

HP Business Service Management

For the Windows and Linux Operating Systems

Software Version: 9.20

BSM Upgrade Guide - 9.1x to 9.20

Document Release Date: November 2012

Software Release Date: August 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 Notice

© 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 (www.apache.org).

This product includes software developed by the JDOM Project (www.jdom.org).

This product includes software developed by the MX4J project (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.

This document was last updated: Thursday, November 08, 2012

Support

Visit the HP Software Support Online 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

Contents

BSM Upgrade Guide - 9.1x to 9.20	1
Contents	5
Introduction	8
Staging vs. Direct Upgrade Overview	9
Direct Upgrade	10
Overview of BSM 9.1x to BSM 9.2x Direct Upgrade	11
Prerequisites	13
General Prerequisites	14
Installation Prerequisites - Windows	16
Installation Prerequisites - Linux	17
Install the Latest BSM 9.1x Patches	18
Configure HPOM Event Buffering	19
Pre-Upgrade Tool	20
Uninstall BSM 9.1x	22
Install BSM 9.20	24
Merge SHA analytics metadata	25
Configure Event Traffic when using OM Agent 8.60	26
9.20 Upgrade Wizard	27
Post-Installation Procedures	28
General Post-Installation Procedures	29
Starting and Stopping BSM	34
Logging In and Out	35
Add Additional BSM Servers	36
Staging Upgrade	37
Overview of BSM 9.1x to BSM 9.20 Staging Upgrade	38
Prerequisites	39
General Prerequisites	40

Installation Prerequisites - Windows	43
Installation Prerequisites - Linux	44
Install the Latest BSM 9.1x Patches	45
Configure HPOM Event Buffering	46
Pre-Upgrade Tool	47
Install BSM 9.20	49
Merge SHA analytics metadata	50
OMi Mid-Upgrade Procedure	51
Replicate Database	53
Configure Event Traffic when using OM Agent 8.60	54
9.20 Upgrade Wizard	55
Staging Mode	56
Staging Data Replicator	57
Staging Data Replicator - Overview	58
Running the Staging Data Replicator (Embedded)	59
Running the Staging Data Replicator (Standalone)	60
Verifying that the SDR Server Can Communicate with the Production Server	62
Unsubscribing the Staging Data Replicator from the Source Server	63
Running the SDR with Basic Authentication	64
SSL Configuration for the Staging Data Replicator	65
Post-Installation Procedures	66
General Post-Installation Procedures	67
Starting and Stopping BSM	72
Logging In and Out	73
Add Additional BSM Servers	74
Complete the Upgrade Process	75
OMi Post-upgrade Procedure	78
Appendix	83
Installing BSM on a Linux Platform	84
Prepare Information Required for Installation	85
Working with the Web Server	86
Installing BSM Servers	87

Installing BSM on a Windows Platform	89
Prepare Information Required for Installation	90
Working with the Web Server	92
Installing BSM Servers	93
Server Deployment and Setting Database Parameters	96
Setup and Database Configuration Utility Overview	97
Setting Database Parameters	98
Required Information for Setting Database Parameters	100
Running the Setup and Database Configuration Utility	102
Upgrade Wizard	105
Upgrade Wizard Overview	106
Preparing Information for the Upgrade Wizard	107
Changing BSM Service Users	108
Upgrading SLAs from BSM 9.x to 9.20 to Work with Baselining	109
Troubleshooting	115
Troubleshooting Resources	116
Installation and Connectivity Troubleshooting	117
Troubleshooting the Upgrade Process	123
Troubleshooting the 9.1x Upgrade Wizard	124

Chapter 1

Introduction

Welcome to the BSM Upgrade Guide. This guide provides a detailed workflow for how to upgrade BSM.

How This Guide is Organized

This book is divided into three sections:

- Section 1 contains the workflow for upgrading using the direct method
- Section 2 contains the workflow for upgrading using the staging method
- Section 3, the appendix, contains reference information that applies to both the staging and upgrade workflows

You should select either the staging or direct workflow. Whichever workflow is chosen should be read and executed in chronological order where relevant.

Chapter 2

Staging vs. Direct Upgrade Overview

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

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 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 servers are functioning as required before disconnecting the original servers.

When upgrading using a staging environment, BSM is installed on the staging servers. Staging mode begins when both production and staging servers are installed. During staging mode, metric data is transferred from the production server to the staging server using the Staging Data Replicator (SDR). Event data is forwarded using a different method.

Only changes to the database are transferred during staging mode, configuration changes made to the production server are not transferred.

Note:

- Scheduled reports are not sent from the staging servers while in staging mode. For more details, see ["Troubleshooting the Upgrade Process" on page 123](#)
- 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.
- There are no BPI components or menus available within BSM or BPI menus until BSM is switched from staging to production environment mode. The Modeler, Process Repository, and the BPI Process Diagram are disabled as part of the upgrade to BSM to protect your BPI data.
- You must upgrade using a staging environment if you are switching operating systems. In BSM 9.2x, Windows Server 2003 is no longer supported, such users would have to perform a staging upgrade to a supported operating system.

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.

This book is divided into three sections:

- Section 1 contains the workflow for upgrading using the direct method.
- Section 2 contains the workflow for upgrading using the staging method
- Section 3 contains reference information that applies to both the staging and direct workflows

Part 1

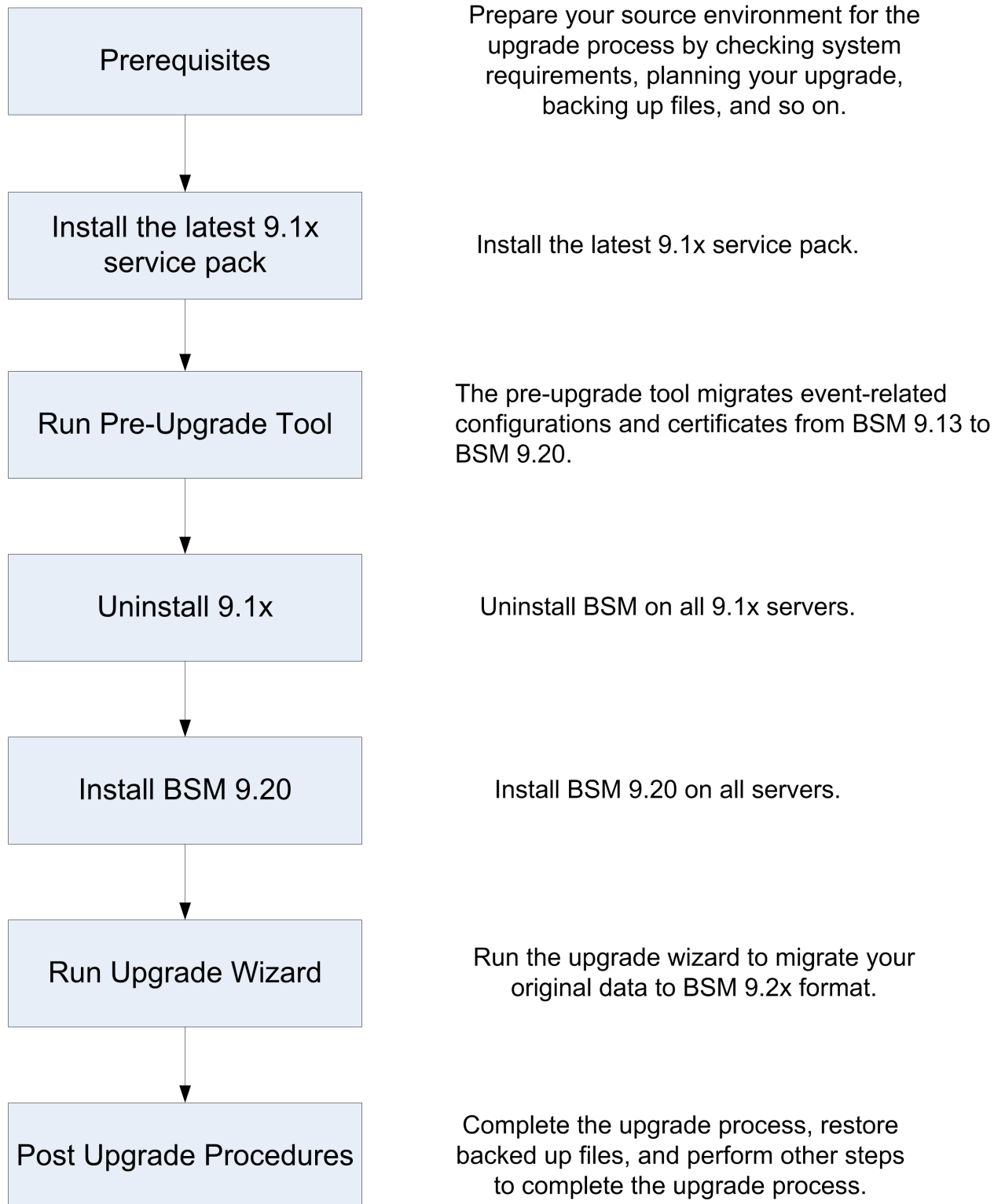
Direct Upgrade

This section contains the workflow for upgrading BSM using the direct method.

Chapter 3

Overview of BSM 9.1x to BSM 9.2x Direct Upgrade

The upgrade from BSM 9.1x to BSM 9.2x involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Chapter 4

Prerequisites

Perform all steps specified in this chapter before continuing with the upgrade process.

- General Prerequisites 14
- Installation Prerequisites - Windows 16
- Installation Prerequisites - Linux 17
- Install the Latest BSM 9.1x Patches 18
- Configure HPOM Event Buffering 19
- Pre-Upgrade Tool 20

General Prerequisites

Perform the following steps where relevant before continuing with the upgrade process.

1. Create deployment plan

Create a complete deployment plan including the required software, hardware, and components. For details, see the BSM Planning Guide and the BSM System Requirements and Support Matrixes.

2. Create upgrade plan

Create an upgrade plan including such items as whether you will be performing a staging or direct upgrade, estimated down-time, and so on.

Database Administrator. During the upgrade process, the services of your Database Administrator may be required.

Multiple servers. If you are upgrading multiple BSM servers, perform the upgrade procedure on only one Gateway and one Data Processing server. When the upgrade process is complete, install any additional servers and connect them to the database schemas using Configuration Wizard as described in the BSM Installation Guide.

3. Order and register licenses

Order licenses with a sales representative based on your deployment plan. Register your copy of BSM 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 BSM on the HP Software Support site <http://www.hp.com/go/hpsupport>.

4. Set up database server

Note: You cannot change the database type during the upgrade if you want to keep your configuration and runtime data. For example, if you currently run Oracle, you must also use Oracle with the new BSM environment.

In BSM 9.20, support for SQL Server 2005 was removed. Make sure your database is supported and the compatibility parameter is up-to-date before starting the upgrade.

Verify that your database has the following settings:

- Oracle: The Oracle Partitioning option must be enabled. Make sure that the parameter **RECYCLEBIN** is set to **Off**, as specified in the BSM Database Guide.

For information about setting up your database server, see the BSM Database Guide.

5. Migrate 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**).

6. 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.

7. Back up files

Back up the following files from your original BSM servers:

- <Gateway Server installation directory>/AppServer/webapps/site.war/openapi/excels directory
- <Data Processing Server installation directory>/cmdb/general directory
- <Data Processing Server installation directory>/BLE/rules/<custom rules jar> file(s)
- <Gateway Server installation directory>/JRE/lib/security/cacerts
- <Gateway Server installation directory>/JRE64/lib/security/cacerts

8. Back up SHA analytics metadata (SHA only)

This procedure is only relevant for Service Health Analyzer users.

If you manually modified the SHA analytics metadata, the changes will be overwritten during the upgrade process. In order to prevent this, back up the relevant files before the upgrade and merge them with the new files after BSM 9.20 is installed.

Back up the following directory: **<SHA analytics server installation directory>/conf/analytics/metadata/default**

9. Disable RTSM integrations (optional)

If integrations are configured in the RTSM Integration Studio (for example, topology synchronization integrations between central UCMDb and RTSM), after upgrading, the Data Flow Probe will run population jobs immediately for active integration points, even if the integration is not scheduled. If you do not want the integration to run, disable the integration before running the upgrade from any BSM 9.x version.

Installation Prerequisites - Windows

Note the following before installing BSM servers on a Windows platform:

- It is recommended that you install BSM servers to a drive with at least 20 GB of free disk space. For more details on server system requirements, see the BSM 9.20 System Requirements and Support Matrixes.
- If BSM 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 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.
- BSM servers must be installed on dedicated machines and must not run other applications. However, the coexistence of BSM servers with SiteScope or 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.
- BSM 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 BSM site when using Microsoft Internet Explorer 7.0 or later.
- During BSM server installation, you can specify a different path for the BSM 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.
- If you plan to run BSM servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the BSM Hardening Guide.
- **Note:** 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.

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.

Installation Prerequisites - Linux

Note the following before installing BSM servers on a Linux platform:

- It is recommended that you install BSM servers to a drive with at least 20 GB of free disk space. For more details on server system requirements, see the BSM System Requirements and Support Matrixes.
- If BSM 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 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.
- BSM servers must be installed on dedicated machines and must not run other applications. However, the coexistence of BSM servers with HP SiteScope or Operations Manager agent has been tested and is supported.
- Before installing BSM on a linux machine, make sure that SELinux will not block it. You can do this by either disabling SELinux, or configuring it to enable java 32-bit to run.
 - To disable SELinux, open the `/etc/selinux/config` file, set the value of **SELINUX=disabled**, and reboot the machine.
 - To configure SELinux to enable java 32-bit to run, execute the command **setsebool -P allow_execmod on**.
- BSM 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 BSM site. To access the BSM site in this case, use the machine's IP address instead of the machine name containing the underscore.
- If you plan to run BSM servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the BSM Hardening Guide.
- You must be a root user to install BSM on the server machine.
- The **DISPLAY** environment variable must be properly configured on the BSM server machine. The machine from which you are installing must be running an X-Server.

Install the Latest BSM 9.1x Patches

Install the latest patches on the BSM 9.1x environment.

1. Prerequisites

- Before installing a BSM patch, it is recommended that you back up all BSM databases.
- Before installing a BSM patch, 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 latest patch and intermediate patch from the SSO site

- a. Go to the SSO site:
<http://support.openview.hp.com/selfsolve/patches>
- b. Select **Application Performance Management (BAC)** and select the most recent patch.
- c. Click **Search** to locate the installation files.
- d. Save the package locally and launch the relevant setup file to install the patch.
- e. Run the installation files on all BSM servers (Gateway and Data Processing).
- f. Run the post-installation wizard. This wizard follows the patch installation automatically.
- g. Repeat this procedure for the latest intermediate patch.

3. Re-apply manual changes

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

Configure HPOM Event Buffering

If you were using HPOM to forward events to BSM, perform this procedure:

During the migration, HPOM continues to attempt sending events to the BSM 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 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. Note the values of **Forwarding delivery timeout (in seconds)** and **Forwarding queue size maximum (in megabytes)**. Record these values to enable you to restore them after the upgrade.
4. Change the value of **Forwarding delivery timeout (in seconds)** (default 1 hour). For example, to set the timeout to 7 days, type **604800**.
5. 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**.
6. *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**.
7. 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. *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. Record these values to enable you to restore them after the upgrade.
2. Adjust the timeout. For example, to set the timeout to 2 days, type:
ovconfchg -ovrg server -ns opc.opcforwm -set REQUEST_TIMEOUT 604800
3. *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>

Note: When the upgrade is complete, you can restore the original values of the buffer.

Pre-Upgrade Tool

The pre-upgrade tool temporarily stores some configuration and certificates in the BSM database to help migrate them to 9.20. It should be run on all BSM Gateway and DPS servers.

1. Run the Pre-Upgrade Tool on a Gateway Server

On one up-to-date BSM Gateway Server, run the PreUpgradeTool using the following command.

- **Linux:** <HPBSM Install Directory>/opr/bin/PreUpgradeTool.sh -d
- **Windows:** <HPBSM Install Directory>\opr\bin\PreUpgradeTool.bat -d

2. Run the Pre-Upgrade Tool on the Active Data Processing Server

On the active BSM Data Processing Server, run the PreUpgradeTool using the following command.

- **Linux:** <HPBSM Install Directory>/opr/bin/PreUpgradeTool.sh -d
- **Windows:** <HPBSM Install Directory>\opr\bin\PreUpgradeTool.bat -d

If there is a large number of closed events stored in the database, upgrading can take a long time. If recommended by the tool, and you want to archive closed events before upgrading starts, enter "Yes" (y) when prompted and specify the target location for the archive file.

Additional Information

Install the latest patches to get the newest version of the Pre-upgrade tool. The tool should first be run on a Gateway Server and then on the active Data Processing Server.

The Pre-Upgrade Tool executes the following steps:

- Backs up files required by the upgraded 9.2x installation (event sync scripts, certificates, and so on)
- Ensures the Sonic Queue is emptied
- Gives the customer the ability to shorten the upgrade process by choosing to not upgrade closed events

Note: If you did not run the Pre-Upgrade Tool before shutting down or uninstalling BSM 9.1x, the following will not be migrated to the 9.20 installation:

- Certificate data including trust relationships for connected servers.
- If you have created Groovy scripts in your BSM 9.1x environment, these scripts are not imported to your BSM 9.20 installation.
- Events from your BSM 9.1x environment may be lost.

In this case, you should execute the following steps manually on your BSM 9.20 installation after the upgrade is successfully completed:

- Define trust relationships for connected servers. For details, see the OMi Setup section of the BSM Application Administration Guide.
- If you have any Groovy scripts that are used to forward events, import them from your production environment if possible.

Chapter 5

Uninstall BSM 9.1x

Disable BSM on all 9.1x servers by selecting **Start > Programs > HP Business Service Management > Administration > Disable HP Business Service Management**.

Uninstall BSM 9.1x on all servers using one of the following procedures:

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 BSM uninstall script to remove any present updates, and follow the on-screen instructions when prompted.

Note: In some cases, this process may take a long time (more than 30 minutes)

Note: When a Minor-Minor BSM Release (for example, 9.01) is removed, any BSM Public Patches installed on top of the release are removed, as well.

3. If the **Show Updates** check box is selected, all the updates installed over BSM are displayed. When BSM is removed, all updates are also removed.
4. Restart the server machine.

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 BSM 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_<version>_HPOvInstaller.txt** log file located in the **/tmp** directory for errors. Previous installation files can be found in the **/tmp/HPOvInstaller/HPBsm_<version>** directory.

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

Chapter 6

Install BSM 9.20

Install BSM 9.20 on a set of BSM servers. This set can be either one Gateway Server and one Data Processing Server or a single one-machine server. In the first case, run the wizards on the Data Processing Server first. The wizard will direct you as to when to begin installation on the Gateway Server.

Run the installation and post-installation wizards. Do not run the upgrade wizard yet. Exit the wizard on the last screen of the post-installation wizard without continuing.

- For Windows:

DVD1 > windows_setup > HPBsm_9.20_setup.exe

- For Linux:

DVD2 > linux_setup > HPBsm_9.20_setup.bin

For more details, see the following sections:

- ["Installing BSM on a Linux Platform" on page 84](#)
- ["Installing BSM on a Windows Platform" on page 89](#)

Chapter 7

Merge SHA analytics metadata

If you backed up your SHA analytics metadata, your manual changes should now be merged onto the new files.

Open any files that had manual changes in the backed up directory:

<SHA analytics server installation directory>/conf/analytics/metadata/default

Merge them using a text editor onto the same files in the following directory:

<Data Processing Server installation directory>/conf/analytics/metadata/default

Chapter 8

Configure Event Traffic when using OM Agent 8.60

If you installed BSM on a Linux machine with OM Agent 8.60, you must run the batch processes below. If you do not run them, the connection of the OM Agent on the BSM server with the OM server may be broken.

Run the following batch processes on all BSM machines (GW and DPS):

- `/opt/OV/lbin/bbc/install/configure.sh`
- `/opt/OV/lbin/xpl/install/configure.sh`

Chapter 9

9.20 Upgrade Wizard

Run the upgrade wizard on all 9.2x machines to transfer your data from the original 9.1x format to the 9.2 format.

The upgrade wizard can be found on all Gateway, Data Processing, and One-machine servers in the following locations:

- Windows:

<BSM Home Directory>\bin\upgrade_wizard_run_from91.bat

- Linux:

/opt/HP/BSM/bin/upgrade_wizard_run_from91.sh

For details about the upgrade wizard, see ["Upgrade Wizard" on page 105](#)

Chapter 10

Post-Installation Procedures

Perform these tasks to complete the upgrade process.

- General Post-Installation Procedures29
- Starting and Stopping BSM 34
- Logging In and Out35
- Add Additional BSM Servers36

General Post-Installation Procedures

Perform these tasks to complete the upgrade process.

• Service Health and SLM repository 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 9.12, 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.

• Service Health Top View post-upgrade

In BSM 9.20, extensive improvements were made to the Top View component. For details, refer to the sections on Top View in the BSM User Guide and in the BSM Application Administration Guide.

As a result of the changes made to the underlying Top View infrastructure, the following infrastructure settings from earlier BSM versions are now deprecated in BSM 9.20:

- **Top View Data Refresh Rate - For Legacy MyBSM**
- **Top View Font Name**
- **Top View Green Color Property**

These infrastructure settings were located in the Service Health Application - Top View Properties section of the Service Health Application infrastructure settings. If you customized these settings prior to upgrade, your customizations are removed.

In addition, if you used a custom background image for Top View, after upgrade save the image in `<Gateway Server root directory>/AppServer/webapps/site.war/images/topview`, and enter the image file name in the **Custom Background Image Name** infrastructure setting.

• **SLM - Upgrading SLAs from BSM 9.x to 9.20 using Baselining**

The following section is only relevant for users who you have SLAs with BPM transaction CIs with the BPM Percentile Sample-Based rule defined on performance HIs, or Groovy rule (Rules API).

BSM 9.20 introduces the concept of baselining. In End User Management, Business Process Monitor performance metrics are analyzed over a period of time, and are used to provide a baseline comparison for establishing acceptable performance ranges.

Baselining influences the transaction thresholds, and will therefore have an impact on your SLA calculation. If you want to minimize this influence so that your SLA calculation results are similar to pre-baselining, perform the steps described in "[Upgrading SLAs from BSM 9.x to 9.20 to Work with Baselining](#)" on page 109 .

• **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 9.2x Data Processing Server:

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

• **Upgrade custom reports**

In some cases, custom reports are not migrated properly during the upgrade. If this is the case, execute the following command from the JMX console as follows:

- a. Open the JMX console from **`http://<DNS of BSM Gateway server>/jmx-console/`**
- b. In the Topaz section, select **EUM Custom report upgrader service**.
- c. Complete the fields and click Invoke.

• **Delete temporary internet files**

When logging into BSM for the first time after upgrading, delete the browser's temporary Internet files. This should be done on each browser that accesses BSM.

• **SHA baseline data**

The following note is relevant if you were using SHA with Performance or Operations Agents which include one of the following SPIs: WebLogic, WebSphere, Oracle, MSSQL.

The baseline may be inaccurate for at least one week after running the upgrade wizard. This is due to an improvement in the way instances in the SPIs are interpreted by SHA.

- **Disable firewall between BSM servers**

In general, placing firewalls between BSM servers is not supported. If an operating system firewall is active on any BSM server machine (GW or DPS), a channel must be left open to allow traffic between the BSM machines (GW and DPS).

- **Copy files from production server or restore them from backup**

Restore the following files from the production server or from backup to the new BSM servers:

- <Gateway Server installation directory>/AppServer/webapps/site.war/openapi/excels directory
- <Data Processing Server installation directory>/cmdb/general directory
- <Data Processing Server installation directory>/BLE/rules/<custom rules jar> file(s)
- <Gateway Server installation directory>/JRE/lib/security/cacerts
- <Gateway Server installation directory>/JRE64/lib/security/cacerts

- **Reconfigure Integration with HPOM**

This procedure is only required if you are performing a staging upgrade. If you had previously configured an integration with HPOM, repeat the following procedure that you performed when configuring this connection for the first time: "How to Set Up a Forwarding Target in the HPOM for UNIX Node Bank" in the BSM - Operations Manager Integration Guide.

- **Perform hardening procedures**

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 BSM Hardening Guide.

- **Ensure all processes started properly**

You can check to ensure that all processes started properly. For details, see "How to View the Status of Processes and Services" in the BSM Platform Administration Guide.

- **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`).

• Overwrite custom changes (optional)

BSM 9.20 comes with built in content packs. If any of the data in these content packs conflicts with a previously existing custom change, BSM keeps the custom change and does not overwrite it.

To overwrite your custom changes with the new 9.20 data:

- a. Open the Content Packs page from **Admin > Platform > Content Packs**.
- b. Select each content pack. In the content pack summary, there is a column indicating the origin of each artifact. For each item whose value is **predefined (customized)**, this indicates that the artifact was customized and is different from the one delivered with 9.20.
- c. To overwrite a change, locate the artifact in the corresponding admin user interface and select **restore to default**.

• 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 108](#).

• Install component setup files

The component setup files are used to install the components used by BSM. The component setup files are not installed as part of the basic BSM installation. They are located separately in

the Web delivery package download area and in the **Data Collectors and Components\components** directory of the BSM DVDs and must be installed separately to the BSM Downloads page. The component setup files can then be downloaded from BSM and used when required. For details on working with the BSM Downloads page, see "Downloads Overview" in the BSM Platform Administration Guide.

You must run all DVDs provided for installation to enable downloading all the BSM 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 BSM after the component's setup files are copied to the Downloads page.

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 BSM.

- **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 BSM 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 BSM 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 BSM Downloads page:

- i. Insert the BSM DVD into the drive of the BSM Gateway Server on which you want to copy the component setup files.
- ii. 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**.
- iii. Follow the on-screen instructions to complete the wizard.

Starting and Stopping BSM

After completing the BSM 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 before restarting the machine.

After installing the BSM 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 BSM on each server machine.

Note: You can check which BSM servers and features are installed on a BSM server machine by viewing the [INSTALLED_SERVERS] section of the **<BSM 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 BSM 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 BSM in Linux:

```
/opt/HP/BSM/scripts/run_hpbsm start | stop
```

To start, stop, or restart BSM using a daemon script:

```
/etc/init.d/hpbsmd {start| stop | restart}
```

Note: When you stop BSM, the BSM service is not removed from Microsoft's Services window. The service is removed only after you uninstall BSM.

Logging In and Out

You log in to BSM from a client machine's browser using the login page. LW-SSO is BSM's default authentication strategy. For details, see "Logging into BSM with LW-SSO" in the BSM Platform Administration Guide.

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 the BSM Platform Administration Guide.

Tip: For complete login help, click the **Help** button on the login page.

To access the BSM 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 BSM server. If there are multiple servers, or if BSM is deployed in a distributed architecture, specify the load balancer or Gateway Server URL, as required.

Note: Users running previous versions of BSM can still use bookmarks set to access the URL `http://<server_name>.<domain_name>/mercuriam` 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 BSM system, see "User Management" in the BSM Platform Administration Guide.

Note:

- For login troubleshooting information, see "Troubleshooting and Limitations" in the BSM Platform Administration Guide.
- For details on login authentication strategies that can be used in BSM, see "Authentication Strategies — Overview" in the BSM Platform Administration Guide.
- For details on accessing BSM securely, see the BSM Hardening Guide.

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.

Add Additional BSM Servers

Now that you have a complete, upgraded 9.20 environment, you can add new Gateway and Data Processing servers as desired.

To add new BSM servers to an existing BSM environment:

1. Run the installation and post-installation wizards.

- Windows:

DVD1 > windows_setup > HPBsm_9.20_setup.exe

For more details, see ["Installing BSM on a Windows Platform" on page 89](#)

- Linux:

DVD2 > linux_setup > HPBsm_9.20_setup.bin

For more details, see ["Installing BSM on a Linux Platform" on page 84](#)

2. Run the Setup and Database Configuration utility.

Select the option to run the configuration utility at the end of the post-installation utility to connect the servers to the staging database server. For more details about this utility, see the BSM 9.20 Installation Guide.

Part 2

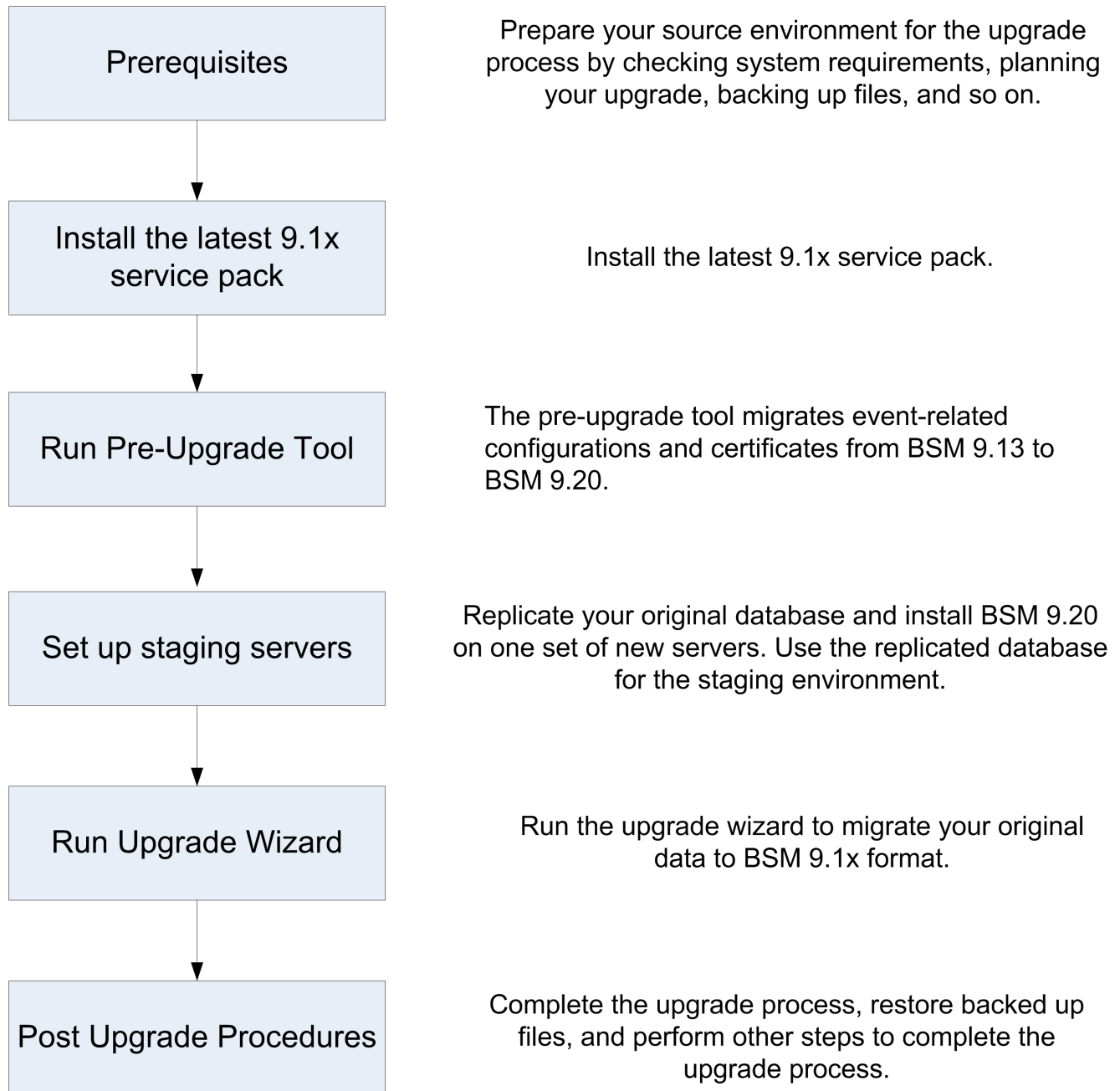
Staging Upgrade

This section contains the workflow for upgrading BSM using the staging method.

Chapter 11

Overview of BSM 9.1x to BSM 9.20 Staging Upgrade

The upgrade from BSM 9.1x to BSM 9.20 involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Chapter 12

Prerequisites

Perform all steps specified in this chapter before continuing with the upgrade process.

- General Prerequisites 40
- Installation Prerequisites - Windows 43
- Installation Prerequisites - Linux 44
- Install the Latest BSM 9.1x Patches 45
- Configure HPOM Event Buffering 46
- Pre-Upgrade Tool 47

General Prerequisites

Perform the following steps where relevant before continuing with the upgrade process.

1. Create deployment plan

Create a complete deployment plan including the required software, hardware, and components. For details, see the BSM Planning Guide and the BSM System Requirements and Support Matrixes.

2. Create upgrade plan

Create an upgrade plan including such items as whether you will be performing a staging or direct upgrade, estimated down-time, and so on.

Allocate additional disk space. The database replication requires 1.5 times the amount of disk space in your original (production) database. If you want to save original data by selecting this option in the upgrade wizard, you will need two times the amount of disk space in your original database.

Staging Data Replicator. 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 57.

Database Administrator. During the upgrade process, the services of your Database Administrator may be required.

Multiple servers. If you are upgrading multiple BSM servers, perform the upgrade procedure on only one Gateway and one Data Processing server. When the upgrade process is complete, install any additional servers and connect them to the database schemas using Configuration Wizard as described in the BSM Installation Guide.

3. Order and register licenses

Order licenses with a sales representative based on your deployment plan. Register your copy of BSM 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 BSM on the HP Software Support site <http://www.hp.com/go/hpsoftwaresupport>.

4. Set up database server

Note: You cannot change the database type during the upgrade if you want to keep your configuration and runtime data. For example, if you currently run Oracle, you must also use Oracle with the new BSM environment.

In BSM 9.20, support for SQL Server 2005 was removed. Make sure your database is supported and the compatibility parameter is up-to-date before starting the upgrade.

Verify that your database has the following settings:

- Oracle: The Oracle Partitioning option must be enabled. Make sure that the parameter **RECYCLEBIN** is set to **Off**, as specified in the BSM Database Guide.
- SQL: 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 BSM Database Guide.

5. Migrate operating systems (optional)

- BSM supports switching the operating systems of your Gateway and Data Processing servers if you are upgrading in staging mode (for example, from Windows to Linux).
- BSM supports switching the operating system of your database server during the upgrade (staging and direct) provided that this is also supported by your database vendor.
- BSM 9.2x no longer supports Windows Server 2003. Windows Server 2003 users upgrading to BSM 9.2x must perform a staging upgrade and must switch to a supported operating system.

6. Set up web server (optional)

BSM installs the Apache web server on all BSM Gateway servers during the installation. If you would like to use the IIS web server, install it on all Gateway servers before installing BSM.

7. Resolve time zone inconsistencies

All BSM machines in the staging environment must be set to the same time zone, daylight savings time, and time as the source environment. This includes BSM Gateway, Data Processing, and Database servers. Incompatible time zone settings can lead to inaccuracies in reporting historical data.

8. Migrate 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**).

9. 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.

10. Back up SHA analytics metadata (SHA only)

This procedure is only relevant for Service Health Analyzer users.

If you manually modified the SHA analytics metadata, the changes will be overwritten during the upgrade process. In order to prevent this, back up the relevant files before the upgrade and merge them with the new files after BSM 9.20 is installed.

Back up the following directory: **<SHA analytics server installation directory>/conf/analytics/metadata/default**

11. **Disable RTSM integrations (optional)**

If integrations are configured in the RTSM Integration Studio (for example, topology synchronization integrations between central UCMDB and RTSM), after upgrading, the Data Flow Probe will run population jobs immediately for active integration points, even if the integration is not scheduled. If you do not want the integration to run, disable the integration before running the upgrade from any BSM 9.x version.

Installation Prerequisites - Windows

Note the following before installing BSM servers on a Windows platform:

- It is recommended that you install BSM servers to a drive with at least 20 GB of free disk space. For more details on server system requirements, see the BSM 9.20 System Requirements and Support Matrixes.
- If BSM 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 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.
- BSM servers must be installed on dedicated machines and must not run other applications. However, the coexistence of BSM servers with SiteScope or 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.
- BSM 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 BSM site when using Microsoft Internet Explorer 7.0 or later.
- During BSM server installation, you can specify a different path for the BSM 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.
- If you plan to run BSM servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the BSM Hardening Guide.
- **Note:** 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.

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.

Installation Prerequisites - Linux

Note the following before installing BSM servers on a Linux platform:

- It is recommended that you install BSM servers to a drive with at least 20 GB of free disk space. For more details on server system requirements, see the BSM System Requirements and Support Matrixes.
- If BSM 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 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.
- BSM servers must be installed on dedicated machines and must not run other applications. However, the coexistence of BSM servers with HP SiteScope or Operations Manager agent has been tested and is supported.
- Before installing BSM on a linux machine, make sure that SELinux will not block it. You can do this by either disabling SELinux, or configuring it to enable java 32-bit to run.
 - To disable SELinux, open the `/etc/selinux/config` file, set the value of **SELINUX=disabled**, and reboot the machine.
 - To configure SELinux to enable java 32-bit to run, execute the command **setsebool -P allow_execmod on**.
- BSM 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 BSM site. To access the BSM site in this case, use the machine's IP address instead of the machine name containing the underscore.
- If you plan to run BSM servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the BSM Hardening Guide.
- You must be a root user to install BSM on the server machine.
- The **DISPLAY** environment variable must be properly configured on the BSM server machine. The machine from which you are installing must be running an X-Server.

Install the Latest BSM 9.1x Patches

Install the latest patches on the BSM 9.1x environment.

1. Prerequisites

- Before installing a BSM patch, it is recommended that you back up all BSM databases.
- Before installing a BSM patch, 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 latest patch and intermediate patch from the SSO site

- a. Go to the SSO site:

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

- b. Select **Application Performance Management (BAC)** and select the most recent patch.
- c. Click **Search** to locate the installation files.
- d. Save the package locally and launch the relevant setup file to install the patch.
- e. Run the installation files on all BSM servers (Gateway and Data Processing).
- f. Run the post-installation wizard. This wizard follows the patch installation automatically.
- g. Repeat this procedure for the latest intermediate patch.

3. Re-apply manual changes

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

Configure HPOM Event Buffering

If you were using HPOM to forward events to BSM, perform this procedure:

During the migration, HPOM continues to attempt sending events to the BSM 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 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. Note the values of **Forwarding delivery timeout (in seconds)** and **Forwarding queue size maximum (in megabytes)**. Record these values to enable you to restore them after the upgrade.
4. Change the value of **Forwarding delivery timeout (in seconds)** (default 1 hour). For example, to set the timeout to 7 days, type **604800**.
5. 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**.
6. *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**.
7. 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. *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. Record these values to enable you to restore them after the upgrade.
2. Adjust the timeout. For example, to set the timeout to 2 days, type:
ovconfchg -ovrg server -ns opc.opcforwm -set REQUEST_TIMEOUT 604800
3. *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>

Note: When the upgrade is complete, you can restore the original values of the buffer.

Pre-Upgrade Tool

The pre-upgrade tool temporarily stores some configuration and certificates in the BSM database to help migrate them to 9.20. It should be run on all BSM Gateway and DPS servers.

1. Run the Pre-Upgrade Tool on a Gateway Server

On one up-to-date BSM Gateway Server, run the PreUpgradeTool using the following command.

- **Linux:** <HPBSM Install Directory>/opr/bin/PreUpgradeTool.sh -s
- **Windows:** <HPBSM Install Directory>\opr\bin\PreUpgradeTool.bat -s

2. Run the Pre-Upgrade Tool on the Active Data Processing Server

On the active BSM Data Processing Server, run the PreUpgradeTool using the following command.

- **Linux:** <HPBSM Install Directory>/opr/bin/PreUpgradeTool.sh -s
- **Windows:** <HPBSM Install Directory>\opr\bin\PreUpgradeTool.bat -s

If there is a large number of closed events stored in the database, upgrading can take a long time. If recommended by the tool, and you want to archive closed events before upgrading starts, enter "Yes" (y) when prompted and specify the target location for the archive file.

Additional Information

Install the latest patches to get the newest version of the Pre-upgrade tool. The tool should first be run on a Gateway Server and then on the active Data Processing Server.

The Pre-Upgrade Tool executes the following steps:

- Backs up files required by the upgraded 9.2x installation (event sync scripts, certificates, and so on)
- Ensures the Sonic Queue is emptied
- Gives the customer the ability to shorten the upgrade process by choosing to not upgrade closed events

Note: If you did not run the Pre-Upgrade Tool before shutting down or uninstalling BSM 9.1x, the following will not be migrated to the 9.20 installation:

- Certificate data including trust relationships for connected servers.
- If you have created Groovy scripts in your BSM 9.1x environment, these scripts are not imported to your BSM 9.20 installation.
- Events from your BSM 9.1x environment may be lost.

In this case, you should execute the following steps manually on your BSM 9.20 installation after the upgrade is successfully completed:

- Define trust relationships for connected servers. For details, see the OMi Setup section of the BSM Application Administration Guide.
- If you have any Groovy scripts that are used to forward events, import them from your production environment if possible.

Chapter 13

Install BSM 9.20

Install BSM 9.20 on a set of staging servers. This set can be either one Gateway Server and one Data Processing Server or one one-machine server. In the first case, run the wizards on the Data Processing Server first. The wizard will direct you as to when to begin installation on the Gateway Server.

Run the installation and post-installation wizards. Do not run the upgrade wizard yet. Exit the wizard on the last screen of the post-installation wizard without continuing.

- For Windows:

DVD1 > windows_setup > HPBsm_9.20_setup.exe

- For Linux:

DVD2 > linux_setup > HPBsm_9.20_setup.bin

For more details, see the following sections:

- ["Installing BSM on a Linux Platform" on page 84](#)
- ["Installing BSM on a Windows Platform" on page 89](#)

Chapter 14

Merge SHA analytics metadata

If you backed up your SHA analytics metadata, your manual changes should now be merged onto the new files.

Open any files that had manual changes in the backed up directory:

<SHA analytics server installation directory>/conf/analytics/metadata/default

Merge them using a text editor onto the same files in the following directory:

<Data Processing Server installation directory>/conf/analytics/metadata/default

Chapter 15

OMi Mid-Upgrade Procedure

If you were using OMi with BSM 9.1x, perform the following steps on the production server:

Configure the BSM production server to forward events to the staging server

Events coming into the production environment should also be forwarded to the new staging environment. These events will be queued in the Operations Management EVENT_SYNC_BUFFER DB table until the BSM 9.20 staging server is up and running.

Note: Make sure the Operations Management Database has enough disk space available to hold the events until the staging server is ready to receive them. A general estimate the required space is 2 KB per event that will occur during this time period.

1. In the production server, go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. In the **applications** field, select **Operations Management** and locate the **Event Forwarding Settings** table
3. In the **Target Server for Forward All** setting, enter the DNS of the staging BSM Gateway server.
4. In the **Forward All** setting, set the value to **true**.

Configure Special Event Type Forwarding

If you were forwarding events of one of the following event types:

Notify, Notify and Update, Synchronize

You need to perform the following procedure to ensure the forwarding information is correctly synchronized from the production server to the staging server.

1. Configure a Connected Server:
 - a. Go to **Administration > Operations Management > Tune Operations Management > Connected Servers**.
 - b. Add a server using the New button with the following properties

Server Type	External Event Processing
--------------------	---------------------------

Server Properties	Target Server: upgrade.server
Integration Type	Select Call Groovy Script Adapter <ul style="list-style-type: none">◦ External Event Processing Type: upgrade◦ Groovy Script File Name: UpgradeAdapter
Outgoing Connection	Connection Credentials: username and password of admin user (must be a super user) Select Use Secure HTTP if the staging server will require SSL and the port number the staging server will require for client connections
Event Drilldown	Fully Qualified DNS Name: DNS name of the staging Gateway server (not the Load Balancer)

2. Go to **Administration > Operations Management > Tune Operations Management > Forwarding Rules**. For each existing forwarding rule that forwards the events of this type, add the above target server to the forwarding rule with forwarding type **Notify**. The forwarding script will synchronize the forwarding information changes that occur after the DB backup starts to the staging server.

Chapter 16

Replicate Database

Replicate your original database as explained in the following procedure:

1. Replicate your original database schema onto a new database server. This server will be used by the staging environment.
2. On the production server, enable event receiving as follows:

Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

In the **applications** field, select **Operations Management** and locate the **Event Pipeline Receiver Settings** table. Set **Disable receiving of Events** to **false**.

Chapter 17

Configure Event Traffic when using OM Agent 8.60

If you installed BSM on a Linux machine with OM Agent 8.60, you must run the batch processes below. If you do not run them, the connection of the OM Agent on the BSM server with the OM server may be broken.

Run the following batch processes on all BSM machines (GW and DPS):

- `/opt/OV/lbin/bbc/install/configure.sh`
- `/opt/OV/lbin/xpl/install/configure.sh`

Chapter 18

9.20 Upgrade Wizard

Run the upgrade wizard on all 9.2x machines to transfer your data from the original 9.1x format to the 9.2 format.

The upgrade wizard can be found on all Gateway, Data Processing, and One-machine servers in the following locations:

- Windows:

<BSM Home Directory>\bin\upgrade_wizard_run_from91.bat

- Linux:

/opt/HP/BSM/bin/upgrade_wizard_run_from91.sh

For details about the upgrade wizard, see ["Upgrade Wizard" on page 105](#)

Chapter 19

Staging Mode

At the end of the upgrade wizard, the Staging Data Replicator (SDR) is run. This tool takes the data coming into your source environment and copies it to the staging environment. The SDR does not transfer event data.

To transfer event data to the staging servers:

1. In the staging environment, go to **Admin > Operations Management > Tune Operations Management**.
 - a. In **Time Based Event Automation**, select and disable each active TBEA rule
 - b. In **Automatic Runbook Rules**, select and disable each active OO rule
 - c. In **Notifications**, select and disable each active Notification Rule
 - d. In **Event Processing Customizations**, select and disable each active EPI step.
2. In the staging environment, go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
 - a. In the **applications** field, select **Operations Management** and locate the **Event Synchronization Settings** table.
 - b. In the **Forward Events** setting, set the value to **false**.
 - c. In the **Change State of Related Events Settings** table, set **Enable changing state of related events** to **false**.
 - d. In the **Duplicate Events Suppression Settings** table, in the **Enable duplicate events suppression** setting, set the value to **false**.
 - e. In the **Event Pipeline Receiver Settings** table, in the **Disable receiving of Events**, set the value to **false**.
3. Allow the events and changes to synchronize from the production server. This process is complete when the event sync buffer is empty. To check if the buffer is empty, run the following command on a Data Processing Server in the production environment:

Windows: %TOPAZ_HOME%\opr\support\opr-jmxClient.bat -system localhost:29622 -user admin -bean opr.backend:name=EventForwardingMBean -m showEventForwardStatistics

Linux: /opt/HP/BSM/opr/support/opr-jmxClient.sh -system localhost:29622 -user admin -bean opr.backend:name=EventForwardingMBean -m showEventForwardStatistics

If the command returns a list of buffers with values, it means those buffers have items in them. If the command returns nothing, it means the buffers are all empty and you can continue with the next step.

During this phase, you should verify and configure your staging environment. The following chapters describe a few steps which should be completed before ending staging mode and turning your staging environment into your production environment.

Chapter 20

Staging Data Replicator

- Staging Data Replicator - Overview58
- Running the Staging Data Replicator (Embedded)59
- Running the Staging Data Replicator (Standalone)60
- Verifying that the SDR Server Can Communicate with the Production Server62
- Unsubscribing the Staging Data Replicator from the Source Server63
- Running the SDR with Basic Authentication64
- SSL Configuration for the Staging Data Replicator65

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\sdreplicator\sdrIgnoredSamples.log** and the general SDR log at **log\sdreplicator\sdreplicator_all.log**.

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

1. Embedded SDR: **HPBSM\SDR\conf\core\Tools\log4j\sdreplicator\sdreplicator.properties**
2. 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 ["Staging vs. Direct Upgrade Overview" on page 9](#).

The SDR must be installed on a machine in the same network as the production environment, with the ability to access the staging environment. If the staging server cannot 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 next page](#)
- ["Running the Staging Data Replicator \(Standalone\)" on page 60](#)

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 next page](#).

Note: The SDR must be installed on a machine in the same network as the production environment, with the ability to access the staging environment. If the staging server cannot communicate with the production server, the SDR must be installed as a standalone utility on a different machine. For details, see ["Running the Staging Data Replicator \(Standalone\)" on next page](#).

To run the SDR (embedded)

1. If the staging server uses basic authentication, the SDR cannot communicate with the staging server unless you run the **basicauth** tool. For details, see ["Running the SDR with Basic Authentication" on page 64](#).
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 65](#).
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 62](#).
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 63](#).

Running the Staging Data Replicator (Standalone)

Typically, the SDR is run embedded in the staging server. It must be installed on a machine in the same network as the production environment, with the ability to access the staging environment. If the staging server cannot communicate with the production server, the SDR must be installed as a standalone utility on a different machine that does meet those requirements.

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 62](#).
2. Run the appropriate replicator file. The files are located on the SDR DVD:
 - **Windows_Setup\HPBsmSDR_9.20_setup.exe**
 - **Linux_Setup\HPBsmSDR_9.20_setup.bin**
 3. Follow the on-screen instructions to install the Staging Data Replicator. Select the type of deployment based on the version of your source environment.
 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) BSM 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/samples&request_timeout=30&force_keep_alive=true&send_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\dat\da_metadata
 - C:\HPBSM\SDR\dat\da_cache
6. If the web server on the staging server uses basic authentication, the SDR cannot communicate with the staging server unless you run the **basicauth** tool. For details, see ["Running the SDR with Basic Authentication" on page 64](#).
 7. If the web server on 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 65](#).
 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/scripts/run_hpbsmsdr.sh start
 9. After starting the SDR, copy the **<SDR installation directory>\dat\sdr\SDRBusConnectionStartTime.properties** file from the SDR server to the staging 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/scripts/run_hpbsmsdr.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 63](#).

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.

You do not have to perform this procedure if you are immediately uninstalling the previous version of BSM 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.
2. Open the **<Staging Data Replicator root directory>\conflb2G_translator.xml** file and locate the two **<Message Selector>** elements.
3. 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" />
4. 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.
5. 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 | -standalone] [enabled username password | disabled]
```

Where:

-embedded is for an SDR that is embedded in the destination environment.

-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 the BSM Hardening Guide.

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

At the end of this line, add the following:

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

Chapter 21

Post-Installation Procedures

Perform these tasks to complete the upgrade process.

- General Post-Installation Procedures67
- Starting and Stopping BSM 72
- Logging In and Out73
- Add Additional BSM Servers74
- Complete the Upgrade Process 75
- OMi Post-upgrade Procedure78

General Post-Installation Procedures

Perform these tasks to complete the upgrade process.

• Service Health and SLM repository 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 9.12, 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.

• Service Health Top View post-upgrade

In BSM 9.20, extensive improvements were made to the Top View component. For details, refer to the sections on Top View in the BSM User Guide and in the BSM Application Administration Guide.

As a result of the changes made to the underlying Top View infrastructure, the following infrastructure settings from earlier BSM versions are now deprecated in BSM 9.20:

- **Top View Data Refresh Rate - For Legacy MyBSM**
- **Top View Font Name**
- **Top View Green Color Property**

These infrastructure settings were located in the Service Health Application - Top View Properties section of the Service Health Application infrastructure settings. If you customized these settings prior to upgrade, your customizations are removed.

In addition, if you used a custom background image for Top View, after upgrade save the image in `<Gateway Server root directory>/AppServer/webapps/site.war/images/topview`, and enter the image file name in the **Custom Background Image Name** infrastructure setting.

• **SLM - Upgrading SLAs from BSM 9.x to 9.20 using Baselining**

The following section is only relevant for users who you have SLAs with BPM transaction CIs with the BPM Percentile Sample-Based rule defined on performance HIs, or Groovy rule (Rules API).

BSM 9.20 introduces the concept of baselining. In End User Management, Business Process Monitor performance metrics are analyzed over a period of time, and are used to provide a baseline comparison for establishing acceptable performance ranges.

Baselining influences the transaction thresholds, and will therefore have an impact on your SLA calculation. If you want to minimize this influence so that your SLA calculation results are similar to pre-baselining, perform the steps described in "[Upgrading SLAs from BSM 9.x to 9.20 to Work with Baselining](#)" on page 109 .

• **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 9.2x Data Processing Server:

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

• **Upgrade custom reports**

In some cases, custom reports are not migrated properly during the upgrade. If this is the case, execute the following command from the JMX console as follows:

- a. Open the JMX console from **`http://<DNS of BSM Gateway server>/jmx-console/`**
- b. In the Topaz section, select **EUM Custom report upgrader service**.
- c. Complete the fields and click Invoke.

• **Delete temporary internet files**

When logging into BSM for the first time after upgrading, delete the browser's temporary Internet files. This should be done on each browser that accesses BSM.

• **SHA baseline data**

The following note is relevant if you were using SHA with Performance or Operations Agents which include one of the following SPIs: WebLogic, WebSphere, Oracle, MSSQL.

The baseline may be inaccurate for at least one week after running the upgrade wizard. This is due to an improvement in the way instances in the SPIs are interpreted by SHA.

- **Disable firewall between BSM servers**

In general, placing firewalls between BSM servers is not supported. If an operating system firewall is active on any BSM server machine (GW or DPS), a channel must be left open to allow traffic between the BSM machines (GW and DPS).

- **Copy files from production server or restore them from backup**

Restore the following files from the production server or from backup to the new BSM servers:

- <Gateway Server installation directory>/AppServer/webapps/site.war/openapi/excels directory
- <Data Processing Server installation directory>/cmdb/general directory
- <Data Processing Server installation directory>/BLE/rules/<custom rules jar> file(s)
- <Gateway Server installation directory>/JRE/lib/security/cacerts
- <Gateway Server installation directory>/JRE64/lib/security/cacerts

- **Reconfigure Integration with HPOM**

This procedure is only required if you are performing a staging upgrade. If you had previously configured an integration with HPOM, repeat the following procedure that you performed when configuring this connection for the first time: "How to Set Up a Forwarding Target in the HPOM for UNIX Node Bank" in the BSM - Operations Manager Integration Guide.

- **Perform hardening procedures**

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 BSM Hardening Guide.

- **Ensure all processes started properly**

You can check to ensure that all processes started properly. For details, see "How to View the Status of Processes and Services" in the BSM Platform Administration Guide.

- **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`).

• Overwrite custom changes (optional)

BSM 9.20 comes with built in content packs. If any of the data in these content packs conflicts with a previously existing custom change, BSM keeps the custom change and does not overwrite it.

To overwrite your custom changes with the new 9.20 data:

- a. Open the Content Packs page from **Admin > Platform > Content Packs**.
- b. Select each content pack. In the content pack summary, there is a column indicating the origin of each artifact. For each item whose value is **predefined (customized)**, this indicates that the artifact was customized and is different from the one delivered with 9.20.
- c. To overwrite a change, locate the artifact in the corresponding admin user interface and select **restore to default**.

• 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 108](#).

• Install component setup files

The component setup files are used to install the components used by BSM. The component setup files are not installed as part of the basic BSM installation. They are located separately in

the Web delivery package download area and in the **Data Collectors and Components\components** directory of the BSM DVDs and must be installed separately to the BSM Downloads page. The component setup files can then be downloaded from BSM and used when required. For details on working with the BSM Downloads page, see "Downloads Overview" in the BSM Platform Administration Guide.

You must run all DVDs provided for installation to enable downloading all the BSM 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 BSM after the component's setup files are copied to the Downloads page.

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 BSM.

- **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 BSM 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 BSM 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 BSM Downloads page:

- i. Insert the BSM DVD into the drive of the BSM Gateway Server on which you want to copy the component setup files.
- ii. 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**.
- iii. Follow the on-screen instructions to complete the wizard.

Starting and Stopping BSM

After completing the BSM 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 before restarting the machine.

After installing the BSM 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 BSM on each server machine.

Note: You can check which BSM servers and features are installed on a BSM server machine by viewing the [INSTALLED_SERVERS] section of the **<BSM 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 BSM 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 BSM in Linux:

```
/opt/HP/BSM/scripts/run_hpbsm start | stop
```

To start, stop, or restart BSM using a daemon script:

```
/etc/init.d/hpbsmd {start| stop | restart}
```

Note: When you stop BSM, the BSM service is not removed from Microsoft's Services window. The service is removed only after you uninstall BSM.

Logging In and Out

You log in to BSM from a client machine's browser using the login page. LW-SSO is BSM's default authentication strategy. For details, see "Logging into BSM with LW-SSO" in the BSM Platform Administration Guide.

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 the BSM Platform Administration Guide.

Tip: For complete login help, click the **Help** button on the login page.

To access the BSM 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 BSM server. If there are multiple servers, or if BSM is deployed in a distributed architecture, specify the load balancer or Gateway Server URL, as required.

Note: Users running previous versions of BSM can still use bookmarks set to access the URL `http://<server_name>.<domain_name>/mercuriam` 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 BSM system, see "User Management" in the BSM Platform Administration Guide.

Note:

- For login troubleshooting information, see "Troubleshooting and Limitations" in the BSM Platform Administration Guide.
- For details on login authentication strategies that can be used in BSM, see "Authentication Strategies — Overview" in the BSM Platform Administration Guide.
- For details on accessing BSM securely, see the BSM Hardening Guide.

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.

Add Additional BSM Servers

Now that you have a complete, upgraded 9.20 environment, you can add new Gateway and Data Processing servers as desired.

To add new BSM servers to an existing BSM environment:

1. Run the installation and post-installation wizards.

- Windows:

DVD1 > windows_setup > HPBsm_9.20_setup.exe

For more details, see "[Installing BSM on a Windows Platform](#)" on page 89

- Linux:

DVD2 > linux_setup > HPBsm_9.20_setup.bin

For more details, see "[Installing BSM on a Linux Platform](#)" on page 84

2. Run the Setup and Database Configuration utility.

Select the option to run the configuration utility at the end of the post-installation utility to connect the servers to the staging database server. For more details about this utility, see the BSM 9.20 Installation Guide.

Complete the Upgrade Process

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

1. If you were using OMi, perform the following procedure to move the processing of events from the production server to the staging server:

- a. **On the production server** disable receiving of events and changes as follows:
 - i. Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**
 - ii. In the **applications** field, select **Operations Management** and locate the **Event Pipeline Receiver Settings** table.
 - iii. Set **Disable receiving of Events** to **true**.

- b. Now that new events will no longer be coming into the production server, enable the remaining events and changes to synchronize with the staging server. This process is complete when the event sync buffer is empty. To check if the buffer is empty, run the following command on a Data Processing Server in the production environment:

Windows: %TOPAZ_HOME%\opr\support\opr-jmxClient.bat -system localhost:29622 -user admin -bean opr.backend:name=EventForwardingMBean -m showEventForwardStatistics

Linux: /opt/HP/BSM/opr/support/opr-jmxClient.sh -system localhost:29622 -user admin -bean opr.backend:name=EventForwardingMBean -m showEventForwardStatistics

If the command returns a list of buffers with values, it means those buffers have items in them. If the command returns nothing, it means the buffers are all empty and you can continue with the next step.

- c. On the production server disable further processing of incoming events as follows:
 - i. Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
 - ii. In the **Applications** field, select **Operations Management** and locate the **Event Synchronization Settings** table. Set **Forward Events** to **true**.
 - iii. In the **Change State of Related Events Settings** table, set **Enable changing state of related events** to **false**.
 - iv. In the **Duplicate Events Suppression Settings** table, set **Enable duplicate events suppression** to **false**.
 - v. In the **Event Synchronization Settings** table, reset the value of **Event Forwarding Expiration** to the default or any desired value (the current value was temporarily set very high for the purposes of the upgrade).
 - vi. Go to **Admin > Operations Management > Tune Operations Management > Forwarding Rules**. Select and disable each active Forwarding Rule.
 - vii. Go to **Tune Operations Management > Time Based Event Automation**. Select and disable each active TBEA rule.
 - viii. Go to **Tune Operations Management > Automatic Runbook Rules**. Select and

- disable each active OO rule.
- ix. Go to **Tune Operations Management > Notifications**. Select and disable each active Notification Rule.
- x. Go to **Tune Operations Management > Event Processing Customizations**. Select and disable each active EPI step.
- d. On the staging server enable processing of incoming events as follows:
 - i. Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
 - ii. In the **applications** field, select **Operations Management** and locate the **Event Synchronization Settings** table. Set **Forward Events** to **true**.
 - iii. In the **Change State of Related Events Settings** table, set **Enable changing state of related events** to **true**.
 - iv. In the **Duplicate Events Suppression Settings** table, in the **Enable duplicate events suppression** setting, set the value to **true**.
 - v. In the **Event Synchronization Settings** table, reset the value of **Event Forwarding Expiration** to the default or any desired value (the current value was temporarily set very high for the purposes of the upgrade).
 - vi. Go to **Admin > Operations Management > Tune Operations Management > Forwarding Rules**. Select and disable each active Forwarding Rule.
 - vii. Go to **Tune Operations Management > Time Based Event Automation**. Select and disable each active TBEA rule.
 - viii. Go to **Tune Operations Management > Automatic Runbook Rules**. Select and disable each active OO rule.
 - ix. Go to **Tune Operations Management > Notifications**. Select and disable each active Notification Rule.
 - x. Go to **Tune Operations Management > Event Processing Customizations**. Select and disable each active EPI step.
- e. Restore the flow of events to the BSM servers to process the events in the data collector queues.
 - i. On the staging server enable event receiving as follows:

Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

In the **applications** field, select **Operations Management** and locate the **Event Pipeline Receiver Settings** table. Set **Disable receiving of Events** to **false**.
 - ii. On the production server enable event receiving as follows:

Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

In the **applications** field, select **Operations Management** and locate the **Event Pipeline Receiver Settings** table. Set **Disable receiving of Events** to **false**.
- 2. Update the data collectors to the communicate with the new servers.

- a. If you have a Load Balancer or Reverse Proxy, set it to communicate with the new servers.
- b. If you do not have a Load Balancer or Reverse Proxy, you must configure each data collector individually to communicate with the new BSM Gateway servers. For details, see the documentation of each data collector.

For the HPOM integration, see ["OMi Post-upgrade Procedure" on next page](#).

3. End the SDR and unsubscribe it from the source server. For details, see ["Staging Data Replicator" on page 57](#)
4. Keep production server alive.

Even though no new events are sent to the production server, there is still a need to keep this server online. Any active events that were forwarded from HPOM to the production server will continue to send updates this server. These updates will be forwarded to the staging server. If receiving these updates is not important to you, you can decommission the production server immediately. Otherwise, you should wait until all or most of the events previously sent to the production server are closed. HP estimates that most events are typically closed within 1-2 weeks.

The upgrade process is now complete. If you experience any problems during the upgrade process, see ["Troubleshooting" on page 115](#).

OMi Post-upgrade Procedure

If you were using OMi with BSM in your production environment, and have not configured event synchronization through a Load Balancer or Reverse Proxy, perform this procedure:

1. Configure HPOM to Forward Events to BSM 9.20

By default, when using a staging environment to upgrade BSM, only the original OMi 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 servers and the new BSM 9.20 environments receive events from HPOM. Until then only the original servers receive the events.

Perform the appropriate procedure below on each HPOM management server, depending on your operating system.

Configuring the HPOM Forwarding Policy - Windows

- a. Start the HPOM console as follows:

Start > Programs (or All Programs) > HP > HP Operations Manager.

- b. In the left pane of the HPOM console, select the following:

Policy management > Server policies grouped by type > Server-based Flexible Management.

- c. In the right pane of the HPOM console, double-click the existing policy that you want to edit. The Server-based Flexible Management Editor dialog opens.
- d. Replace the existing message target server to point to the new 9.20 BSM Gateway server (or Reverse Proxy or Load Balancer) as shown in the following example policy text:

CONTEMPLATES

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 "<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.

- e. Replace *<fully qualified host name>* in the text with the fully qualified hostname of the new Gateway Server 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 (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 *BSM Installation Guide*.

- f. Click **Check Syntax** to check for syntax errors in the new policy text.
- g. After correcting any syntax errors, click **Save and Close**.
- h. Redeploy the server-based flexible management policy on the HPOM management server.

Configuring the HPOM Forwarding Policy - Linux and UNIX

- a. Change to the work_respmgrs directory as follows:

```
cd /etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs/
```

- b. Policy template files can be found in:

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

- c. Edit the existing policy to which you want to add the OMi system as a target as follows:

```
vi <policy file name>
```

- d. Replace the existing message target server to point to the new 9.20 BSM Gateway server (or Reverse Proxy or Load Balancer) 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 "<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.

- e. Replace *<fully qualified host name>* in the text with the fully qualified hostname of the Gateway Server 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 (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 *BSM Installation Guide*.

- f. Enter the following command to check for syntax errors in the new policy text:

/opt/OV/bin/OpC/opcmomchk -msgforw <policy file name>

- g. 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/

- h. Restart the server processes as follows:

```
/opt/OV/bin/OpC/opcsv -stop  
  
/opt/OV/bin/OpC/opcsv -start
```

- i. Set Up a Forwarding Target in the HPOM for UNIX Node Bank

Note: Make sure that the SNMP agent is running before adding a managed node to the HPOM database.

The forwarding target (BSM Gateway Server, Reverse Proxy, or Load Balancer) must be set up in the node bank as a managed node. You must add the managed node by using the `opcnode` command line tool, for example:

```
/opt/OV/bin/OpC/utils/opcnode -add_node node_name=<node_name>  
net_type=NETWORK_IP mach_type=<machine_type> group_name=<group_  
name> node_label=<node_name>
```

<machine_type> relates to the operating system of the BSM host system:

- **Linux:** MACH_BBC_LX26RPM_X64
- **Windows:** MACH_BBC_WIN2K3_X64

<group_name> relates to the operating system of the HPOM management server host system and is one of the following:

- linux
- hp_ux
- solaris

2. Replace the 9.2x Servers as Target Servers for Topology Synchronization

If topology synchronization was configured between BSM 9.1x and HPOM, add the fully qualified domain name (FQDN) of the new BSM 9.2x staging servers to the list of target servers to forward discovery data. Follow the appropriate procedure below depending on your operating system.

Note: Make sure that certificates are exchanged between new BSM server system and the HPOM server system.

To add a server to the list of target servers in Windows:

- a. In the console tree, right-click **Operations Manager**, and then click **Configure_`Server...**. The Server Configuration dialog box opens.
- b. Click **Namespaces**, and then click **Discovery Server**. A list of values appears.
- c. Add the hostname of the BSM 9.2x staging servers to **List of target servers to forward discovery data**.

If there is more than one target server, separate the hostnames with semicolons, for example:

server1.example.com;server2.example.com

If the target server uses a port other than port 383, append the port number to the hostname, for example:

server1.example.com:65530;server2.example.com:65531

- d. Make sure that the value of **Enable discovery WMI listener** is **true**. This is the default value.
- e. Click **OK** to save your changes and close the Server Configuration dialog box.
- f. Restart the **OvAutoDiscovery Server** process for your changes to take effect.
- g. Start the initial synchronization of topology data:
 - i. In the console tree, select **Tools HP Operations Manager Tools**.
 - ii. Right-click **Synchronize Topology** and select **All Tasks Launch Tool....**

The tool **startInitialSync.bat** is started and begins to send all the topology data to the configured target management servers.

To add a server to the list of target servers in Linux:

- a. Type the following command to enable topology synchronization:

/opt/OV/contrib/OpC/enableToposync.sh -online -target <comma_separated_server_list>

Replace **<comma_separated_server_list>** with the fully qualified domain name of the target management server. If you have more than one target management server, separate each server name with a comma (,). Do not include spaces in the server list, for example:

server1.example.com;server2.example.com

If the target server uses a port other than port 383, append the port number to the hostname, for example:

server1.example.com:65530;server2.example.com:65531

This command restarts the service discovery server. The source management server begins to send any topology data changes immediately.

- b. Type the following command to start the initial synchronization of topology data:
/opt/OV/bin/OpC/startInitialSync.sh
- c. Make sure that the value of **Enable discovery WMI listener** is **true**. This is the default value.
- d. Restart the **OvAutoDiscovery Server** process for your changes to take effect.
- e. Start the initial synchronization of topology data:
- f. The tool **startInitialSync.xxx** is started and begins to send all the topology data to the configured target management servers.

Part 3

Appendix

Chapter 22

Installing BSM on a Linux Platform

This chapter contains the following topics:

Prepare Information Required for Installation	85
Working with the Web Server	86
Installing BSM Servers	87

Prepare Information Required for Installation

Have the following information ready before installation:

- **Maintenance number.** This is the number you received with your BSM 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 BSM.
- **Name of the Gateway Server machine.**
- **Name of the load balancer** (if any). This is the load balancer used to access the BSM site.
- **Port number used by the Web server.** The default port is 80.

Working with the Web Server

BSM installed on a Linux platform works with Apache HTTP Server.

Note: There must only be one running Web server on a BSM server machine.

Apache HTTP Server

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

BSM 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 BSM installation, reconfigure the service using that port to use a different port.
- During BSM 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 BSM, as configured in the Apache configuration file (**httpd.conf** and **httpd-ssl.conf**).

Installing BSM Servers

You install BSM servers—the Gateway Server and Data Processing Server—from the BSM DVD provided with the BSM 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 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 BSM. 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 BSM servers:

1. Log in to the server as user **root**.
2. Insert the BSM 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_9.20_setup.bin
```

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

Note: If BSM 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 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 30-60 minutes 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, BSM notifies you to resolve the conflict.
- **View the Web server type and enter the BSM administrator email address.** BSM 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 BSM sends.

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**.

Chapter 23

Installing BSM on a Windows Platform

This chapter contains the following topics:

Prepare Information Required for Installation	90
Working with the Web Server	92
Installing BSM Servers	93

Prepare Information Required for Installation

Have the following information ready before installation:

- **Target directory names.** During installation BSM 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 BSM components), you can do so within the BSM 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 the BSM Platform Administration Guide.

- **Maintenance number.** This is the maintenance number you received with your BSM package.
- **Administrator's e-mail address.**
- **Port number used by the Web server.** This is the port for access to BSM. 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 BSM site.
- **SMTP mail server name.**
- **SMTP sender name.** This name appears on notifications sent from BSM. This name cannot 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**.

Working with the Web Server

BSM 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 BSM uses. For example, if you select to use Apache HTTP Server during BSM 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

BSM uses an Apache HTTP Server version that has been adapted by HP for use with BSM. 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 BSM, 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:
 - a. **Common HTTP Features** section: **Static Content** (usually enabled by default)
 - b. **Application Development** section: **ISAPI Extensions** and **ISAPI Filters**.
 - c. **Management Tools** section: **IIS Management Scripts and Tools**
6. Click **Install**.

Installing BSM Servers

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

You need administrative privileges for the machines on which you are installing BSM 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 BSM servers:

1. Insert the BSM 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_9.20_setup.exe. The setup file for BSM servers is located in the **Windows_Setup** directory of the DVD. For example, enter d:\Windows_Setup\HPBsm_9.20_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 blank 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 30-60 minutes 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 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:**
 - i. **Apache HTTP Server.** If port 80, the default port, is already in use by the existing Web server, BSM notifies you to resolve the conflict. If you select Apache, you must also enter the email address of the BSM administrator.
 - ii. **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 BSM 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 BSM with Microsoft IIS, click **Cancel** to exit the wizard. Install IIS and rerun the BSM 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 BSM sends. If BSM 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 BSM servers using the above steps.

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**.

Chapter 24

Server Deployment and Setting Database Parameters

This chapter contains the following topics:

Setup and Database Configuration Utility Overview	97
Setting Database Parameters	98
Required Information for Setting Database Parameters	100
Running the Setup and Database Configuration Utility	102

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

Setup and Database Configuration Utility Overview

You configure your server deployment and create and connect to the databases/user schemas by using the Setup and Database Configuration utility.

You can run the Setup and Database Configuration utility as part of the BSM server installation 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.

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 (**Start > Programs > HP Business Service Management > Administration > Disable HP Business Service Management**).

After modifying database type or connection parameters, restart all BSM servers and data collectors.

Note: Modifying connection parameters for the management, RTSM, RTSM history, Business Process Insight, and Event databases after BSM 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 next page](#) and ["Required Information for Setting Database Parameters" on page 100](#).

For detailed information on preparing either MS SQL Server or Oracle Server in your system for use with BSM, see the BSM Database Guide.

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" below](#).
- Specify the connection parameters to the database or user schema. See ["Connecting to Existing Databases" below](#).

Note: If you need to change an active management database for BSM, 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 BSM Database Guide. For instructions on creating user schemas manually on Oracle Server, see "Manually Creating the Oracle Server Database Schemas" in the BSM Database Guide.

Note: Each database/user schema created in BSM(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 BSM 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 BSM, see "Deployment Configurations" in the BSM Planning Guide.

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. BSM 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 BSM Service Users" on page 108](#). For information on adding a Windows user to MS SQL Server, see ["Using Windows Authentication to Access Microsoft SQL Server Databases"](#) in the BSM Database Guide.

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 BSM Database Guide.

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 BSM user schemas, see "Oracle Server Configuration and Sizing Guidelines" in the BSM Database Guide.

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. BSM automatically displays the default port, **1521**.
- **SID.** The Oracle instance name that uniquely identifies the Oracle database instance being used by BSM.
- **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 BSM Installation process or separately. If you run the Setup and Database Configuration utility separately from BSM Installation process, note the following important points:

- If the command prompt window is open on the BSM 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 BSM 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:
 - At the end of the post-installation wizard, select the option to run the Setup and Database Configuration utility.
 - **Windows:** On the BSM server, select **Start > Programs > HP Business Service Management > Administration > Configure HP Business Service Management**. BSM launches the Setup and Database Configuration utility. Alternatively, you can run the file directly from `<BSM_Installation_Directory>\bin\config-server-wizard.bat`.
 - **Linux:** On the BSM 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 BSM is installed in the Licenses Management page of Platform Administration. For details, see "Licenses" in the BSM Platform Administration Guide.

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 the BSM Planning Guide.
- **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 RUM, BPI, and TransactionVision.

6. **IIS Configuration.** If you are using Microsoft Internet Information Server (IIS) version 7.X on Microsoft Windows Server 2008, BSM requires that the following IIS roles are enabled:

- ISAPI Extensions
- ISAPI Filters
- IIS Management Scripts and Tools
- Static Content

If they are already enabled, the IIS Configuration screen is not displayed.

If any of the roles are not enabled, you can request that they are automatically configured now by selecting **Automatically enable IIS roles** and clicking **Next**.

If you want to configure them manually, select **Manually enable IIS roles** and click **Next**.

7. **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.
 - If you choose to configure automatically, **only port 383** (the event system default port) is configured. When the user decides to configure the firewall automatically we check which port is configured for BBC in XPL config and open this port. 383 is the default BBC port but if the user changed this in XPL config we open that port in the firewall instead of port 383.

You must then 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 the BSM Platform Administration Guide.
 - If you choose to configure manually, no port configuration is executed and you must manually configure on both the Gateway Server and the Data Processing Server.
8. To enable the database connections, you must click **Finish** at the end of the utility.
9. If you ran the Setup and Database Configuration utility as part of the BSM server installation, you must start BSM on all servers only after successfully setting the parameters for all the databases. For details, see ["Starting and Stopping BSM " on page 72](#).

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>\conflumashup\import**. This contains two directories: **\loaded**, and **\tload**.
- Copy the contents of the **\loaded** directory into the **\tload** directory. Restart BSM.

Chapter 25

Upgrade Wizard

This chapter provides information about the BSM upgrade wizard.

Upgrade Wizard Overview106

Preparing Information for the Upgrade Wizard 107

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 BSM 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 BSM Database Guide.

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

- **Windows:** wizard_run_from91.bat
- **Linux:** wizard_run_from91.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 your original BAC or BSM architecture including data collectors / components / servers.
- **BAC/BSM Servers.** Location, credentials, and access to files for all original and new BAC or 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.

Chapter 26

Changing BSM Service Users

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.

Chapter 27

Upgrading SLAs from BSM 9.x to 9.20 to Work with Baselining

BSM 9.20 introduces the concept of **baselining**. In End User Management, Business Process Monitor performance metrics are analyzed over a period of time, and are used to provide a baseline comparison for establishing acceptable performance ranges. When a transaction's performance exceeds that range by some value, the transaction can signal a performance problem. The acceptable performance range of a transaction is determined by how far the current performance is from the baseline. For details, refer to the Baselines for BPM section in the BSM Application Administration Guide.

The following section is *only* relevant if you are upgrading from BSM 9.x to 9.20 and you want to add baselining to your existing SLAs, and your 9.x SLAs contain one of the following:

- BPM transaction CIs with the BPM Percentile Sample-Based rule defined on performance HIs.
- Groovy rule (Rules API) that use the tot_ok, tot_minor, or tot_critical fields from the trans_t sample in their rule calculation.

Baselining influences the transaction thresholds, and will therefore have an impact on your SLA calculation. If you want to minimize this influence so that your SLA calculation results are similar to pre-baselining, perform the steps described in the following section.

Note: If you have Groovy rules that use the above fields, you may prefer to change your rule script to use a different field from the sample, instead of performing the following procedure.

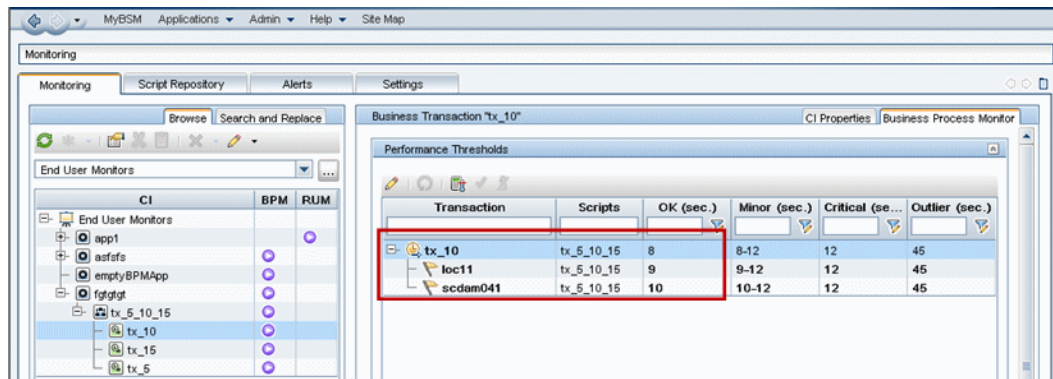
In this procedure you will clone your original SLA (before enabling baselining) to save calculation results; change rules on the cloned SLA to rules that are not influenced by baselining; stop the original SLA; and then configure baselining without it influencing SLA calculation.

Depending on your SLA, proceed with one of the following procedures:

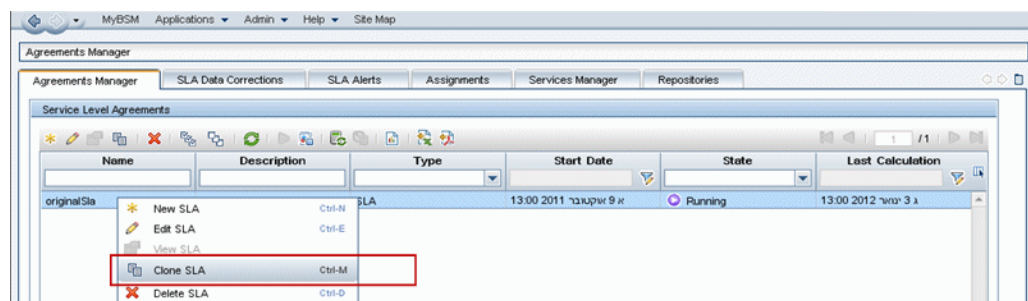
- ["To update SLAs with different thresholds in each location:" below.](#)
- ["To update SLAs with the same thresholds in each location:" on page 113.](#)

To update SLAs with different thresholds in each location:

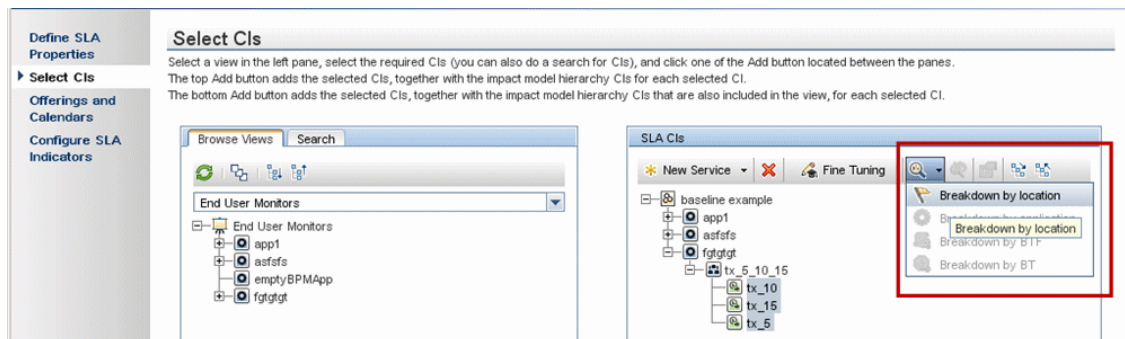
If you have different thresholds for a transaction in each BPM location perform the following procedure:



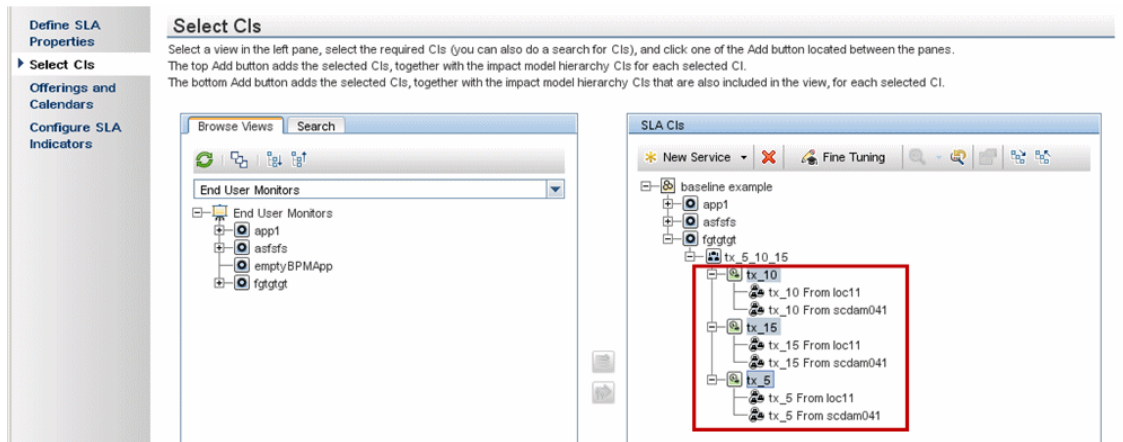
1. Within **Admin > Service Level Management**, clone your SLA; this saves your original SLA with its old calculation results.



2. Within **Admin > Service Level Management**, edit the duplicated SLA. In the SLA wizard, open the **Select CIs** page. Select all the BPM transaction CIs in the SLA, and perform a breakdown for all locations.



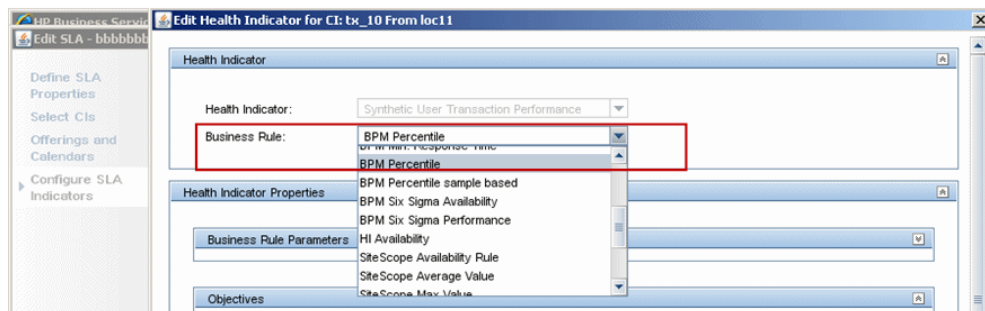
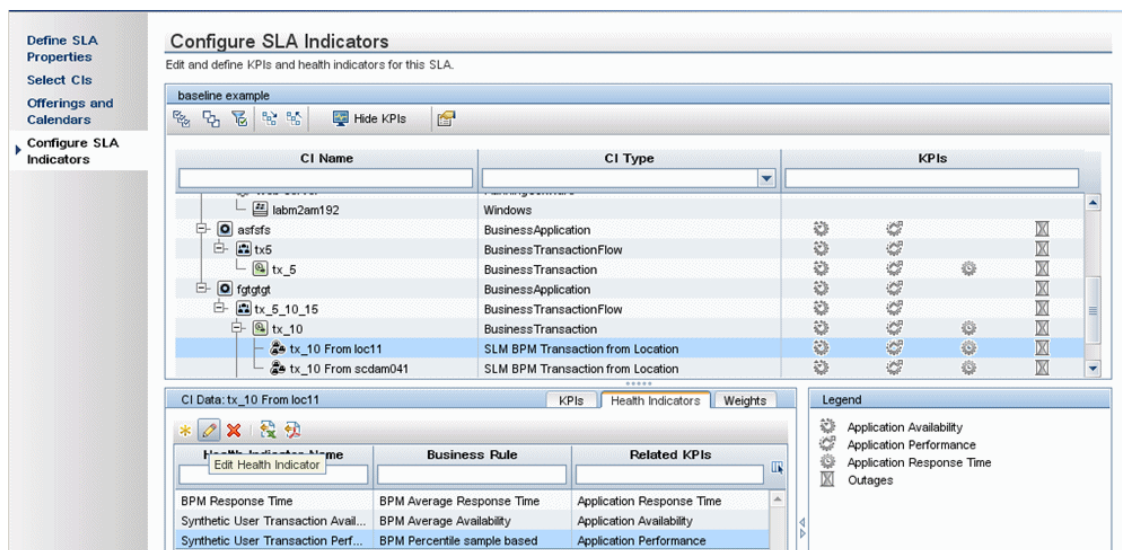
The result is as follows:



Note: If a new location was added to the application inside the SLA, to add the location to the breakdown you must disable the breakdown for the selected transaction using the **Undo Breakdown** button, and then enable it again.

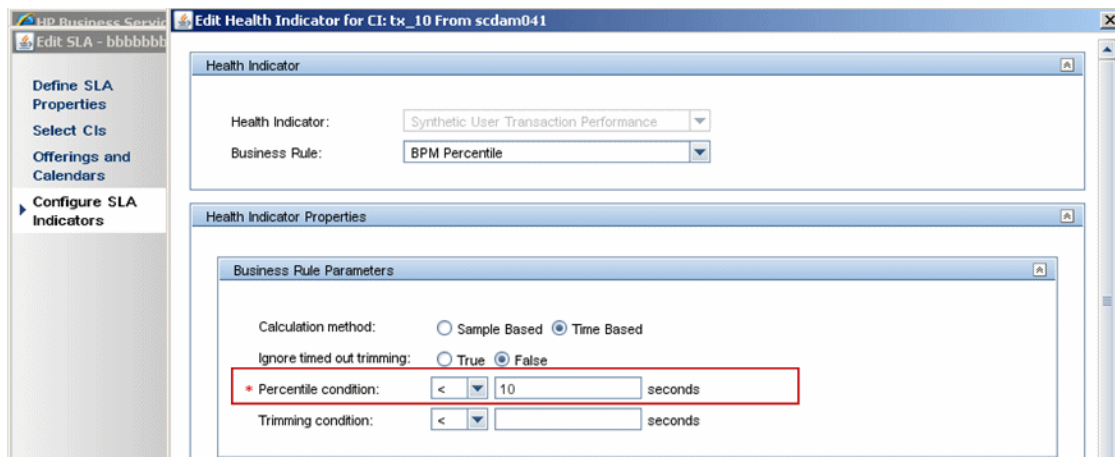
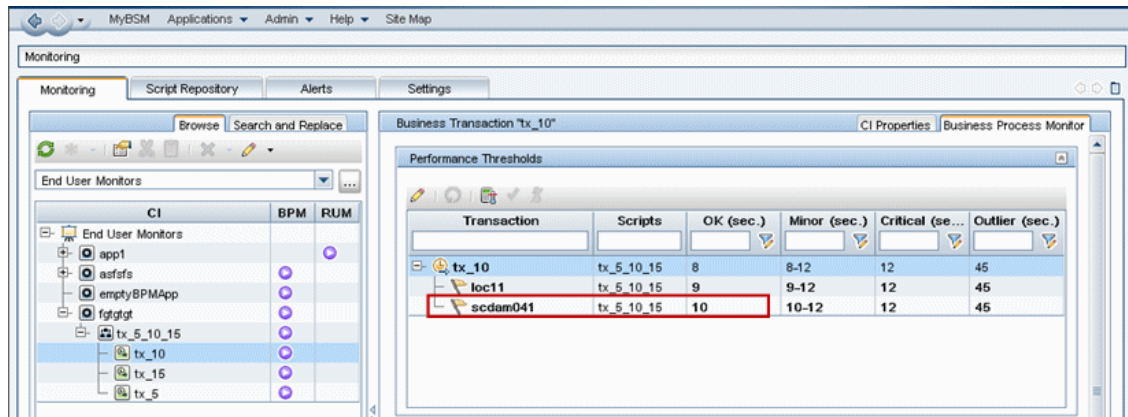
3. Within **Admin > Service Level Management**, edit the duplicated SLA. In the SLA wizard, open the **Configure SLA Indicators** page. On each of the performance HIs under the transaction from location CIs, change the percentile rule from BPM Percentile Sample-Based to BPM Percentile.

For details on these rules, refer to the list of SLM calculation rules in the the BSM Application Administration Guide.

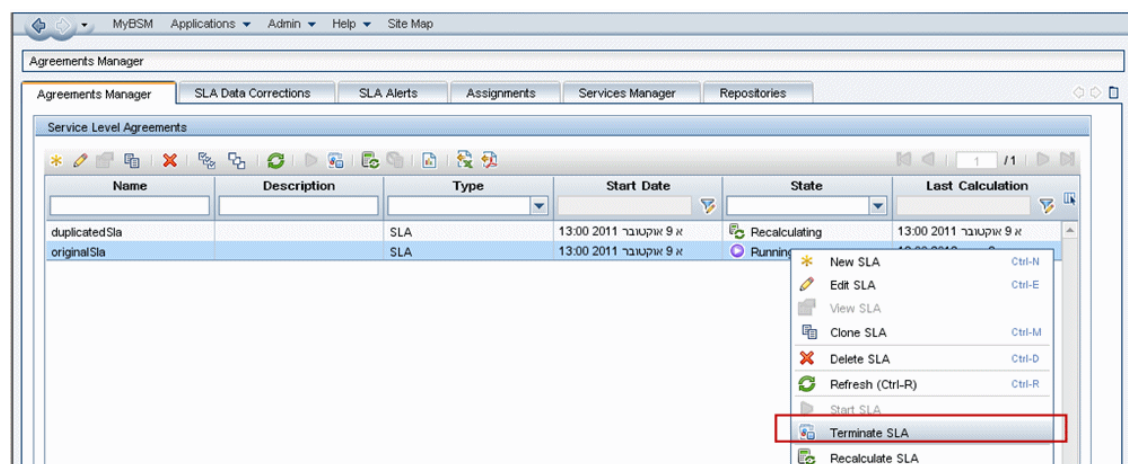


- For each of the transaction from location CIs whose rule you changed, copy the OK performance threshold defined for the CI in EUM Admin, and use it to define the Percentile Condition rule parameter.

For example, for transaction tx_10 and location scdam041 the threshold is 10:



- When you finish creating and editing the duplicated SLA, stop the original SLA.

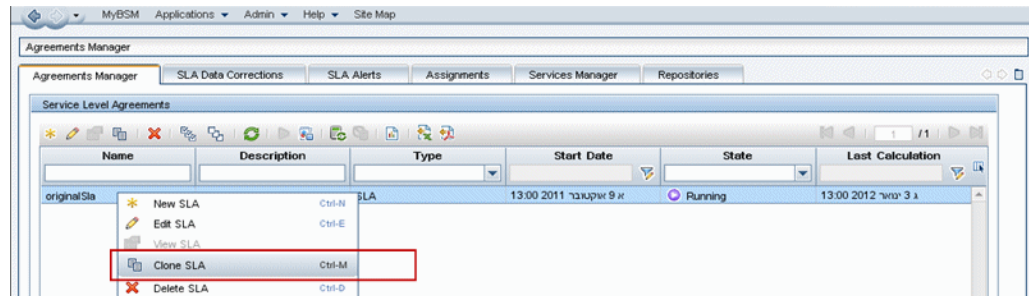


You can now configure baselining without influencing the SLA's calculation.

To update SLAs with the same thresholds in each location:

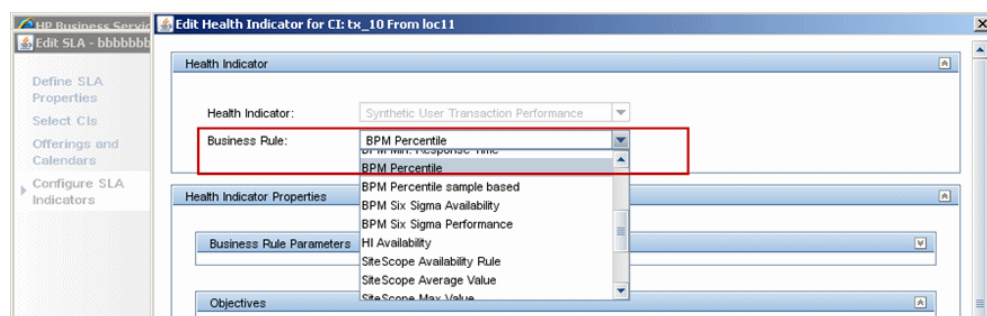
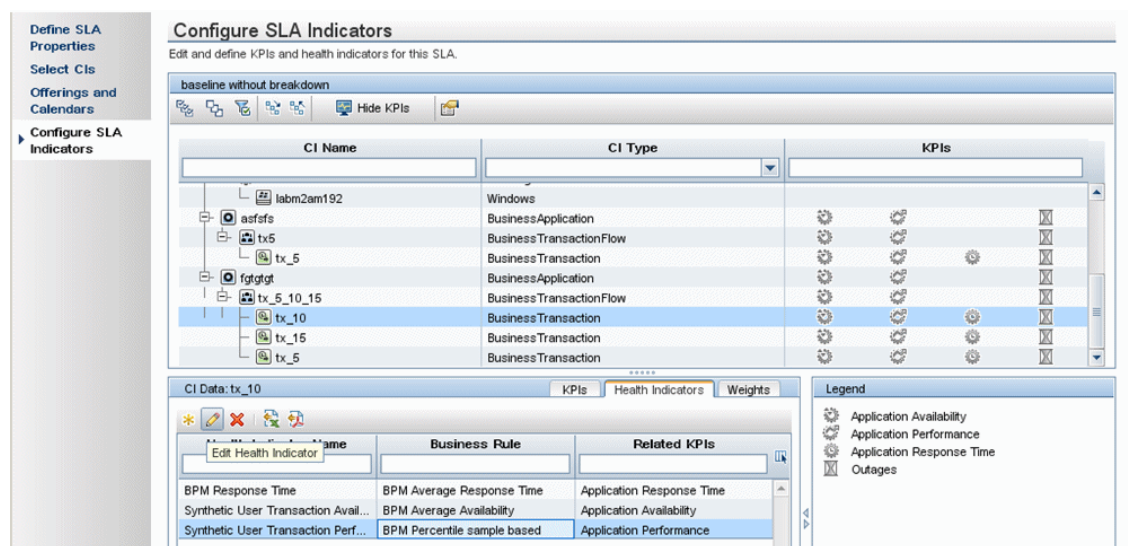
If you have the same threshold for all locations, perform the following procedure:

1. Within **Admin > Service Level Management**, clone your SLA; this saves your original SLA with its old calculation results.



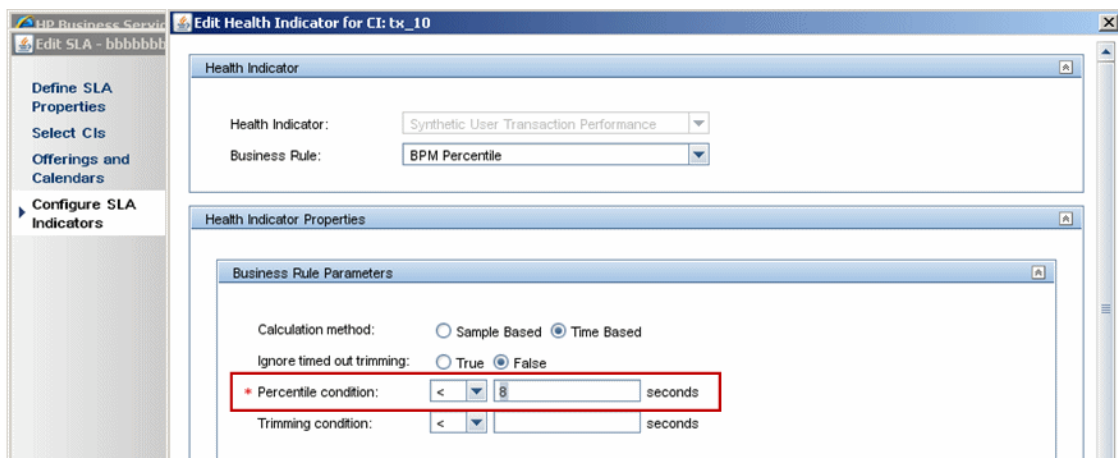
2. Within **Admin > Service Level Management**, edit the duplicated SLA. In the SLA wizard, open the **Configure SLA Indicators** page. On each of the performance HIs under the BPM transaction CIs, change the percentile rule from BPM Percentile Sample-Based to BPM Percentile.

For details on these rules, refer to the list of SLM calculation rules in the the BSM Application Administration Guide.

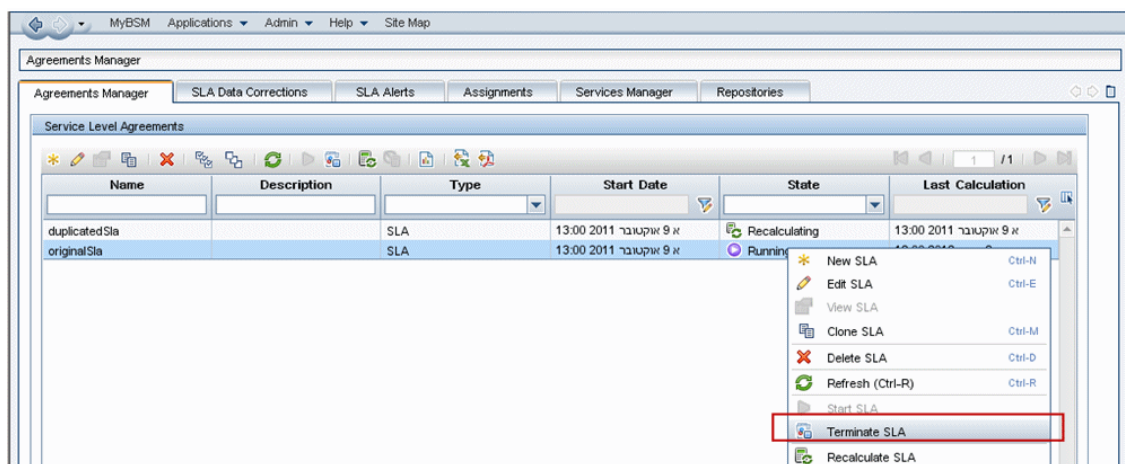


3. For each of the transaction CIs whose rule you changed, copy the OK performance threshold defined for the CI in EUM Admin, and use it to define the Percentile Condition rule parameter.

For example, for transaction tx_10 the threshold is 8:



4. When you finish creating and editing the duplicated SLA, stop the original SLA.



You can now configure baselining without influencing the SLA's calculation.

Chapter 28

Troubleshooting

This chapter contains the following topics:

Troubleshooting Resources	116
Installation and Connectivity Troubleshooting	117
Troubleshooting the Upgrade Process	123
Troubleshooting the 9.1x Upgrade Wizard	124

Troubleshooting Resources

- **Installation log files.** For details, see "Check installation log files" on page 70.
- **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/hpssoftwaresupport>).
- **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>

Installation and Connectivity Troubleshooting

This section describes common problems that you may encounter when installing BSM or connecting to BSM following installation, and the solutions to these problems.

The Setup and Database Configuration Utility does not allow you to enter a password

When running this utility on a Linux machine, in some cases the password field will not allow any entries. This was discovered on a Japanese RHEL5 64 machine.

Workaround:

Execute the wizard using a terminal emulator application such PuTTY or GNOME.

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 the BSM 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 BSM.

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 BSM servers causes a conflict with the Tomcat servlet engine.

Solution:

Stop the Oracle HTTP Server service, disable and then enable BSM.

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 BSM 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 tasks:

1. Verify that all BSM processes were started by accessing the status page. For details, see "How to View the Status of Processes and Services" in the BSM Platform Administration Guide.
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 92.
5. The Apache server may not be successfully starting because of a port collision.

After uninstalling BSM and reinstalling to a different directory, BSM 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 BSM 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 BSM

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:<br><b>api_reporttransactions_ex.asp</b><br> is <b>not</b>
mapped to an API Adapter.<br>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 BSM and may be left over from previous versions of BSM.

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 **<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.swapiness = 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.

Java applets not opening

- 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**).

Troubleshooting the Upgrade Process

This section describes problems that you may encounter when upgrading BSM, and the solutions to these problems.

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.

Sending Scheduled Reports

Scheduled reports are not sent from the staging servers while they are in staging mode. This prevents multiple reports from being sent. Non-scheduled reports can be sent by opening the **Report Manager**, selecting the report, and clicking the **Email This Report** button.

You can manually modify this setting so that BSM does send scheduled reports from the staging servers. To do so, enter an email address in the **Platform > Setup and Management > Infrastructure Settings > HP BSM Evaluation > Alerts mail address** setting.

SISConfigurationEnrichmentUpgrader failure

Description: During BSM upgrade, if the SISConfigurationEnrichmentUpgrader reports FAILED, PARTIALLY FAILED, or NOT REQUIRED status, the BSM content packs may not automatically upload upon restart.

Workaround: Delete the blockAutoUpload file located in the <HPBSM root directory>\conf\opr\content folder after SISConfigurationEnrichmentUpgrader finished and before BSM restart.

Troubleshooting the 9.1x Upgrade Wizard

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:

1. Open **<SDRroot directory>\conf\core\Tools\log4j\sdrreplicator\sdrreplicator.properties**. Modify the **loglevel** to **debug**.
2. Open **<BSM Directory>\>\conf\core\Tools\log4j\sdrreplicator\wde.properties**. Modify the **loglevel** to **debug**.
3. 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.
4. Modify the **loglevel** settings to **INFO** in the **sdrreplicator.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
```