BSM Logging Administrator.** This tool allows you to temporarily modify the level of details displayed in BSM logs, as well as create custom logs. To open the BSM Logging Administrator Tool, open the following URL:

<http://<BSM Gateway Server>/topaz/logAdminBsm.jsp>

Troubleshooting the Upgrade Process

This section describes problems that you may encounter when upgrading HP Business Service Management, and the solutions to these problems.

This section contains the following topics:

- "General issues" on page 458
- "Introduction screen" on page 459
- "Upgrade Settings screen" on page 459
- "Copying Files screen" on page 459
- "Database Connection - Profile Schema Settings" on page 460
- "Schema Upgrade" on page 460
- "Update Environment" on page 460
- "CMDB Upgrade" on page 461
- "Start BSM" on page 461
- "Configuration Upgrade" on page 462
- "Data Upgrade" on page 463
- "Staging Data Replicator (SDR)" on page 463
- "Data Transfer Tool" on page 463
- "Verifying Digitally Signed HP Files" on page 464

General issues

- If you are using remote desktop and the upgrade wizard is not displayed properly, try reconnecting with remote desktop at a different resolution, or from a different machine.

- ▶ Within the wizard, if the **Next** button or **Back** button do not work, check the `upgradeFramework.log` for the cause of the error. In most cases, restarting the upgrade wizard resolves the problem.
- ▶ If the Upgrade Wizard hangs when pressing the **Back** button in the OPR Database Settings dialog, stop the Upgrade Wizard and restart it. Using the **Next** button, progress to the dialog that you want to edit and continue with the upgrade.

Introduction screen

If the introduction screen opens without **Next** or **Back** buttons, close the wizard and reopen it. If repeating this action does not help, restart the wizard.

Upgrade Settings screen

If the server type shown in the upgrade settings screen is not the type you expect, you must reinstall BSM on this machine.

Copying Files screen

- ▶ Make sure you copy DPS files to the DPS, and Gateway files to the Gateway. Do not accidentally copy Gateway files to the DPS.
- ▶ If you forget to copy the **excels** folder (or you copy it to the wrong location), you can copy it later without consequence. If you have not yet installed the Gateway, save the **excels** folder to a temporary location, and copy it to the correct location after you install the Gateway.
- ▶ If you forget to copy the **cmdb/adapters** folder (or you copy it to the wrong location), the EUM configuration upgrade will fail. You can then copy the files and re-run the configuration upgrade with no consequence.
- ▶ If you have Service Health custom rule jars and you did not copy them (or copied them to the wrong location), after you start BSM the online engine fails when calculating HIs or KPIs with the custom rule. The log files contain errors, and the HIs or KPIs are shown without status. To resolve this, copy the custom rule jars at any stage and then continue with the upgrade.

- ▶ If you have SLM custom rule jars and you did not copy them (or copied them to the wrong location), the offline engine fails when calculating HIs or KPIs with the custom rule. The log files contain errors, and the HIs or KPIs are shown without status. To resolve this, copy the custom rule jars and run recalculation of all your SLAs, before the relevant data is purged from the database.

Database Connection - Profile Schema Settings

If you enter the details of the wrong profile database and you run the schema upgrade, the upgrade fails and the following message appears: **The current schema is not compatible with version 8.0.** The differences between your database and the schema will be greater than expected. Restore the Databases, and restart the upgrade.

Schema Upgrade

- ▶ If the schema upgrade step fails, follow the on-screen instructions. In most cases, an SQL script is generated that resolves the problems that caused the failure of the schema upgrade.
- ▶ If the schema upgrade fails because you have users connected to the database, but the user shown is the current machine, click **Next** and re-run the schema upgrade. If this happens more than a reasonable number of times, you can ask your DBA to kill the connections, and then click **Next**.

Update Environment

- ▶ Use the export tool log to verify that the LDAP Database Export/Import tool worked properly, or to see details of problems encountered.
- ▶ Server Deployment: If you select the wrong applications, you may fail with memory issues at any point in the upgrade. To fix the incorrect configuration, change the server deployment and restart BSM.
- ▶ Server Deployment: If you receive a message stating that the machine is not aligned with the current deployment and a restart of BSM is required, disregard this message. BSM will be restarted as part of the upgrade process at a later stage.

- ▶ **Login Settings:** If you are using a non-default password for RTSM, update all data collectors with the new password when you finish upgrading to the new servers.
- ▶ **Login Settings:** If you re-run the upgrade wizard and enter a different password for RTSM than the one you used the first time, the configuration upgrade (Geo Attributes upgrader) will fail. The logs will contain the following message: **Failed to connect to RTSM**. Re-run the upgrade wizard, and enter the password for RTSM which you used the first time you ran the upgrade.
- ▶ **Content Pack Import:** If the user is not an administrative user, the oprContentUpgrader will fail. In this case, delete the file OprUpload, and re-run the upgrade wizard using administrative credentials.
- ▶ **Content Pack Import:** If an LDAP was configured in the production environment and is not accessible, you will fail on the oprContentUpgrader. In this case, disable the LDAP and re-run the upgrade wizard.

CMDB Upgrade

- ▶ If an upgrader fails, review the following log file:
HPBSM\odb\runtime\log\upgrade\upgrade.short.log.
- ▶ If the CMDB upgrade fails, and the failure requires restoring the database, you only need to restore the CMDB schemas. You do not need to re-run all previous steps of the wizard. Additionally, you need to delete the following directory from the Data Processing Server running the upgrade wizard: HPBSM\odb\runtime.

Start BSM

- ▶ At this point in the upgrade wizard, when you start BSM not all processes are up, and the UI is not available. This is because BSM is temporarily in Upgrade mode; at a later stage you will restart BSM in Full Mode.
- ▶ When the upgrade wizard reaches the Start BSM step, certain steps are marked as successful and will not run again. If you want to rerun these steps (for example, if the DB is restored to the backup) remove all files under **<BSM installation directory>\Temp** that start with **opr**.

Configuration Upgrade

- ▶ If you passed the Start BSM step and ran the configuration upgrade, but the second upgrader (Geo Attributes) has failed, you may have run the configuration upgrade without BSM being completely ready - all processes and all services must be up. Check that BSM is up, and click the Upgrade button to re-run the configuration upgrade.
- ▶ If an optional upgrader fails, do not continue to the next step, but rather investigate the problem. You should then fix the problem and re-run the upgrade, or, if you decide that the problem does not prevent you from declaring the upgrade successful, finish the upgrade.
- ▶ If an optional upgrader fails and you proceed with the upgrade anyway, you can return to the configuration upgrade at a later stage. In this case, before you re-run the upgrader you must perform the following procedure:
 - a Run the setVersion JMX with the value 8.0.0.0. The setVersion JMX is under port 8080, Topaz service=Upgrade Framework.
 - b Disable BSM and restart the upgrade wizard.
 - c Re-run the configuration upgrade.
- ▶ When all upgraders have passed, check the logs for minor errors by running the upgrade log tool located at <HP Business Service Management server root directory>\tools\logTool. The log tool is also useful when an upgrader fails.
- ▶ If a mandatory upgrader partially failed and you accidentally selected **Pass Upgrade**, the status is set to PASSED and the upgrader cannot be re-run. To re-run, use the jmx setUpgraderStatus and set the upgrader to failed.

Data Upgrade

If the failures column contains an entry greater than 0, check the logs for errors; this may be a database problem that is easily resolved. Otherwise, contact HP Support.

Staging Data Replicator (SDR)

To verify that SDR is working:

- a Open <SDRroot directory>\conf\core\Tools\log4j\sdreplicator\sdreplicator.properties. Modify the **loglevel** to **debug**.
- b Open <BSM Directory>\>\conf\core\Tools\log4j\sdreplicator\wde.properties. Modify the **loglevel** to **debug**.
- c Find the most recent sample in <SDR root directory>/log/sdrPublishedSamples.log and make sure that you can locate it in <BSM destination>/log/wde/wdePublishedSamples.log. If samples are appearing in both logs, the SDR is working.
- d Modify the **loglevel** settings to **INFO** in the **sdreplicator.properties** and **wde.properties** files.

Data Transfer Tool

- Verify that the SDR is working before running the Data Transfer Tool; you can check the SDR log to see that the SDR is working. If you ran the Data Transfer Tool and the SDR did not run, a message will appear when you click Next (SDR initiation Date warning).
- If you exit the wizard (or the wizard crashes) during the data transfer tool sequence of steps, re-run the tool on the same dates it ran earlier (see upgrade_all.log for the exact times).
- If you decide not to run the Data Transfer Tool, you will have missing data. Take this into account when looking at reports.
- If you did not record the time of the database backup, choose a date prior to the date of backup. You will have no data missing, but the Data Transfer Tool will take longer than necessary.
- When you run the Data Transfer Tool for a second time, you must choose a different path for the temporary folder than the one chosen for the first run.

- ▶ If you accidentally enter the credentials of the staging DB and not the production DB, you will receive the following error message: **Operation Failed ... FileNotFoundException**. Enter the correct details, and continue.
- ▶ The UI allows you to pause the Transferred data upgrade, but actually this does not have any effect.

Verifying Digitally Signed HP Files

All HP installation files that are in the format listed below are digitally signed:

- ▶ **Windows:** MSI, EXE, DLL, VBS, JS, CPL.
- ▶ **Linux:** RPM files only.

To verify that the installation files are original HP-provided code and have not been manipulated by a third party, you can do the following:

For Windows files:

- 1 Right-click the file and select **Properties**.
- 2 Select the **Digital Signatures** tab and verify that the name of the signer is Hewlett-Packard.

For Linux files:

Open a command line, and run the following commands:

```
# rpm -v -checksig    ${RPM_FILE_NAME}
# rpm -v -qi -p      ${RPM_FILE_NAME}
```


For example:

```
# rpm -v --checksig HPBsmFndCom1-9.10.320-Linux2.6_64.rpm
HPBsmFndCom1-9.10.320-Linux2.6_64.rpm:
  Header V3 DSA signature: OK, key ID 2689b887
  Header SHA1 digest: OK (a4b436a86ca52dde34113c964866d5838b50bbc5)
  MD5 digest: OK (59def5f6719a78eac778324bdb0f6f05)
  V3 DSA signature: OK, key ID 2689b887

# rpm -v -qi -p HPBsmFndCom1-9.10.320-Linux2.6_64.rpm
Name       : HPBsmFndCom1           Relocations: (not relocatable)
Version    : 9.10.320              Vendor: Hewlett-Packard Company
Release    : 1                    Build Date: Sun 27 Mar 2011 06:15:37 PM IST
Install Date: (not installed)     Build Host: LABM1AMRND02.devlab.ad
Group      : Applications/System   Source RPM: HPBsmFndCom1-9.10.320-
1.src.rpm
Size       : 298420659            License: Hewlett-Packard Development Company,
L.P.
Signature  : DSA/SHA1, Sun 27 Mar 2011 07:04:03 PM IST, Key ID
527bc53a2689b887
Summary    : HP BSM Foundations Common Components Pack_1
Description:
HP BSM Foundations Common Components Pack_1
```

Installation and Connectivity Troubleshooting

This section describes common problems that you may encounter when installing HP Business Service Management or connecting to HP Business Service Management following installation, and the solutions to these problems.

This section contains the following topics:

- ▶ "Receive error message: not enough space on the drive to extract the installation files" on page 467
- ▶ "Connection to a Microsoft SQL Server database fails when running the Setup and Database Configuration utility" on page 468
- ▶ "A network login prompt appears when completing an HP Business Service Management server installation" on page 468
- ▶ "Tomcat servlet engine does not start and gives an error" on page 468

- ▶ "Inability to install HP Business Service Management components due to administrative restrictions" on page 469
- ▶ "After installing, receive http error 404 on the page when attempting to access BSM:" on page 469
- ▶ "After uninstalling HP Business Service Management and reinstalling to a different directory, HP Business Service Management does not work" on page 470
- ▶ "Business Process Monitor or SiteScope data are not being reported to HP Business Service Management" on page 470
- ▶ "Business Process Monitors fail to report to the Gateway Server running on IIS" on page 470
- ▶ "Business Process Monitor is unable to connect via the Internet to the Gateway Server installed on an Apache Web server" on page 472
- ▶ "Post-Installation Wizard fails during BSM installation on Linux machine" on page 472
- ▶ "Failed to install Adobe Flash Player" on page 472
- ▶ "BSM fails to start or BSM configuration wizard does not open" on page 472
- ▶ "Failure to log in based on FQDN" on page 473
- ▶ "After pressing Login, nothing happens. Or user logs in, but Sitemap is empty." on page 473

Receive error message: not enough space on the drive to extract the installation files

This happens during component installation. If you enter a new path for a different drive with sufficient space, the same error message is displayed.

Possible Cause:

During the file extraction process, certain data is always saved to the TEMP directory on the system drive, even if you choose to save the installation files to a different location from the default path.

Solution:

- Free up sufficient disk space on the system drive (as specified in the error message), then continue with the installation procedure.
- If it is not possible to free up sufficient disk space on the system drive, change the path for the system's TEMP variable. To do this, select **Start > Settings > Control Panel > System > Advanced tab > Environment Variables**, and edit the path for the **TEMP** variable in the User variables area.

Connection to a Microsoft SQL Server database fails when running the Setup and Database Configuration utility

Verify that the user under whom the SQL Server service is running has permissions to write to the disk on which you are creating the database.

A network login prompt appears when completing an HP Business Service Management server installation

Possible Cause:

This can occur if the IIS server's authentication method is not set to the default setting, **Allow Anonymous Access**.

Solution:

Reset the IIS server's authentication method to the default setting, **Allow Anonymous Access**, and ensure that the default user account **IUSR_XXX** (where "XXX" represents the name of the machine) is selected (the user account **IUSR_XXX** is generated during IIS installation). Then uninstall and reinstall HP Business Service Management.

Tomcat servlet engine does not start and gives an error

The error message is as follows:

```
java.lang.reflect.InvocationTargetException:  
org.apache.tomcat.core.TomcatException: Root cause - Address in use:  
JVM_Bind
```

Possible Cause:

Running Oracle HTTP Server, installed with a typical Oracle installation, on the same machine as HP Business Service Management servers causes a conflict with the Tomcat servlet engine.

Solution:

Stop the Oracle HTTP Server service, disable and then enable HP Business Service Management.

To prevent the problem from recurring after the machine is restarted, change the Oracle HTTP Server service's startup setting to **manual**.

Inability to install HP Business Service Management components due to administrative restrictions

Possible Cause:

The machine on which you are installing has policy management software that restricts access to files, directories, the Windows registry, and so forth.

Solution:

If this type of software is running, contact your organization's network administration staff to obtain the permissions required to install and save files on the machine.

After installing, receive http error 404 on the page when attempting to access BSM:

Perform the following:

- 1** Verify that all BSM processes were started by accessing the status page. For details, see "Viewing the Status of the Services" on page 434.
- 2** If all the services appear green in the status page, browse to BSM using port 8080 (http://MACHINE_NAME:8080).
Try to access the JMX console. If you can access the console, continue with step 3 trying to discover the problem.
- 3** Check if the Web server is started (http://MACHINE_NAME). If the Web server is started, you probably have a problem with the ISAPI filter.
- 4** If the problem is with the ISAPI filter and you are running on a Microsoft Windows 2008 server, check that you followed the procedure for creating a role. For details, see "Working with the Web Server" on page 152.
- 5** The Apache server may not be successfully starting because of a port collision.

After uninstalling HP Business Service Management and reinstalling to a different directory, HP Business Service Management does not work

Possible Cause: When uninstalling and reinstalling to a different location, the IIS ISAPI filter did not get updated to the new path.

Solution:

To update the IIS ISAPI filter to the new path:

- 1** Open the IIS Internet Services Manager.
- 2** Right-click the machine name in the tree and select **Properties**.
- 3** With **WWW Service** displayed in the Master Properties list, click **Edit**.
- 4** Select the **ISAPI Filter** tab.
- 5** Ensure that **jakartaFilter** is pointing to the correct HP Business Service Management directory.
- 6** Apply your changes and quit the Internet Services Manager.
- 7** Restart the IIS service.

Business Process Monitor or SiteScope data are not being reported to HP Business Service Management

There are various conditions that may cause this problem. For details on causes and possible solutions, refer to the HP Software Self-solve knowledge base, and search for article number KM438393 (<http://h20230.www2.hp.com/selfsolve/document/KM438393>).

Business Process Monitors fail to report to the Gateway Server running on IIS

Symptoms/Possible Causes:

- No data reported to loaders
- No data in Web site reports
- An error in the **data_deport.txt** log on the Business Process Monitor machine similar to the following:

Topaz returned an error (<html><head><title>Error Dispatching URL</title></head>

<body>

The URI:
api_reporttransactions_ex.asp
 is not mapped to an API Adapter.
Either the URI is misspelled or the mapping file is incorrect (the mapping file is located at:

D:\HPBAC/AppServer/TMC/resources/ServletDispatcher.xml)

</body>

</html>)

The problem can be confirmed by opening the page http://<machine name>/ext/mod_mdrv_wrap.dll?type=report_transaction. If there is a problem, a Service Temporarily Unavailable message is displayed.

You can also submit the following URL to verify Web Data Entry status:

http://<machine name>/ext/mod_mdrv_wrap.dll?type=test

This problem may be caused by the existence of **MercRedirectFilter**, which is a deprecated filter that is no longer needed for HP Business Service Management and may be left over from previous versions of HP Business Service Management.

Solution:

Delete the **MercRedirectFilter** filter and ensure that the **jakartaFilter** is the only IIS ISAPI filter running.

Business Process Monitor is unable to connect via the Internet to the Gateway Server installed on an Apache Web server

Possible Cause:

The Business Process Monitor machine is unable to resolve the Gateway Server name correctly.

Solution:

- ▶ Add the Gateway Server name to the Business Process Monitor machine's <Windows system root directory>\system32\drivers\etc\hosts file.
- ▶ Change the Gateway Server name in the <HP Business Service Management root directory>\WebServer\conf\httpd.conf file on the Gateway Server to a recognized name in the DNS.

Post-Installation Wizard fails during BSM installation on Linux machine

This may be due to a Linux bug. Open the `/etc/sysctl.conf` file and remove the line `vm.swappiness = 0`. Restart the post installation wizard.

Failed to install Adobe Flash Player

Adobe Flash Player is installed using the Adobe Download Manager which cannot handle automatic proxy configuration scripts. If Internet Explorer is configured to use an automatic proxy configuration, the download manager fails and hangs with no visual response. Try configuring a proxy host manually or see the Flash Player documentation.

BSM fails to start or BSM configuration wizard does not open

Check the supervisorwrapper.log file for the following error:

```
C:\HPBSM\conf\supervisor\manager\nannyManager.wrapper wrapper | OpenService failed - Access is denied.
```


If this error is present, the issue may be due to having User Access Control (UAC) enabled on a Windows 2008 SP2 system during the installation process. Disable UAC on all BSM servers running Windows 2008 SP2 during the installation process.

Failure to log in based on FQDN

If you see the following error in the login screen: **The HP Business Service Management URL must include the Fully Qualified Domain Name (FQDN). Please retype HP Business Service Management URL in the address bar**, but you are connecting via FQDN, check if there is a DNS resolution for Load Balanced virtual IPs from the BSM gateways. You may need to add LB virtual IPs (for application users and for data collectors if needed) to the hosts file on BSM gateway.

After pressing Login, nothing happens. Or user logs in, but Sitemap is empty.

Possible Cause:

You are trying to login to BSM from the Windows Server instead of the client machine. On Windows Server, the Internet Explorer Enhanced Security Configuration is typically enabled. With this configuration, several BSM UI features including BSM login page, may not work.

Resolution:

Check if the Internet Explorer Enhanced Security Configuration is enabled. If it is enabled, use a regular client for login, and not the Windows server.

If you must login from the server, either disable Internet Explorer Enhanced Security Configuration (**Control Panel > Add/remove Windows components**) or add the BSM URL to the trusted sites in the IE Security Settings.

After restart, service reassigned to backup DPS server

Possible Cause:

If you enabled automatic failover as well as set the **keep alive timeout** to less than ten minutes, this can cause BSM services to move to the backup server after a restart.

Resolution:

To prevent this from happening, when disabling BSM, shut down the backup server before the primary server. When enabling BSM, enable the primary server and verify that all services have started before enabling the backup server.