HPE Business Service Management

Software Version: 9.26

BSM Upgrade Guide - 8.0x to 9.26

Document Release Date: January 2017
Software Release Date: September 2016

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

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 Server® and Windows Vista™ are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

UNIX® is a registered trademark of The Open Group.

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: https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HP Software Support web site at: **https://softwaresupport.hp.com**

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

HP Software 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 **https://softwaresupport.hp.com** and click **Register**.

To find more information about access levels, go to: **https://softwaresupport.hp.com/web/softwaresupport/access-levels**

HP Software Integrations, Solutions and Best Practices

Visit the Integrations and Solutions Catalog at https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710 to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at **https://hpln.hp.com/group/best-practices-hpsw** to access a wide variety of best practice documents and materials.

Contents

Introduction

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

How This Guide is Organized

This book is divided into three parts:

- Part I contains the workflow for upgrading using the direct method
- Part II contains the workflow for upgrading using the staging method
- Part III, 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.

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 not transferred during staging mode.

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

Note:

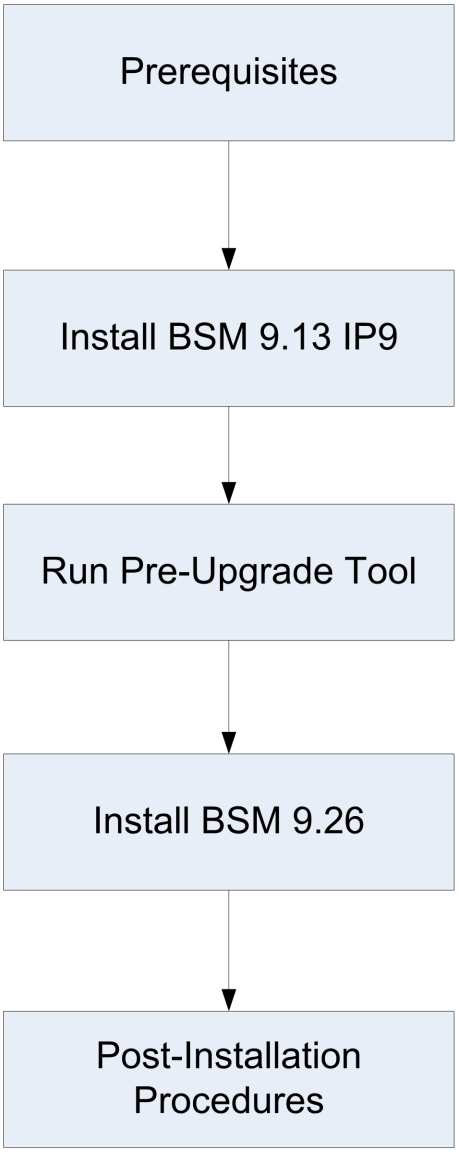
- If you are upgrading to BSM 9.26 and are running Red Hat Enterprise Linux 5.x, upgrade your operating system to Red Hat Enterprise Linux 6.x or 7.x and then perform the upgrade using Method I (Direct) or Method II (Indirect) in the BSM Upgrade Guide - 9.2x to 9.26.
- Scheduled reports are not sent from the staging servers while in staging mode. For more details, see "Troubleshooting the Upgrade Process" on page 230.
- 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.
- 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.

Part I: Direct Upgrade

Chapter 1: Overview of BSM 8.0x to 9.2x Direct Upgrade

The upgrade from BSM 8.0x to BSM 9.2x involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Prepare your source environment for the upgrade process by checking system requirements, planning your upgrade, backing up files, and so on.

This involves the following major steps:

-Uninstalling BSM 8.0x
-Installing BSM 9.10
-Performing intermediate procedures
-Running the BSM 9.13 IP9 upgrade wizard

The pre-upgrade tool migrates event-related configurations and certificates from BSM 9.13 IP9 to BSM 9.26.

This involves the following major steps:

-Uninstalling BSM 9.13 IP9
-Installing BSM 9.26

Perform various post-installation procedures, log in, and install additional BSM servers if desired.

Chapter 2: Prerequisites

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

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 Getting Started 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.

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

Product	Details
Operations Orchestration (OO)	If you were using OO with BSM 8.0x, you must upgrade to OO 7.51 or later. For more information, see the support matrix.
Service Manager (SM)	If you had integration between SM and BSM 8.0x via HP Universal CMDB, follow the instructions in the HP Universal CMDB upgrade procedures. For details, see "Upgrading HP Universal CMDB Integration - Splitting Procedure" on page 197.
CLIP	For information about upgrading an integration with HP CLIP 1.5, contact customer support.
HP Universal CMDB	For information about upgrading HP Universal CMDB and products that integrate with it, see "HP Universal CMDB (embedded/external) Upgrade Information" on page 195.

Product	Details
Network Node Manager i (NNMi)	You can continue to use BSM 9.1x without upgrading your integration with NNMi. If you choose to upgrade to NNMi 9.x, there are optional upgrades to this integration. For more information, see "NNMi Upgrade Information" on page 199

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 https://softwaresupport.hp.com.

4. Review relevant information

Review relevant information describing changes from BSM 8.0x to BSM 9.1x. Depending on your BSM configuration, review the relevant upgrade chapters in the BSM 9.1x Upgrade Guide.

5. 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. In BSM 9.23, support for SQL Server 2012 was added. Make sure 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.

6. Install the latest BSM 8.0x service pack

Install the latest service pack on the BSM 8.0x servers (8.07 at the time of the 9.23 release). If you are starting from BSM 8.0, this can be done by installing 8.01, then 8.07. For details, see the Service Pack release notes.

Note: If your version of BAC is older than 8.0x (such as 7.50), you need to perform an upgrade to BAC 8.0x before starting the processes described in this upgrade guide. For details about, see the Upgrade section of the BAC 8.0x Deployment Guide.

7. Run pre-upgrade tool

   Run the pre-upgrade tool to view a customized list of items that may need attention before starting the upgrade. For details, see the BSM 8.07 Pre-Upgrade Tool Guide.

8. Upgrade external HP Universal CMDB

   If you have an external HP Universal CMDB, upgrade it to a version compatible with your version of BSM.

9. Import DDM Content Pack 8

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

10. EUM Pre-Upgrade Procedures

    Ensure that all necessary Session Identification configurations do not have empty session ID values. Those with empty session ID values are not upgraded.

    Check-in all BPM scripts to the Script Repository. The upgrade process does not preserve the checked-out status of scripts.

11. Migrate custom integration adapters

    If you have custom integration adapters or if you modified out-of-the-box adapters, you will need to manually migrate these to BSM 9.1x. For details, see "Migrating Modified UCMDB Integration (Federation) Adapters" on page 200.

12. Migrate custom rules in Service Health and SLM

    If you created custom Java rules, custom rule .jar files, or custom Groovy rule files in pre-9.0 versions of BSM, contact HP Support for instructions on modifying and packaging them for BSM 9.x before upgrading. For details, see "Custom Rules" on page 213.

13. 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**).

14. Verify Content Pack compatibility

    Make sure your content packs are compatible with your version of HP Universal CMDB. Incompatibilities can cause problems during the upgrade. For example, installing Content Pack 9 with HP Universal CMDB 8.x could result in problems during the upgrade procedure.

15. Back up database schema (recommended)

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

16. 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

17. 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 40 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. Certain BSM components can coexist on BSM servers. For details on coexistence support, see the BSM System Requirements and Support Matrixes Guide.
- If you plan to use the IIS web server, install it prior to BSM installation and enable it after the installation is completed. For more information, see "Working with the Web Server" on page 158.
- 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**.
- The installation directory name should consist of only alphanumeric characters (a-z, A-Z, 0-9).
- User Access Control (UAC) must be disabled before installing BSM. UAC is enabled by default in some version of Windows Server (for example: 2008 SP2) and must be manually disabled.
- 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.
- If you do not have a profile database on your source environment, please add one before starting the upgrade. The database should be marked as the default profile database. Most users already have a profile database, but in some scenarios where BSM is being used exclusively for OMi, a profile database may not have been previously created.

- You must have administrator privileges to install BSM on the server machine.
- In the BSM cluster, open port 21212 on the Data Processing Server.

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, 29000-29000, 4444-4444, 8083-8083, 8093-8093.

These port 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 40 GB of free disk space. The /tmp directory should have at least 2.5 GB of free disk space. You can change the /tmp directory by running the following command:

  ```
  export IATEMPDIR=/new/tmp/dir
  ```

  ```
  export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/dir
  ```

  where `/new/tmp/dir` is the new /tmp directory

  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. Certain BSM components can coexist on BSM servers. For details on coexistence support, see the BSM System Requirements and Support Matrixes Guide.

- Before installing BSM on a Linux machine, make sure that SELinux does 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.

  On systems with SELinux disabled, the `SELINUX=disabled` option is configured in **/etc/selinux/config**:

  ```
  # This file controls the state of SELinux on the system.
  # SELINUX= can take one of these three values:
  #       enforcing - SELinux security policy is enforced.
  #       permissive - SELinux prints warnings instead of enforcing.
  #       disabled - No SELinux policy is loaded.
  SELINUX=disabled
  # SELINUXTYPE= can take one of these two values:
  #       targeted - Targeted processes are protected.
  #       mls - Multi Level Security protection.
  SELINUXTYPE=targeted
  ```

Also, the `getenforce` command returns **Disabled**:

```
~]$ getenforce
Disabled
```

To confirm that the aforementioned packages are installed, use the rpm utility:

```
~]$ rpm -qa | grep selinux
selinux-policy-3.12.1-136.el7.noarch
libselinux-2.2.2-4.el7.x86_64
selinux-policy-targeted-3.12.1-136.el7.noarch
libselinux-utils-2.2.2-4.el7.x86_64
libselinux-python-2.2.2-4.el7.x86_64
```

```
~]$ rpm -qa | grep policycoreutils
policycoreutils-2.2.5-6.el7.x86_64
policycoreutils-python-2.2.5-6.el7.x86_64
```

```
~]$ rpm -qa | grep setroubleshoot
setroubleshoot-server-3.2.17-2.el7.x86_64
setroubleshoot-3.2.17-2.el7.x86_64
setroubleshoot-plugins-3.0.58-2.el7.noarch
```

Before SELinux is enabled, each file on the file system must be labeled with an SELinux context. Before this happens, confined domains may be denied access, preventing your system from booting correctly.

To prevent this, configure `SELINUX=permissive` in the **/etc/selinux/config file**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

As a root user, restart the system. During the next boot, file systems are labeled. The label process labels all files with an SELinux context:

```
~]# reboot
```

In permissive mode, SELinux policy is not enforced, but denials are logged for actions that would have been denied if running in enforcing mode.

Before changing to enforcing mode, as a root user, run the following command to confirm that SELinux did not deny actions during the last boot. If SELinux did not deny actions during the last boot, this command does not return any output.

```
~]# grep "SELinux is preventing" /var/log/messages
```

If there were no denial messages in the **/var/log/messages** file, configure `SELINUX=enforcing` in **/etc/selinux/config**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Reboot your system. After reboot, confirm that `getenforce` returns **Enforcing**:

```
~]$ getenforce
Enforcing
```

```
~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
```

- 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 as the upgrade process cannot be performed silently.

- If you do not have a profile database on your source environment, please add one before starting the upgrade. The database should be marked as the default profile database. Most users already have a profile database, but in some scenarios where BSM is being used exclusively for OMi, a profile database may not have been previously created.
- In the BSM cluster, open port 21212 on the Data Processing Server.
- Before installing BSM 9.26 on Oracle Linux (OEL) or Red Hat Enterprise Linux operating systems for supported 6.x versions and 7.x versions, you must install the following RPM packages on all machines running BSM:

■ glibc	■ libXext
■ glibc-common	■ libXtst
■ nss-softokn-freebl	■ compat-libstdc++-33
■ libXau	■ libXrender
■ libxcb	■ libgcc
■ libX11	■ openssl098e
■ compat-expat1	■ rpm-devel

To install the RPM packages listed in the upper table, run the RPM installation tool on all machines running BSM:

<BSM_install_folder>/rhel_oel_installation_fix/rpm_installer.sh.

- If the script fails to install any of the RPM packages, the following message appears:

```
!!! ERROR: package <package name> has not been installed successfully

In this case, refer the problem to your system administrator.
```

- If the script detects that an RPM package is already installed, it skips that package and continues with the next package.

  However, you can force the tool to try to re-install any pre-installed packages by adding the **f** parameter to the command:

  <BSM_install_folder>/rhel_oel_installation_fix/rpm_installer.sh f

If the Yum Linux upgrade service is not functional on your machine, you will need to download and install the necessary RPM packages manually by running the following command:

yum install -y openssl098e glibc.i686 glibc-common.i686 nss-softokn-freebl.i686 libXau.i686 libxcb.i686 libX11.i686 libXext.i686 libXtst.i686 compat-libstdc++-33.i686 libXrender.i686 libgcc.i686 compat-expat1 rpm-devel

The version of these packages changes from system to system. You can download the packages from any RPM repository site that matches your system specifications. The following RPM search tool can assist you in this task (http://rpm.pbone.net/).

To determine the package version you need to download, execute the following command in a terminal window:

rpm –qa ${PACKAGE_NAME} (ex: rpm -qa glibc)

The command will return the following text:

```
# rpm -qa glibc

glibc-2.12-1.132.el6.x86_64
```

This text indicates the package version required for your machine.

In this case, you would need to download the i686 architecture package with the same version - glibc-2.12-1.132.el6.i686 – and install it manually.

OMi Pre-Upgrade Procedure

If you were using OMi with BSM 8.0x, perform the following steps before beginning the BAC 8.x to BSM 9.1x upgrade.

Note: The OMi database schema is not automatically upgraded by this process. A new OMi DB schema must be created during the upgrade from 8.x. Some of the following steps are required in order to insure OMi configuration can be restored at the completion of the upgrade.

1. ## Verify the Supported HPOM Versions

   Make sure that the version of HPOM that you plan to use with BSM 9.26 is supported. For more information about supported versions, see the BSM System Requirements and Support Matrixes.

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

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

   http://support.openview.hp.com/selfsolve/document/KM32348

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

   ### Limitations

   The following limitations may arise if you do not upgrade the SPIs

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

Indicator	9.1x Content Pack
Ping Availability	Infrastructure Content Pack and some dependent Content Packs
Server Load	Lync Server Content Pack
EJB Timeout Rate	JEE Application Server Content Pack

Indicator	9.1x Content Pack
JMS Server Utilization	JEE Application Server Content Pack
Transaction Timeout Errors	JEE Application Server Content Pack
Transaction Capacity Utilization	JEE Application Server Content Pack
Transaction System Errors	JEE Application Server Content Pack

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

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

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

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

4. Back Up the OMi Configuration Files - Recommended

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

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

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

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

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

%TOPAZ_HOME%\conf\opr

b. Save these files to a safe location, for example:

- Windows: **%TEMP%\migration**
- Linux: **/tmp/migration**

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

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

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

%TOPAZ_HOME%\opr\resources\images\hivalues

b. Save these files to a safe location, for example:

- Windows: **%TEMP%\migration**
- Linux: **/tmp/migration**

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

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

a. Make a note of each Event Assignment rule and each associated filter.

b. Recreate these filters and Event Assignment rules in the migrated installation.

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

a. Make a note of each user and the filter configurations associated with that user.

b. Recreate these filters in the migrated installation.

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

a. Make a note of each Graph Template and Graph Assignment that has been created. (After migrating from BAC 8.x to 9.1x, when you install content packs 9.1x on BSM 9.1x, new graph

templates for all content packs are available in the Content Manager.)

b. Recreate your Graph Templates and Graph Assignments in the migrated installation.

5. Delete CIs with Short Hostnames

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

To delete CIs with short hostnames:

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

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

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

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

c. Identify and delete all SQL Server CIs whose name field is not filled with the FQDN.

6. Update Empty Host Name Attributes of Host CIs

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

To update empty Host Name attributes, complete the following steps:

a. In the BAC 8.x Enrichment Manager, create a new, active enrichment rule based on a new TQL:

Select **Admin > Universal CMDB > Modeling > Enrichment Manager**.

To create a new enrichment rule, right-click anywhere in the Enrichment Rules pane and click **New**.

In the enrichment rule wizard, specify a name and description for the rule. Select **Rule is active**. As base TQL type, select **Base the Enrichment on a new TQL**. Close the wizard by clicking **Finish**.

b. Drag the CI type **Host** to the editing pane.

c. Right-click **Host** in the editing pane and select **Node Properties**.

d. Add a new attribute condition by clicking the button with the green plus sign. If necessary, select the new condition, then select Host Name - (string) from the **Attribute name:** drop-down list.

   Select Is null from the **Operator:** drop-down list. (The Value field remains empty.) Click **OK**.

e. *Optional:* Calculate the TQL query results.

f. In the upper-left corner of the editing pane, click **TQL Mode** and select **Enrichment Mode**.

g. Right-click **Host** in the editing pane and select **Update Node**.

h. In the **Node Definition** dialog, select the **Host Name** attribute in the **Name** column, then click the **By Attribute** button. The string **Host** appears in the drop-down list next to the **By Attribute** button.

   To specify the attribute to be taken, select the **Name** attribute in the drop-down list to the right of the Host attribute. Click **OK**.

i. Navigate to Scheduler, select:

   Admin > Universal CMDB > Settings > Scheduler

   Add a new job by clicking the button with the green plus sign. The **Job Definition** dialog opens where you specify a name and a definition.

   To add an action to the job, click the button with the green plus sign under **Actions**. The **Action Definition** dialog opens. Select **Run an Enrichment rule** and click **Next**. Select the enrichment rule that you created above and click **Finish**.

j. In the **Job Definition** dialog, under **Scheduler**, select **Once** and specify the current time. Click **OK** to save the job definition and close the dialog.

k. Wait for the enrichment to finish. Check that the enrichment query created above no longer matches any hosts.

   For more information about enrichment rules and scheduling, see the *Model Management* section in the HP UCMDB online help.

7. Export the OMi Configuration Data - Optional

This task describes how to export the OMi configuration data using the Content Manager command line interface.

Export the OMi 8.10 configuration data in the following situations:

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

To export the OMi configuration data, complete the following steps:

a. From a BAC 8.x Gateway Server, in a command prompt window, go to the following directory:

   %TOPAZ_HOME%\opr\bin

b. If you are retaining the HPOM Plug-ins (SPIs) that you have been using with your OMi 8.10 installation, export *all* 8.10 content packs. Enter the following command:

   ContentManager -snapshot -username <*administrator account*> -password <*administrator password*> -o <*snapshot file name*>.xml

   Where the administrator account must have read and write access to the Content Manager.

c. If you collected your modifications to OMi 8.10 content in a custom content pack, export that custom content pack. Enter the following command:

   ContentManager -username *administrator account*> -password <*administrator password*> -e <*custom content pack name*> -o <*custom file name*>.xml

   Where the administrator account must have read and write access to the Content Manager.

d. Save the exported data output file to a temporary location, for example:

   - Windows: **%TEMP%\migration**
   - Linux: **/tmp/migration**

   (Staging only) If you are upgrading in Staging Mode and the BSM 9.1x Gateway Server host system is already installed and available, copy the exported data output file to a temporary location on the BSM 9.1x Gateway Server host system.

   The exported data must be converted to the syntax and model required by the BSM 9.1x version. For details, see "Convert OMi 8.10 Content Packs to 9.1x Model and Syntax - Optional" on page 105.

8. Archive Events - Optional

This task closes and archives any outstanding events. Execute this task on any BSM server (GW or DPS). Execute the following command line tools to close and archive the events.

a. %TOPAZ_HOME%\bin\opr-close-events.bat -all

b. %TOPAZ_HOME%\bin\opr-archive-events.bat -o %TEMP%\opr-event-archive-8.0.xml -u 2099.01.01

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 2 GB, type 2000.
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 GB, type 2000.
7. Click **OK** to save the new values and close the dialog box.

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.

Chapter 3: Uninstall BSM 8.0x

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

Uninstall BSM 8.0x 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. Uninstall BSM via the Windows user interface or silently.
    a. Uninstall BSM Using the Windows user interface:
        i. On the machine from which you are uninstalling HP Business Service Management, select **Start > Control Panel > Programs and Features**. Select **HP Business Service Management**.
        ii. 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).

        iii. 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.
    b. Uninstall BSM silently:
        i. Stop all BSM servers.
        ii. Run the command **<HPBSM Installation Directory>\installation\bin\uninstall.bat -i silent**
2. 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. Stop all BSM servers.

4. Run the following script to uninstall in UI mode: **./uninstall.sh**. To peform this step in silent mode, use the command **./uninstall.sh -i silent**.

5. The BSM uninstall program begins. Follow the on-screen instructions. When the uninstall program is complete, a success message is displayed.

6. Click **Finish**.

7. 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 4: Install BSM 9.10

Install BSM 9.10 on a set of BSM 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_9.10_setup.exe

- For Linux:

  DVD2 > linux_setup > HPBsm_9.10_setup.bin

For more details, see the following sections:

"Installing BSM on a Windows Platform" on page 155

"Installing BSM on a Linux Platform" on page 163

Chapter 5: Install the Latest BSM 9.1x Minor-Minor Release and Patch

Install the latest minor minor version of BSM 9.1x and patch (if available).

1. **Prerequisites**

   - It is recommended that you back up all BSM databases and files you made custom changes to.
   - 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 HP Software Support site**

   a. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.

   b. Click **Search**.

   c. Select the relevant product, most recent 9.1x minor minor version, and operating system.

   d. Under Document Type, select **Patches**.

   e. Locate the installation files.

   f. Save the package locally and launch the relevant setup file to install the patch.

   g. Run the installation files on all BSM servers (Gateway and Data Processing).

   h. Run the post-installation wizard. This wizard follows the patch installation automatically.

   i. Repeat this procedure for the latest intermediate patch (if available).

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>

Chapter 6: OMi Mid-Upgrade Procedure

If you were using OMi with BSM 8.0x, perform this procedure between running the post-installation wizard and the upgrade wizard when upgrading BAC 8.x to BSM 9.1x.

1. Establish Trust Relationship

For connection and communication between the BSM and HPOM systems, you must establish a trust relationship between the systems.

> **Note:** The following steps use the ovcert, ovconfchg, and bbcutil command line tools. The tools are located in:
>
> Windows: **%OvInstallDir%\bin**
>
> Linux: **/opt/OV/bin**

To establish a trust relationship between BSM and HPOM systems:

a. Ensure that certificates have been set up on the Gateway and Processing Servers. For details, see "Post-Installation Tasks" in the BSM Installation Guide.

b. On all BSM Processing Servers, execute the following command:

ovcert -exporttrusted -file BSM_DPS<#>.cer

c. On the HPOM management server, execute the following command:

ovcert -exporttrusted -file other.cer

d. Copy other.cer from the HPOM management server to all BSM Processing Servers.

e. Copy BSM_DPS<#>.cer from the BSM Processing Server to the HPOM management server and all other BSM Processing Servers.

f. On all BSM Processing Servers, execute the following commands:

ovcert -importtrusted -file other.cer

ovcert -importtrusted -file other.cer -ovrg server

g. On the HPOM management server and on all BSM Processing Servers, execute the following commands:

ovcert -importtrusted -file BSM_DPS<#>.cer

ovcert -importtrusted -file BSM_DPS<#>.cer -ovrg server

h. If you have a multi-machine deployment, execute the following command on all Gateway Servers:

setup-secure-communication <BSM processing server>

If you are not sure if the certificate was already issued for the Gateway server, use the command **ovconfchg -edit** to check the **hp.XplConfig.ovconfchg** file. If **sec.cm.client.certificate_server** is set to the HPOM management server, then the certificate was already issued.

i. If the certificate was already installed on the system, execute the following command on all Gateway servers:

ovcert -updatetrusted

j. Configure the load balancers and reverse proxies according to the instructions in the BSM Installation Guide depending on your certificate authority and setup. Make sure that the new Data Processing Server certificates are trusted if no central certificate authority is used.

After establishing a trust relationship between the BSM and HPOM systems, check the connection between the two systems.

To check the connection between BSM and HPOM:

a. From the HPOM management server, verify that communication to the BSM installation is possible (the return value should be eServiceOk) by executing the following command on the HPOM server:

bbcutil -ping https://<BSM load_balancer, proxy server, or single_gateway_server>

Example of the command result:

https://<BSM servername>: status=eServiceOKcoreID=7c66bf42-d06b-752e-0e93-e82d1644cef8 bbcV=06.10.105appN=ovbbccb appV=06.10.105 conn=1 time=1094 ms

b. From all BSM Processing Server hosts, verify that communication with the HPOM management server host is possible (the return value should be eServiceOk) by executing the following command:

bbcutil -ping https://<HPOM_management_server_hostname>

Example of the command result:

https://<HPOM servername>: status=eServiceOK coreID=0c43c032-5c94-7535-064a-f7654a86f2d3 bbcV=06.10.070appN=ovbbccb appV=06.10.070 conn=7 time=140 ms

c. On the HPOM management server, add any new BSM Gateway Servers, load balancers, or reverse proxies to the list of target servers for discovery data.

Restart the discovery server processes on the HPOM management server:

HPOM for Windows:

- **net stop "OvAutoDiscovery Server"**
- **net start "OvAutoDiscovery Server"**

HPOM for UNIX or Linux:

- **ovc -stop opcsvcdisc**
- **ovc -start opcsvcdisc**

2. Convert OMi 8.10 Content Packs to 9.1x Model and Syntax - Optional

Convert the content packs that you exported from your OMi 8.10 installation to the syntax and model required by BSM 9.1x. You only need to complete this step if you exported content as described in "OMi Pre-Upgrade Procedure" on page 88.

The ContentMigration migration tool is located in:

- Windows: **%TOPAZ_HOME%\opr\bin\ContentMigration.bat**
- Linux: **/opt/HP/BSM/opr/bin/ContentMigration.sh**

The ContentMigration migration tool accepts the following options:

ContentMigration <inputFileName> <outputFileName> [-A Availability_KPI_UUID] [-P Performance_KPI_UUID]

For more information about the parameters that the ContentMigration command, see the following list:

<inputFileName>

Name of the input file. This must be an OMi Content Pack in XML file format from OMi 8.10.

<outputFileName>

Name of the output file, to which the BSM 9.1x formatted content pack XML file is written.

[-A <Availability_KPI_UUID>]

Optional: Specify an alternative availabilty KPI as the standard availability KPI assignment. For details, see "Alternative KPIs" on the next page.

[-P <Performance_KPI_UUID>]

Optional: Specify an alternative performance KPI as the standard availability KPI assignment. For details, see "Alternative KPIs" on the next page.

Note: By default the OMi 8.10 KPI assignments to Availability and Performance are replaced by assignments to System Availability and System Performance respectively. To assign alternative KPIs as the standard availability KPI assignment, see "Alternative KPIs" on the next page.

To convert an OMi 8.10 content pack to the model and syntax required by BSM 9.1x:

a. Copy the exported data output file of the content packs that you exported from your OMi 8.10 installation in the "OMi Pre-Upgrade Procedure" on page 88. Store the output file in a temporary location on the BSM 9.1x Gateway Server host system that is upgraded first, for example:

   - Windows: **%TEMP%\migration**
   - Linux: **\tmp\migration**

b. On the BSM 9.1x Gateway Server host system, convert the exported content packs:

   - To convert the exported snapshot of all OMi 8.10 content packs, enter the following command:
     - Windows: **%TOPAZ_HOME%\opr\bin\ContentMigration <**snapshot file name**> <**output file name**>**
     - Linux: **/opt/HP/BSM/opr/bin/ContentMigration <**snapshot file name**> <**output file name**>**
   - To convert the exported custom content pack that contains your OMi 8.10 modifications, enter the following command:
     - Windows: **%TOPAZ_HOME%\opr\bin\ContentMigration <**custom file name**> <**output file name**>**

- Linux: **/opt/HP/BSM/opr/bin/ContentMigration <**custom file name**> <**output file name**>**

Substitute the appropriate file names and specify alternative KPIs, if necessary. See also "Alternative KPIs" below.

c. Copy the converted OMi 8.10 content pack *snapshot* to the following location on the BSM 9.1x Gateway Server host system:

- Windows: **%TOPAZ_HOME%\conf\opr\content\migration**
- Linux: **/opt/HP/BSM/conf/opr/content/migration**

The upgrade wizard automatically uploads all converted content packs that reside in that location.

d. *Optional:* Delete the original, unconverted OMi 8.10 content packs from the following temporary directory on the BSM 9.1x Data Processing Server host system:

- Windows: **%TEMP%\migration**
- Linux: **/tmp/migration**

Alternative KPIs

You can assign alternative KPIs to the default ones. To do this you need to know what KPIs are available and what their stableId attributes are in the **SH-DefaultKPIs.xml** file.

To assign alternative KPIs, complete the following steps:

a. Open the following file:

- Windows: **%TOPAZ_HOME%\conf\opr\content\en_US\SH-DefaultKPIs.xml**
- Linux: **/opt/HP/BSM/conf/opr/content/en_US/SH-DefaultKPIs.xml**

b. Select an alternative KPI by its stabeId attribute.

KPIs are contained in XML elements named <Dimension>. Select a KPI where the application attribute is equal to dashboard (application="dashboard").

c. Run the ContentMigration migration tool and specify the stableId attribute of the selected KPI for the -A or -P parameters.

ContentMigration <exported_OMi_8.10_content_pack>.xml <converted_BSM_9.1x_content_pack>.xml -A <stableId_of_alternative_Availability_KPI> -P <stableId_of_alternative_Performance_KPI>

3. Restore Custom Icons from OMi 8.10 - Optional

If you have saved copies of OMi 8.10 icons for health indicators and want to continue to use them, copy the saved OMi 8.10 files to the BSM 9.1x installation.

a. Because some of the icons have changed in 9.1x, from a BSM 9.1x Gateway Server host system, make a backup copy of all the files in the following directory and subdirectories:

   - Windows: **%TOPAZ_HOME%\AppServer\webapps\site.war\images\gui\severities**
   - Linux: **/opt/HP/BSM/AppServer/webapps/site.war/images/gui/severities**

b. Copy the custom icon files that you saved from your OMi 8.10 installation in the step "OMi Pre-Upgrade Procedure" on page 88 to the following location on the BSM 9.1x Gateway Server host system:

   - Windows: **%TOPAZ_HOME%\AppServer\webapps\site.war\images\gui\severities**
   - Linux: **/opt/HP/BSM/AppServer/webapps/site.war/images/gui/severities**

4. Import Security Certificates to JRE Truststore

Secure environments only: To re-enable the trust relationship between the Java Runtime Environment (JRE) and the LDAP server, you must import the LDAP trusted certificate to the JRE truststore.

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

- **<Gateway Server installation directory>/JRE/lib/security/cacerts**
- **<Gateway Server installation directory>/JRE64/lib/security/cacerts**

5. Upgrade Wizard Notes

Migrated OMi 8.10 content and 9.1x content is uploaded using the create mode. The overwrite mode is not used and the OMi 8.10 content is retained to support the SPI DVD release 2008.1 SPIs.

The upgrade wizard first uploads the content packs for the locale set for the system, followed by English-language content packs that were not uploaded during the first upload phase. For example, if the locale is set to Japanese, Japanese-language content packs will be uploaded first, followed by English-language content packs. This can result in mixed-language content.

Note: If the OprUpgrader component partially fails during the configuration upgrade, check the opr-admin.log file to make sure that the HPOprInf, HPOprJEE, HPOprMss, and

HPOprOra content packs are loaded successfully:

- Windows: **%TOPAZ_HOME%\log\EJBContainer\opr-admin.log**
- Linux: **/opt/HP/BSM/log/EJBContainer/opr-admin.log**

If these content packs are loaded successfully, you can click Pass Upgrade and continue with the upgrade. If one of these content packs is not upgraded successfully, you must first correct the problem. Otherwise the subsequent SiSConfigurationEnrichment upgrade fails.

Chapter 7: 9.1x Upgrade Wizard

Run the BSM 9.1x upgrade wizard on all 9.1x machines to transfer your data from the original 8.0x format to the 9.1x format. The SDR and Data Transfer Tool must not be executed yet. When the upgrade wizard reaches the screen instructing you to run the SDR, select external SDR in order to continue with the wizard without running the SDR.

On the last screen of the wizard, select the option to **Perform cleanup now**. The upgrade wizard runs a second time in completion mode and finalizes the upgrade process.

Note: When running this wizard, you must create a new Event database schema. Do not use the pre-existing schema as this may cause the upgrade to fail.

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.bat

- Linux:

  /opt/HP/BSM/bin/upgrade_wizard_run.sh

When the wizard is finished, start all BSM servers. For details, see "Starting and Stopping BSM" on page 147.

For details about the upgrade wizard, see "Upgrade Wizard" on page 186.

Chapter 8: Configuration Procedures

Follow the procedures in this chapter. Note that some procedures depend on your specific BSM environment and are not required in all BSM upgrade scenarios.

OMi Post-Upgrade Procedure

If you were using OMi with BSM 8.0x, perform this procedure after running the upgrade wizard when upgrading from BAC 8.x to BSM 9.1x.

1. Update the Key Attribute of CI Collections Synchronized from HPOM

   With BSM 9.10 a new key attribute was introduced for the CI collection CI type.

   If you have previously synchronized HPOM node groups with BSM 8.x or BSM 9.0x, create an enrichment rule that copies the value of the Name attribute to the CI Collection ID attribute.

   To update the CI Collection ID attribute, complete the following steps:

   a. In the Enrichment manager, create a new active enrichment rule based on a new TQL as follows:

      i. Select **Admin -> RTSM Administration -> Enrichment manager**

      ii. Right-click in the **Enrichment Rules** pane and click **New**.

      iii. In the enrichment rule wizard, specify a name and description for the rule.

      iv. Select **Rule is active** and click **Next**.

      v. For the Base Query Type, select **Base the Enrichment on a new query**.

      vi. Click **Finish** to save the enrichment rule.

   b. Drag the CI type **Ci Collection** to the editing pane of the newly created enrichment rule.

   c. Right-click **Ci Collection** in the editing pane and select **Query Node Properties**.

   d. In the **Query Node Properties** window, clear **Include subtypes**.

   e. Add a new attribute condition ().

   f. Select the new condition, and from the **Attribute name:** drop-down list select **Ci Collection ID - (string)**.

   g. From the **Operator:** drop-down list, select **Is null**. (The **Value** field remains empty.)

   h. Add another new attribute condition (). Check that this condition is linked with **AND** to the previous condition.

   i. Select the new condition, and from the **Attribute name:** drop-down list select **Monitored By - (string_list)**.

j. From the **Operator:** drop-down list, select **Contains**.

k. In the Value field, enter OM.

l. Click **OK** to save the query node properties.

m. *Optional:* Calculate the query results.

n. Change **Query Mode** to **Enrichment Mode** (first field, top-left corner of the editing pane).

o. Right-click the **Ci Collection** icon in the editing pane and select **Update Query Node**.

p. In the Query Node Definition dialog, select the **CI Collection ID** attribute from the **Name** column.

q. Select the **By Attribute** radio button. The string name **CI Collection** appears in the first drop-down list next to the **By Attribute** button.

   To specify the attribute to be taken, select the **Name** attribute in the dropdown list to the right of the CI Collection attribute field.

   Click the **Save** icon.

r. Click **OK**.

s. Navigate to the Scheduler:

   Admin > RTSM Administration > Scheduler

t. Add a new job condition ( ).

   Specify a name and a definition in the Job Definition dialog box.

u. Add an action to the job (under Actions in the Job Definition dialog box).

v. In the Action Definition dialog box, select **Run an Enrichment rule** and click **Next**.

w. Select the enrichment rule that you created in Step 1 and click **Finish**.

x. In the Job Definition dialog box, under **Scheduler**, select **Once** and specify the current time.

y. Click **OK** to save the job definition and close the dialog box.

z. Wait for the enrichment to finish. Check that the enrichment query created in Step 1 no longer matches any hosts.

   For more information about enrichment rules and scheduling, see the Model Management section in the BSM online help.

2. Exchange Certificates Between HPOM and BSM

   Establish a trust relationship between the systems. For details, see "How to Establish a Trust Relationship for a Server Connection" on page 204

3. Manage BSM Nodes in HPOM

   In HPOM, update the nodes that represent the BSM systems.

   To enable communication between HPOM and OMi 8.10, the BAC 8.x servers were set up as managed nodes in HPOM (but no HP Operations Agent software installed). After the migration, the managed nodes that represent the BAC 8.x servers are no longer needed in HPOM and you can delete them. For details, see "Deleting BAC 8.x Managed Nodes in HPOM" below. (The BSM 9.1x servers do not need to be added to HPOM to enable communication.)

   Do not delete the BAC 8.x managed nodes if the HP Operations Agent software is installed and HPOM monitors the BAC 8.x servers for the purpose of system and performance management:

   - For direct upgrades, if this is the case, you must update the nodes' core IDs in HPOM because the systems have received new certificates. For details, see " Updating the Core IDs in HPOM for Windows" on the next page and " Updating the Core IDs in HPOM for UNIX and HPOM for Linux" on page 50.
   - If you are performing a staging upgrade and you want to monitor the new BSM 9.1x systems with HPOM, add the 9.1x systems as new managed nodes to HPOM and install the HP Operations Agent software to these nodes. For details, see the HPOM documentation.

Deleting BAC 8.x Managed Nodes in HPOM

To enable communication between HPOM and OMi 8.10, the BAC 8.x servers were set up as managed nodes in HPOM (but no agent software installed). After the migration, the managed nodes that represent the BAC 8.x servers are no longer needed in HPOM and you can delete them.

Note: Do not delete the BAC 8.x managed nodes if the HP Operations Agent software is installed and HPOM monitors the BAC 8.x servers for the purpose of system and performance management.

To delete the BAC 8.x managed nodes in HPOM for Windows, complete the following steps:

a. Open the Configure Nodes dialog, right-click the **Nodes** folder in the console tree and select **Configure > Nodes**.

b. Select the nodes that represent the BAC 8.x servers and press the **Delete** key.

c. Click **Yes** to confirm that you want to delete the nodes.

d. Close the Configure Nodes dialog.

To delete the BAC 8.x managed nodes in HPOM for UNIX or Linux, complete the following step:

On the HPOM for UNIX or Linux management server, use the opcnode command line tool to delete the nodes, type:

 # opcnode -del_node node_name=<node_name> \net_type=< network_type>

<node_name>: Name of the managed node that you want to remove from the HPOM database.

<network_type>: Type of managed node, for example: Non IP, IP (Network), or External (Node).

The opcnode command also ensures that the managed node's assignment to any node groups is removed. For more information about the opcnode command and its parameters and options, see the *opcnode(1m)* manual page.

Updating the Core IDs in HPOM for Windows

The BAC 8.x Data Processing Servers, Gateway Servers, and load balancers still exist as managed nodes in HPOM. However, because these systems may have received new certificates, you must update their core IDs in HPOM.

To update the core ID in HPOM complete the following steps:

a. On the BSM 9.1x Processing Servers, Gateway Servers, and load balancers identify the core ID, type:

   - Windows: ovcoreid
   - Linux: /opt/OV/bin/ovcoreid

b. On the HPOM system, start the HPOM console as follows:

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

c. Click **HP Operations Manager Console**.

d. Right-click **Nodes** and select **Configure > Nodes**.

The **Configure Managed Nodes** dialog box opens.

e. Right-click the managed node that you want to modify in the right pane and select **Properties**.

The **Node Properties** dialog box opens.

f. Click **General** to open the **General** tab.

g. Click **Advanced Configuration**.

The **Advanced Configuration** dialog box opens.

h. Select **Modify Agent ID/Core-ID** and paste the new core ID into the box.

i. Click **OK** to save your changes and close all dialog boxes.

Updating the Core IDs in HPOM for UNIX and HPOM for Linux

The BAC 8.x Data Processing Servers, Gateway Servers, and load balancers still exist as managed nodes in HPOM. However, because these systems may have received new certificates, you must update their core IDs in HPOM. Complete the following steps:

To update the core ID in HPOM complete the following steps:

a. On the BSM 9.1x Processing Servers, Gateway Servers, and load balancers identify the core ID, type:

- Windows: **ovcoreid**
- Linux: **/opt/OV/bin/ovcoreid**

b. On the HPOM for UNIX or HPOM for Linux system, type the following command:

/opt/OV/bin/OpC/utils/opcnode -chg_id node_name=<node_name> id=<new_id>

Replace <*node_name*> with the fully qualified domain name of the BSM Processing Server, Gateway Server, and or balancer. Replace <*new_id*> with the output of the ovcoreid command.

4. Configure Dynamic Topology Synchronization

Before configuring forwarding of topology (node and service) data to Operations Management from Operations Manager management servers, perform the procedure "How to Run Dynamic Topology Synchronization" on page 207.

5. Validate Topology Synchronization

If you have modified the out-of-the-box topology synchronization packages, you must manually recreate your changes in the 9.1x topology synchronization packages.

If you have created and saved your own custom topology synchronization packages in OMi 8.10, copy the saved custom packages to the BSM 9.1x installation. If these custom synchronization packages use out-of-the-box CI types, make sure that your synchronization packages still produce the desired results in BSM 9.1x, complete the following steps.

To validate topology synchronization, complete the following steps:

a. Copy the custom topology synchronization rules that you saved from your OMi 8.10 installation in the step "OMi Pre-Upgrade Procedure" on page 88 to the following location on the BSM 9.1x Data Processing Server host system:

   - Windows: **%TOPAZ_HOME%\conf\opr\topology-sync\sync-packages**
   - Linux: **/opt/HP/BSM/conf/opr/topology-sync/sync-packages**

b. On the BSM 9.1x Data Processing Server host system, run basic topology synchronization. Open a command prompt or shell and type:

   - Windows: **%TOPAZ_HOME%\bin\opr-startTopologySync.bat**
   - Linux: **/opt/HP/BSM/bin/opr-startTopologySync.sh**

c. If out-of-the-box CI types have changed in BSM 9.1x, the synchronization process ends with errors. Check the synchronization log file:

   - Windows: **%TOPAZ_HOME%\log\opr-topologysync**
   - Linux: **/opt/HP/BSM/log/opr-topologysync**

d. Enable the data dump option and verify the CI attributes:

   i. Navigate to the HPOM Topology Synchronization settings in the Infrastructure Settings Manager:

      Infrastructure Settings > Applications > Operations Management > Operations Management - HPOM Topology Synchronization Settings > Dump data

   ii. Change the value of **Dump data** to **true**.

   iii. Run the Topology Sync tool with the following command:

- Windows: **<HPBSM root directory>\bin\opr-startTopologySync.bat**
- Linux: **<HPBSM root directory>/bin/opr-startTopologySync.sh**

iv. Check if the file in the following directory contains all expected attributes for the CIs of your synchronization package:

- Windows: **%TOPAZ_HOME%\opr\tmp\datadump\postenrichment**
- Linux: **/opt/HP/BSM/opr/tmp/datadump/postenrichment**

e. Use the BSM 9.1x CI Type Manager to find changed CI types, adapt your mapping rules, and run topology synchronization again.

Repeat this process until all mapping errors have been resolved.

For more information about topology synchronization, see the HP Operations Manager i *Extensibility Guide*.

6. Recreate Your OMi 8.10 Modifications in 9.1x - Optional

If you upgraded the SPIs to SPI DVD release 2010 before the migration, you must manually recreate the modifications that you applied to the OMi 8.10 content in your 9.1x installation. Refer to your notes taken in "Make a Note of Each Modification to the OMi 8.10 Content Packs" on page 89.

Alternatively, if you exported and converted a custom content pack, upload the custom content pack in create mode after the migration.

To recreate upload the custom content pack in create mode, complete the following steps:

a. Change to the temporary location on the BSM 9.1x Gateway Server host system, where the converted custom content pack resides, for example:

- Windows: **%TEMP%\migration**
- Linux: **/tmp/migration**

b. Upload the custom content pack in create mode, enter the following command:

<HPBSM Install Directory>/opr/bin/ContentManager -username admin -password admin -i <converted custom content pack>

Where the administrator account must have read and write access to the Content Manager.

c. Verify the uploaded content pack in the Content Packs Manager.

7. Re-import the 9.1x Content - Optional

If you did *not* upgrade the SPIs to the SPI DVD 2010 release before the migration, but rather decide to switch to the new SPIs after the migration, you must reimport the 9.1x content with overwrite mode. However, the overwrite mode will overwrite *all* of your modifications. You must then manually recreate your OMi 8.10 modifications in the 9.1x content.

To reimport 9.1x content, complete the following steps:

a. Upgrade the HP Operations SPIs to SPI DVD release 2010 as described in the documentation provided with the SPIs.

b. Reimport the 9.1x content in overwrite mode, enter the following command:

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

c. Manually recreate your OMi 8.10 modifications in the 9.1x content. Refer to the notes taken in "Make a Note of Each Modification to the OMi 8.10 Content Packs" on page 89.

General Configuration Procedures

Perform the following procedures:

- Upgrading Customized Service Health KPIs

  In BSM 9.2x, the internal format of the KPI parameter “KPI is critical if” was changed. As a result, this value may be incorrect following upgrade, if you have created or customized KPIs.

  To fix this, perform the following:

  a. Access the JMX console on the Gateway Server via http://<Gateway Server name>:29000/jmx-console, and enter your user name and password.

  b. Click **service=repositories-manager** in the Topaz section.

  c. Locate the **upgradeCriticalIf()** operation.

  d. Click **Invoke**.

- Service Health and SLM repository post-upgrade procedure

  When you installed BSM 9.1x, content that was imported using out-of-the-box content packs was categorized in the Service Health and SLM repositories as **Custom** or **Predefined (Customized)**, rather than as **Predefined**.

  After you install BSM 9.2x, 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>:29000/jmx-console**, and enter your 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 9.2x, 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 9.2x:

  - **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 9.2x using Baselining

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

  BSM 9.2x 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 9.2x to Work with Baselining" on page 214.

- 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 Etl 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://<FQDN of BSM Gateway server>:29000/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.

- Back up files

  Back up the following files from the BSM 9.1x 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)

- 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.

Pre-Upgrade Tool

The pre-upgrade tool temporarily stores some configuration and certificates in the BSM database to help migrate them to 9.2x. It should be run on all BSM Gateway and the active DPS servers.

1. **Run the Pre-Upgrade Tool on all BSM Gateway servers**

   On all BSM Gateway servers, 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 9.2x 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 9.2x installation.
- Events from your BSM 9.1x environment may be lost.

In this case, you should execute the following steps manually on your BSM 9.2x 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 9: 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. Uninstall BSM via the Windows user interface or silently.
    a. Uninstall BSM Using the Windows user interface:
        i. On the machine from which you are uninstalling HP Business Service Management, select **Start > Control Panel > Programs and Features**. Select **HP Business Service Management**.
        ii. 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).

        iii. 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.
    b. Uninstall BSM silently:
        i. Stop all BSM servers.
        ii. Run the command **<HPBSM Installation Directory>\installation\bin\uninstall.bat -i silent**
2. 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. Stop all BSM servers.

4. Run the following script to uninstall in UI mode: **./uninstall.sh**. To peform this step in silent mode, use the command **./uninstall.sh -i silent**.

5. The BSM uninstall program begins. Follow the on-screen instructions. When the uninstall program is complete, a success message is displayed.

6. Click **Finish**.

7. 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 10: Migrate Database to MS SQL 2012 (optional)

If you would like to use MS SQL 2012, migrate your staging database to a new MS SQL 2012 database. For details, refer to MS SQL documentation.

Chapter 11: Install BSM 9.26

Install BSM 9.26 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.

Do not install additional servers at this time, you can install them towards the end of the workflow.

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.

Go to My software updates (use your HP Passport credentials) and click the BSM 9.26 installation package.

Or

1. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.
2. Click **Search**.
3. For Windows, select **Application Performance Management (BAC) > 9.26> Windows**).

   For Linux, select **Application Performance Management (BAC) > 9.26> Linux**).
4. Under Document Type, select **Patches**.
5. Locate the BSM 9.26 package and save it locally.
6. Launch the relevant setup file to install BSM 9.26.

Alternatively, you can run these wizards in silent mode. For details, see "Installing BSM Silently" on page 180.

For more details, see the following sections:

- "Installing BSM on a Linux Platform" on page 163
- "Installing BSM on a Windows Platform" on page 155

Chapter 12: 9.26 Upgrade Wizard

Run the BSM 9.26 upgrade wizard on the 9.26 BSM servers to transfer your data from the original 8.0x format to the 9.26 format. When this is complete, run the upgrade wizard a second time. The upgrade wizard runs in completion mode and finalizes the upgrade process.

You should only have one set of 9.26 servers installed at this time. Do not run the upgrade wizard on more than one set of 9.26 servers.

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_from80.bat

- Linux:

  /opt/HP/BSM/bin/upgrade_wizard_run_from80.sh

For details about the upgrade wizard, see "Upgrade Wizard" on page 186.

Chapter 13: Post-Installation Procedures

Perform these tasks to complete the upgrade process:

General Post-Installation Procedures

Perform these tasks to complete the upgrade process:

Note: If you use the IIS web server, stop the **IIS Web Server** service before running the post installation procedure. Do not change the **Startup Type** setting of this service. Do not remove **IIS Web Server** as role.

- Disable firewall between BSM Gateway and Data Processing 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 all traffic between all BSM Gateway and DPS servers.

  Additionally, to enable BSM users and data collectors to communicate with the BSM Gateway servers, you must leave open the relevant ports depending on your BSM configuration. The required ports are typically 443 or 80, and 383. For details, see "Port Usage" in the BSM Platform Administration Guide.

- Update Data Collectors

  See the System Requirements and Support Matrixes, available from **Help > Planning and Deployment** and the Updated Components section in the HP Business Service Management Release Notes to determine if you must upgrade your data collector to the latest supported version.

- Copy files from production server or restore them from backup

  Restore the following files to the BSM:

  - <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 and you are upgrading using a staging environment, you need to repeat the hardening procedures described in the BSM Hardening Guide.

  If your original environment was secured with SSL and you are upgrading directly, you need to repeat the following hardening procedures:

  a. If you had previously made changes to **<HP BSM root directory>\EJBContainer\server\mercury\deploy\jboss-web.deployer\server.xml** while performing hardening procedures on your system, repeat the “Securing JBOSS” procedure in the Hardening Guide after the patch installation on all relevant BSM machines.

  b. If you had previously configured SSL on an IIS web server used by BSM, you need to verify HTTPS port binding in IIS is set to the correct port (443).

  c. If you had previously configured SSL on the Apache web server used by BSM, you may need to reapply the changes to httpd.conf and httpd-ssl.conf files as follows:

     - In **<HP BSM root directory>\WebServer\conf\httpd.conf**, uncomment the following two lines:

       LoadModule ssl_module modules/mod_ssl.so

       Include conf/extra/httpd-ssl.conf

     - In **<HP BSM root directory>\WebServer\conf\extra\httpd-ssl.conf**, specify paths to **SSLCertificateFile** and **SSLCertificateKeyFile**

     - Restart the HP BSM Apache web service

- 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.

- 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\<BSM version>** directory.

  In a Linux environment, the logs files are located in the **/tmp/HPOvInstaller/<BSM version>** 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_9.26_2015.10.21_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_BPMPkg_install.log).

- Overwrite custom changes (optional)

  BSM 9.26 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 9.26 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 who value is **predefined (customized)**, this indicates that the artifact was customized and is different from the one delivered with 9.26.

  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 192.

- 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. You can upload them 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" in the BSM Platform Administration Guide.

  Note:

  - The components on the Downloads page are updated for each major and minor release (for example, 9.00 and 9.20). To download updated components for minor minor releases and patches (for example, 9.26), go to the HP Software Support site (https://softwaresupport.hp.com).
  - You can install a component by using the component's setup file directly from the network. 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.

  To install component setup files, 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.

- Enable IPv6 Support (optional)

  BSM by default communicates using IPv4. If your environment uses IPv4 and IPv6, you can choose to use either IPv4 or IPv6, but not both.To enable IPv6, run the following commands on all BSM servers (GW and DPS):

  ovconfchg -ns sec.cm.server -set IsIPV6Enabled TRUE

  ovc -kill

  ovc -start

- **Update the LW-SSO Configuration.**

  You must update the LW-SSO configuration even if you are not using LW-SSO authorization. Be sure to install all patches before performing this step. For instructions, see the BSM 9.26 Build Patch Installation Guide (https://softwaresupport.hpe.com/km/KM02140729).

a. Go to the JMX console – LW-SSO Configuration :

http://<Gateway or Data Processing Server >:29000/mbean?objectname= Topaz%3Aservice%3DLW-SSO+Configuration

where

<Gateway or Data Processing Server name> is the name of the machine on which BSM is running.

b. Search for InitString and copy the value.

c. Access the flat xml file located at:

\HPBSM\conf\settings\SingleSignOn\lwssofmconf.xml.

d. Search for InitString and paste the value you just copied.

e. Go to the JMX console – Infrastructure Settings Manager:

http://<Gateway or Data Processing Server name>:29000/mbean?objectname= Foundations%3Aservice%3DInfrastructure+Settings+Manager

where

<Gateway or Data Processing Server name> is the name of the machine on which BSM is running.

Note: This step must be performed in either Firefox or Chrome.

f. Search for the **setGlobalSettingValue()** method.

g. Enter the following values and invoke the method:

- **contextName:** SingleSignOn
- **settingName:** lw.sso.configuration.xml
- **newValue:** paste the content of the lwssofmconf.xml file

Note: Format the content of the lwssofmconf.xml file on one line.

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 | restart}

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>/mercuryam and http://<server_name>.<domain_name>/topaz

2. Enter the default administrator user ("admin"), and the password specified in the Setup and Database Configuration utility, and click **Log In**. After logging in, the user name appears at the top right.

3. (Recommended) Create additional administrative users to enable BSM administrators to access the system. For details on creating users in the 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.

Adding Additional BSM Servers

After you have a working BSM 9.26 environment, you can add new Gateway and Data Processing servers as desired.

To add new BSM servers to an existing BSM environment:

1. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.
2. Click **Search**.
3. For Windows, select **Application Performance Management (BAC) > 9.26 > Windows**).

   For Linux, select **Application Performance Management (BAC) > 9.26 > Linux**).
4. Under Document Type, select **Patches**.
5. Locate the 9.26 patch and save the package locally.
6. Launch the relevant setup file to install the patch.
7. Run the installation files on all BSM servers (Gateway and Data Processing).
8. 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**. 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**.

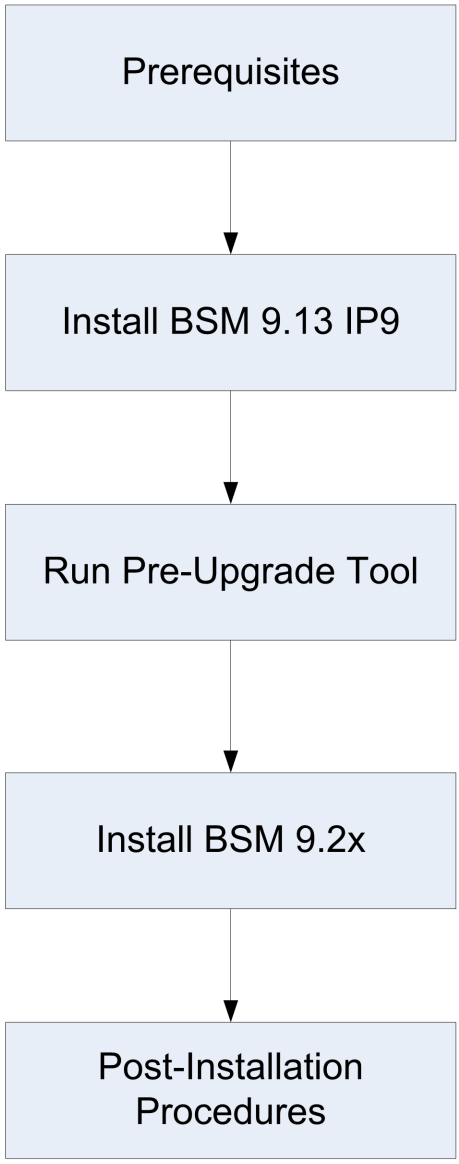
   For more details about this utility, see "Server Deployment and Setting Database Parameters" on page 169.
9. Restart all BSM servers.

   After you have installed all additional servers, restart all other BSM servers and data collectors to allow them to recognize the new servers.

Part II: Staging Upgrade

Chapter 14: Overview of BSM 8.0x to 9.26 Staging Upgrade

The upgrade from BSM 8.0x to BSM 9.26 involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Prepare your source environment for the upgrade process by checking system requirements, planning your upgrade, backing up files, and so on.

This includes the following major steps:

-Installing BSM 9.10 on staging servers
-Install BSM 9.13 IP9
-Replicating the database schema
-Performing intermediate procedures
-Running the BSM 9.13 IP9 upgrade wizard

The pre-upgrade tool migrates event-related configurations and certificates from BSM 9.13 IP9 to BSM 9.26.

This includes the following major steps:

-Uninstalling BSM 9.13 IP9
-Installing BSM 9.26
-Running the BSM 9.26 upgrade wizard

Configure the staging servers, complete the upgrade process, and perform other steps to complete the upgrade process.

Chapter 15: Prerequisites

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

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 Getting Started 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 131.

   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.

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

Product	Details
Operations Orchestration (OO)	If you were using OO with BSM 8.0x, you must upgrade to OO 7.51 or later. For more information, see the support matrix.

Product	Details
Service Manager (SM)	If you had integration between SM and BSM 8.0x via HP Universal CMDB, follow the instructions in the HP Universal CMDB upgrade procedures. For details, see "Upgrading HP Universal CMDB Integration - Splitting Procedure" on page 197.
CLIP	For information about upgrading an integration with HP CLIP 1.5, contact customer support.
HP Universal CMDB	For information about upgrading HP Universal CMDB and products that integrate with it, see "HP Universal CMDB (embedded/external) Upgrade Information" on page 195.
Network Node Manager i (NNMi)	You can continue to use BSM 9.1x without upgrading your integration with NNMi. If you choose to upgrade to NNMi 9.x, there are optional upgrades to this integration. For more information, see "NNMi Upgrade Information" on page 199

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 https://softwaresupport.hp.com.

4. Review relevant information

Review relevant information describing changes from BSM 8.0x to BSM 9.1x. Depending on your BSM configuration, review the relevant upgrade chapters in the BSM 9.1x Upgrade Guide.

5. 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. In BSM 9.23, support for SQL Server 2012 was added. Make sure 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.

6. 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.

7. 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.

8. Install the latest BSM 8.0x service pack

Install the latest service pack on the BSM 8.0x servers (8.07 at the time of the 9.23 release). If you are starting from BSM 8.0, this can be done by installing 8.01, then 8.07. For details, see the Service Pack release notes.

Note: If your version of BAC is older than 8.0x (such as 7.50), you need to perform an upgrade to BAC 8.0x before starting the processes described in this upgrade guide. For details about, see the Upgrade section of the BAC 8.0x Deployment Guide.

9. Run pre-upgrade tool

Run the pre-upgrade tool to view a customized list of items that may need attention before starting the upgrade. For details, see the BSM 8.07 Pre-Upgrade Tool Guide.

10. Upgrade external HP Universal CMDB

    If you have an external HP Universal CMDB, upgrade it to a version compatible with your version of BSM.

11. Import DDM Content Pack 8

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

12. 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.

13. EUM Pre-Upgrade Procedures

    Ensure that all necessary Session Identification configurations do not have empty session ID values. Those with empty session ID values are not upgraded.

    Check-in all BPM scripts to the Script Repository. The upgrade process does not preserve the checked-out status of scripts.

14. Migrate custom integration adapters

    If you have custom integration adapters or if you modified out-of-the-box adapters, you will need to manually migrate these to BSM 9.1x. For details, see "Migrating Modified UCMDB Integration (Federation) Adapters" on page 200.

15. Migrate custom rules in Service Health and SLM

    If you created custom Java rules, custom rule .jar files, or custom Groovy rule files in pre-9.0 versions of BSM, contact HP Support for instructions on modifying and packaging them for BSM 9.x before upgrading. For details, see "Custom Rules" on page 213.

16. 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**).

17. Verify Content Pack compatibility

    Make sure your content packs are compatible with your version of HP Universal CMDB. Incompatibilities can cause problems during the upgrade. For example, installing Content Pack 9 with HP Universal CMDB 8.x could result in problems during the upgrade procedure.

18. Back up database schema (recommended)

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

19. 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 40 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. Certain BSM components can coexist on BSM servers. For details on coexistence support, see the BSM System Requirements and Support Matrixes Guide.
- If you plan to use the IIS web server, install it prior to BSM installation and enable it after the installation is completed. For more information, see "Working with the Web Server" on page 158.
- 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**.
- The installation directory name should consist of only alphanumeric characters (a-z, A-Z, 0-9).
- User Access Control (UAC) must be disabled before installing BSM. UAC is enabled by default in some version of Windows Server (for example: 2008 SP2) and must be manually disabled.
- 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.
- If you do not have a profile database on your source environment, please add one before starting the upgrade. The database should be marked as the default profile database. Most users already have a profile database, but in some scenarios where BSM is being used exclusively for OMi, a profile database may not have been previously created.

- You must have administrator privileges to install BSM on the server machine.
- In the BSM cluster, open port 21212 on the Data Processing Server.

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, 29000-29000, 4444-4444, 8083-8083, 8093-8093.

These port 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 40 GB of free disk space. The /tmp directory should have at least 2.5 GB of free disk space. You can change the /tmp directory by running the following command:

  ```
  export IATEMPDIR=/new/tmp/dir
  ```

  ```
  export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/dir
  ```

  where `/new/tmp/dir` is the new /tmp directory

  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. Certain BSM components can coexist on BSM servers. For details on coexistence support, see the BSM System Requirements and Support Matrixes Guide.

- Before installing BSM on a Linux machine, make sure that SELinux does 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.

  On systems with SELinux disabled, the `SELINUX=disabled` option is configured in **/etc/selinux/config**:

  ```
  # This file controls the state of SELinux on the system.
  # SELINUX= can take one of these three values:
  #       enforcing - SELinux security policy is enforced.
  #       permissive - SELinux prints warnings instead of enforcing.
  #       disabled - No SELinux policy is loaded.
  SELINUX=disabled
  # SELINUXTYPE= can take one of these two values:
  #       targeted - Targeted processes are protected.
  #       mls - Multi Level Security protection.
  SELINUXTYPE=targeted
  ```

Also, the `getenforce` command returns **Disabled**:

```
~]$ getenforce
Disabled
```

To confirm that the aforementioned packages are installed, use the rpm utility:

```
~]$ rpm -qa | grep selinux
selinux-policy-3.12.1-136.el7.noarch
libselinux-2.2.2-4.el7.x86_64
selinux-policy-targeted-3.12.1-136.el7.noarch
libselinux-utils-2.2.2-4.el7.x86_64
libselinux-python-2.2.2-4.el7.x86_64
```

```
~]$ rpm -qa | grep policycoreutils
policycoreutils-2.2.5-6.el7.x86_64
policycoreutils-python-2.2.5-6.el7.x86_64
```

```
~]$ rpm -qa | grep setroubleshoot
setroubleshoot-server-3.2.17-2.el7.x86_64
setroubleshoot-3.2.17-2.el7.x86_64
setroubleshoot-plugins-3.0.58-2.el7.noarch
```

Before SELinux is enabled, each file on the file system must be labeled with an SELinux context. Before this happens, confined domains may be denied access, preventing your system from booting correctly.

To prevent this, configure `SELINUX=permissive` in the **/etc/selinux/config file**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

As a root user, restart the system. During the next boot, file systems are labeled. The label process labels all files with an SELinux context:

```
~]# reboot
```

In permissive mode, SELinux policy is not enforced, but denials are logged for actions that would have been denied if running in enforcing mode.

Before changing to enforcing mode, as a root user, run the following command to confirm that SELinux did not deny actions during the last boot. If SELinux did not deny actions during the last boot, this command does not return any output.

```
~]# grep "SELinux is preventing" /var/log/messages
```

If there were no denial messages in the **/var/log/messages** file, configure `SELINUX=enforcing` in **/etc/selinux/config**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Reboot your system. After reboot, confirm that `getenforce` returns **Enforcing**:

```
~]$ getenforce
Enforcing
```

```
~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
```

- 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 as the upgrade process cannot be performed silently.

- If you do not have a profile database on your source environment, please add one before starting the upgrade. The database should be marked as the default profile database. Most users already have a profile database, but in some scenarios where BSM is being used exclusively for OMi, a profile database may not have been previously created.
- In the BSM cluster, open port 21212 on the Data Processing Server.
- Before installing BSM 9.26 on Oracle Linux (OEL) or Red Hat Enterprise Linux operating systems for supported 6.x versions and 7.x versions, you must install the following RPM packages on all machines running BSM:

■ glibc	■ libXext
■ glibc-common	■ libXtst
■ nss-softokn-freebl	■ compat-libstdc++-33
■ libXau	■ libXrender
■ libxcb	■ libgcc
■ libX11	■ openssl098e
■ compat-expat1	■ rpm-devel

To install the RPM packages listed in the upper table, run the RPM installation tool on all machines running BSM:

<BSM_install_folder>/rhel_oel_installation_fix/rpm_installer.sh.

- If the script fails to install any of the RPM packages, the following message appears:

```
!!! ERROR: package <package name> has not been installed successfully

In this case, refer the problem to your system administrator.
```

- If the script detects that an RPM package is already installed, it skips that package and continues with the next package.

  However, you can force the tool to try to re-install any pre-installed packages by adding the **f** parameter to the command:

  <BSM_install_folder>/rhel_oel_installation_fix/rpm_installer.sh f

If the Yum Linux upgrade service is not functional on your machine, you will need to download and install the necessary RPM packages manually by running the following command:

yum install -y openssl098e glibc.i686 glibc-common.i686 nss-softokn-freebl.i686 libXau.i686 libxcb.i686 libX11.i686 libXext.i686 libXtst.i686 compat-libstdc++-33.i686 libXrender.i686 libgcc.i686 compat-expat1 rpm-devel

The version of these packages changes from system to system. You can download the packages from any RPM repository site that matches your system specifications. The following RPM search tool can assist you in this task (http://rpm.pbone.net/).

To determine the package version you need to download, execute the following command in a terminal window:

rpm –qa ${PACKAGE_NAME} (ex: rpm -qa glibc)

The command will return the following text:

```
# rpm -qa glibc

glibc-2.12-1.132.el6.x86_64
```

This text indicates the package version required for your machine.

In this case, you would need to download the i686 architecture package with the same version - glibc-2.12-1.132.el6.i686 – and install it manually.

OMi Pre-Upgrade Procedure

If you were using OMi with BSM 8.0x, perform the following steps before beginning the BAC 8.x to BSM 9.1x upgrade.

Note: The OMi database schema is not automatically upgraded by this process. A new OMi DB schema must be created during the upgrade from 8.x. Some of the following steps are required in order to insure OMi configuration can be restored at the completion of the upgrade.

1. ## Verify the Supported HPOM Versions

   Make sure that the version of HPOM that you plan to use with BSM 9.26 is supported. For more information about supported versions, see the BSM System Requirements and Support Matrixes.

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

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

   http://support.openview.hp.com/selfsolve/document/KM32348

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

   ### Limitations

   The following limitations may arise if you do not upgrade the SPIs

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

Indicator	9.1x Content Pack
Ping Availability	Infrastructure Content Pack and some dependent Content Packs
Server Load	Lync Server Content Pack
EJB Timeout Rate	JEE Application Server Content Pack

Indicator	9.1x Content Pack
JMS Server Utilization	JEE Application Server Content Pack
Transaction Timeout Errors	JEE Application Server Content Pack
Transaction Capacity Utilization	JEE Application Server Content Pack
Transaction System Errors	JEE Application Server Content Pack

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

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

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

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

4. Back Up the OMi Configuration Files - Recommended

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

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

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

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

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

%TOPAZ_HOME%\conf\opr

b. Save these files to a safe location, for example:

- Windows: **%TEMP%\migration**
- Linux: **/tmp/migration**

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

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

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

%TOPAZ_HOME%\opr\resources\images\hivalues

b. Save these files to a safe location, for example:

- Windows: **%TEMP%\migration**
- Linux: **/tmp/migration**

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

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

a. Make a note of each Event Assignment rule and each associated filter.

b. Recreate these filters and Event Assignment rules in the migrated installation.

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

a. Make a note of each user and the filter configurations associated with that user.

b. Recreate these filters in the migrated installation.

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

a. Make a note of each Graph Template and Graph Assignment that has been created. (After migrating from BAC 8.x to 9.1x, when you install content packs 9.1x on BSM 9.1x, new graph

templates for all content packs are available in the Content Manager.)

b. Recreate your Graph Templates and Graph Assignments in the migrated installation.

5. Delete CIs with Short Hostnames

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

To delete CIs with short hostnames:

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

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

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

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

c. Identify and delete all SQL Server CIs whose name field is not filled with the FQDN.

6. Update Empty Host Name Attributes of Host CIs

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

To update empty Host Name attributes, complete the following steps:

a. In the BAC 8.x Enrichment Manager, create a new, active enrichment rule based on a new TQL:

Select **Admin > Universal CMDB > Modeling > Enrichment Manager**.

To create a new enrichment rule, right-click anywhere in the Enrichment Rules pane and click **New**.

In the enrichment rule wizard, specify a name and description for the rule. Select **Rule is active**. As base TQL type, select **Base the Enrichment on a new TQL**. Close the wizard by clicking **Finish**.

b. Drag the CI type **Host** to the editing pane.

c. Right-click **Host** in the editing pane and select **Node Properties**.

d. Add a new attribute condition by clicking the button with the green plus sign. If necessary, select the new condition, then select Host Name - (string) from the **Attribute name:** drop-down list.

   Select Is null from the **Operator:** drop-down list. (The Value field remains empty.) Click **OK**.

e. *Optional:* Calculate the TQL query results.

f. In the upper-left corner of the editing pane, click **TQL Mode** and select **Enrichment Mode**.

g. Right-click **Host** in the editing pane and select **Update Node**.

h. In the **Node Definition** dialog, select the **Host Name** attribute in the **Name** column, then click the **By Attribute** button. The string **Host** appears in the drop-down list next to the **By Attribute** button.

   To specify the attribute to be taken, select the **Name** attribute in the drop-down list to the right of the Host attribute. Click **OK**.

i. Navigate to Scheduler, select:

   Admin > Universal CMDB > Settings > Scheduler

   Add a new job by clicking the button with the green plus sign. The **Job Definition** dialog opens where you specify a name and a definition.

   To add an action to the job, click the button with the green plus sign under **Actions**. The **Action Definition** dialog opens. Select **Run an Enrichment rule** and click **Next**. Select the enrichment rule that you created above and click **Finish**.

j. In the **Job Definition** dialog, under **Scheduler**, select **Once** and specify the current time. Click **OK** to save the job definition and close the dialog.

k. Wait for the enrichment to finish. Check that the enrichment query created above no longer matches any hosts.

   For more information about enrichment rules and scheduling, see the *Model Management* section in the HP UCMDB online help.

7. Export the OMi Configuration Data - Optional

This task describes how to export the OMi configuration data using the Content Manager command line interface.

Export the OMi 8.10 configuration data in the following situations:

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

To export the OMi configuration data, complete the following steps:

a. From a BAC 8.x Gateway Server, in a command prompt window, go to the following directory:

   %TOPAZ_HOME%\opr\bin

b. If you are retaining the HPOM Plug-ins (SPIs) that you have been using with your OMi 8.10 installation, export *all* 8.10 content packs. Enter the following command:

   ContentManager -snapshot -username <*administrator account*> -password <*administrator password*> -o <*snapshot file name*>.xml

   Where the administrator account must have read and write access to the Content Manager.

c. If you collected your modifications to OMi 8.10 content in a custom content pack, export that custom content pack. Enter the following command:

   ContentManager -username *administrator account*> -password <*administrator password*> -e <*custom content pack name*> -o <*custom file name*>.xml

   Where the administrator account must have read and write access to the Content Manager.

d. Save the exported data output file to a temporary location, for example:

   - Windows: **%TEMP%\migration**
   - Linux: **/tmp/migration**

   (Staging only) If you are upgrading in Staging Mode and the BSM 9.1x Gateway Server host system is already installed and available, copy the exported data output file to a temporary location on the BSM 9.1x Gateway Server host system.

   The exported data must be converted to the syntax and model required by the BSM 9.1x version. For details, see "Convert OMi 8.10 Content Packs to 9.1x Model and Syntax - Optional" on page 105.

8. Archive Events - Optional

This task closes and archives any outstanding events. Execute this task on any BSM server (GW or DPS). Execute the following command line tools to close and archive the events.

a. %TOPAZ_HOME%\bin\opr-close-events.bat -all

b. %TOPAZ_HOME%\bin\opr-archive-events.bat -o %TEMP%\opr-event-archive-8.0.xml -u 2099.01.01

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 2 GB, type 2000.
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 GB, type 2000.
7. Click **OK** to save the new values and close the dialog box.

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.

Chapter 16: Install BSM 9.10

Install BSM 9.10 on one 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.

Note: Do not install more than one set of BSM servers. The upgrade process will use one set of servers to upgrade the database, and you will be directed to install any additional servers towards the end of the upgrade procedure

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_9.10_setup.exe

- For Linux:

  DVD2 > linux_setup > HPBsm_9.10_setup.bin

For more details, see the following sections:

"Installing BSM on a Windows Platform" on page 155

"Installing BSM on a Linux Platform" on page 163

Chapter 17: Install the Latest BSM 9.1x Minor-Minor Release and Patch

Install the latest minor minor version of BSM 9.1x and patch (if available).

1. **Prerequisites**

   - It is recommended that you back up all BSM databases and files you made custom changes to.
   - 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 HP Software Support site**

   a. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.

   b. Click **Search**.

   c. Select the relevant product, most recent 9.1x minor minor version, and operating system.

   d. Under Document Type, select **Patches**.

   e. Locate the installation files.

   f. Save the package locally and launch the relevant setup file to install the patch.

   g. Run the installation files on all BSM servers (Gateway and Data Processing).

   h. Run the post-installation wizard. This wizard follows the patch installation automatically.

   i. Repeat this procedure for the latest intermediate patch (if available).

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>

Chapter 18: Replicate Database

Replicate your original database onto a new database server. The new database will be used by the staging environment, upgraded, and eventually used as your BSM 9.26 database.

Make sure that your database version is supported in both the original and new BSM environments.

Chapter 19: OMi Mid-Upgrade Procedure

If you were using OMi with BSM 8.0x, perform this procedure between running the post-installation wizard and the upgrade wizard when upgrading BAC 8.x to BSM 9.1x.

1. Establish Trust Relationship

For connection and communication between the BSM and HPOM systems, you must establish a trust relationship between the systems.

> **Note:** The following steps use the ovcert, ovconfchg, and bbcutil command line tools. The tools are located in:
>
> Windows: **%OvInstallDir%\bin**
>
> Linux: **/opt/OV/bin**

To establish a trust relationship between BSM and HPOM systems:

a. Ensure that certificates have been set up on the Gateway and Processing Servers. For details, see "Post-Installation Tasks" in the BSM Installation Guide.

b. On all BSM Processing Servers, execute the following command:

ovcert -exporttrusted -file BSM_DPS<#>.cer

c. On the HPOM management server, execute the following command:

ovcert -exporttrusted -file other.cer

d. Copy other.cer from the HPOM management server to all BSM Processing Servers.

e. Copy BSM_DPS<#>.cer from the BSM Processing Server to the HPOM management server and all other BSM Processing Servers.

f. On all BSM Processing Servers, execute the following commands:

ovcert -importtrusted -file other.cer

ovcert -importtrusted -file other.cer -ovrg server

g. On the HPOM management server and on all BSM Processing Servers, execute the following commands:

ovcert -importtrusted -file BSM_DPS<#>.cer

ovcert -importtrusted -file BSM_DPS<#>.cer -ovrg server

h. If you have a multi-machine deployment, execute the following command on all Gateway Servers:

setup-secure-communication <BSM processing server>

If you are not sure if the certificate was already issued for the Gateway server, use the command **ovconfchg -edit** to check the **hp.XplConfig.ovconfchg** file. If **sec.cm.client.certificate_server** is set to the HPOM management server, then the certificate was already issued.

i. If the certificate was already installed on the system, execute the following command on all Gateway servers:

ovcert -updatetrusted

j. Configure the load balancers and reverse proxies according to the instructions in the BSM Installation Guide depending on your certificate authority and setup. Make sure that the new Data Processing Server certificates are trusted if no central certificate authority is used.

After establishing a trust relationship between the BSM and HPOM systems, check the connection between the two systems.

To check the connection between BSM and HPOM:

a. From the HPOM management server, verify that communication to the BSM installation is possible (the return value should be eServiceOk) by executing the following command on the HPOM server:

bbcutil -ping https://<BSM load_balancer, proxy server, or single_gateway_server>

Example of the command result:

https://<BSM servername>: status=eServiceOKcoreID=7c66bf42-d06b-752e-0e93-e82d1644cef8 bbcV=06.10.105appN=ovbbccb appV=06.10.105 conn=1 time=1094 ms

b. From all BSM Processing Server hosts, verify that communication with the HPOM management server host is possible (the return value should be eServiceOk) by executing the following command:

bbcutil -ping https://<HPOM_management_server_hostname>

Example of the command result:

https://<HPOM servername>: status=eServiceOK coreID=0c43c032-5c94-7535-064a-f7654a86f2d3 bbcV=06.10.070appN=ovbbccb appV=06.10.070 conn=7 time=140 ms

c. On the HPOM management server, add any new BSM Gateway Servers, load balancers, or reverse proxies to the list of target servers for discovery data.

Restart the discovery server processes on the HPOM management server:

HPOM for Windows:

- **net stop "OvAutoDiscovery Server"**
- **net start "OvAutoDiscovery Server"**

HPOM for UNIX or Linux:

- **ovc -stop opcsvcdisc**
- **ovc -start opcsvcdisc**

2. Configure HPOM to Forward Events to BSM 9.1x

By default, when using a staging environment to upgrade BSM, only the original OMi 8.10 servers receive events from HPOM. To allow event forwarding to the new staging servers, update the HPOM message forwarding policies as appropriate. As soon as the staging servers are online, both the original OMi 8.10 and the new BSM 9.1x environments receive events from HPOM. Until then only the original servers receive the events.

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. Add another message target manager 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 "$OPC_ALWAYS"
       OPCMGR IP 0.0.0.0 "<OMi 8.10 fully qualified host name>"
        MSGTARGETMANAGER
        TIMETEMPLATE "$OPC_ALWAYS"
        OPCMGR IP 0.0.0.0 "<BSM 9.1x fully qualified host name>"
```

Note: This forwards all messages to OMi. If you want to reduce the number of messages to be sent, see “Server-based Flexible Management” in the HPOM documentation and modify the text of the policy, so that only a selected subset of messages is sent to OMi.

e. Replace <*fully qualified host name*> in the text with the fully qualified hostname of the Gateway Server system that should receive HPOM messages (for example, HPGwSrv.example.com).

In deployments involving a load balancer, a NAT device, or a reverse proxy, use the fully qualified hostname of the system used to access the Gateway Server system (for example, VirtualSrv.example.com).

For details about load balancing and high availability, see the section “High Availability for HP Business Service Management” in the HP Business Service Management *Deployment Guide*.

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. Add another message target manager as shown in the following example policy text:

```
TIMETEMPLATES
# none

RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
  SECONDARYMANAGERS
  ACTIONALLOWMANAGERS

  MSGTARGETRULES
    MSGTARGETRULE DESCRIPTION "Forward all messages rule"
      MSGTARGETRULECONDS
      MSGTARGETRULECOND DESCRIPTION "Forward all messages"

      MSGTARGETMANAGERS
        MSGTARGETMANAGER
        TIMETEMPLATE "$OPC_ALWAYS"
        OPCMGR IP 0.0.0.0 "<First Target Manager>"

          MSGTARGETMANAGER
          TIMETEMPLATE "$OPC_ALWAYS"
          OPCMGR IP 0.0.0.0 "<OMi 8.10 fully qualified host name>"
          MSGTARGETMANAGER
          TIMETEMPLATE "$OPC_ALWAYS"
          OPCMGR IP 0.0.0.0 "<BSM 9.1x fully qualified host name>"
```

Note: This forwards all messages to OMi. If you want to reduce the number of messages to be sent, see “Server-based Flexible Management” in the HPOM documentation and

modify the text of the policy, so that only a selected subset of messages is sent to OMi.

e. Replace <*fully qualified host name*> in the text with the fully qualified hostname of the Gateway Server system that should receive HPOM messages (for example, HPGwSrv.example.com).

   In deployments involving a load balancer, a NAT device, or a reverse proxy, use the fully qualified hostname of the system used to access the Gateway Server system (for example, VirtualSrv.example.com).

   For details about load balancing and high availability, see the section “High Availability for HP Business Service Management” in the HP Business Service Management *Deployment Guide*.

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

3. Convert OMi 8.10 Content Packs to 9.1x Model and Syntax - Optional

Convert the content packs that you exported from your OMi 8.10 installation to the syntax and model required by BSM 9.1x. You only need to complete this step if you exported content as described in "OMi Pre-Upgrade Procedure" on page 88.

The ContentMigration migration tool is located in:

- Windows: **%TOPAZ_HOME%\opr\bin\ContentMigration.bat**
- Linux: **/opt/HP/BSM/opr/bin/ContentMigration.sh**

The ContentMigration migration tool accepts the following options:

ContentMigration <inputFileName> <outputFileName> [-A Availability_KPI_UUID] [-P Performance_KPI_UUID]

For more information about the parameters that the ContentMigration command, see the following list:

<inputFileName>

Name of the input file. This must be an OMi Content Pack in XML file format from OMi 8.10.

<outputFileName>

Name of the output file, to which the BSM 9.1x formatted content pack XML file is written.

[-A <Availability_KPI_UUID>]

Optional: Specify an alternative availabilty KPI as the standard availability KPI assignment. For details, see "Alternative KPIs" on the next page.

[-P <Performance_KPI_UUID>]

Optional: Specify an alternative performance KPI as the standard availability KPI assignment. For details, see "Alternative KPIs" on the next page.

Note: By default the OMi 8.10 KPI assignments to Availability and Performance are replaced by assignments to System Availability and System Performance respectively. To assign alternative KPIs as the standard availability KPI assignment, see "Alternative KPIs" on the next page.

To convert an OMi 8.10 content pack to the model and syntax required by BSM 9.1x:

a. Copy the exported data output file of the content packs that you exported from your OMi 8.10 installation in the "OMi Pre-Upgrade Procedure" on page 88. Store the output file in a temporary location on the BSM 9.1x Gateway Server host system that is upgraded first, for example:

   - Windows: **%TEMP%\migration**
   - Linux: **\tmp\migration**

b. On the BSM 9.1x Gateway Server host system, convert the exported content packs:

   - To convert the exported snapshot of all OMi 8.10 content packs, enter the following command:
     - Windows: **%TOPAZ_HOME%\opr\bin\ContentMigration <**snapshot file name**> <**output file name**>**

- Linux: **/opt/HP/BSM/opr/bin/ContentMigration <**snapshot file name**> <**output file name**>**

◦ To convert the exported custom content pack that contains your OMi 8.10 modifications, enter the following command:

- Windows: **%TOPAZ_HOME%\opr\bin\ContentMigration <**custom file name**> <**output file name**>**
- Linux: **/opt/HP/BSM/opr/bin/ContentMigration <**custom file name**> <**output file name**>**

Substitute the appropriate file names and specify alternative KPIs, if necessary. See also "Alternative KPIs" below.

c. Copy the converted OMi 8.10 content pack *snapshot* to the following location on the BSM 9.1x Gateway Server host system:

◦ Windows: **%TOPAZ_HOME%\conf\opr\content\migration**

◦ Linux: **/opt/HP/BSM/conf/opr/content/migration**

The upgrade wizard automatically uploads all converted content packs that reside in that location.

d. *Optional:* Delete the original, unconverted OMi 8.10 content packs from the following temporary directory on the BSM 9.1x Data Processing Server host system:

◦ Windows: **%TEMP%\migration**

◦ Linux: **/tmp/migration**

Alternative KPIs

You can assign alternative KPIs to the default ones. To do this you need to know what KPIs are available and what their stableId attributes are in the **SH-DefaultKPIs.xml** file.

To assign alternative KPIs, complete the following steps:

a. Open the following file:

◦ Windows: **%TOPAZ_HOME%\conf\opr\content\en_US\SH-DefaultKPIs.xml**

◦ Linux: **/opt/HP/BSM/conf/opr/content/en_US/SH-DefaultKPIs.xml**

b. Select an alternative KPI by its stabeId attribute.

KPIs are contained in XML elements named <Dimension>. Select a KPI where the application attribute is equal to dashboard (application="dashboard").

c. Run the ContentMigration migration tool and specify the stableId attribute of the selected KPI for the -A or -P parameters.

ContentMigration <exported_OMi_8.10_content_pack>.xml <converted_BSM_9.1x_content_pack>.xml -A <stableId_of_alternative_Availability_KPI> -P <stableId_of_alternative_Performance_KPI>

4. Restore Custom Icons from OMi 8.10 - Optional

If you have saved copies of OMi 8.10 icons for health indicators and want to continue to use them, copy the saved OMi 8.10 files to the BSM 9.1x installation.

a. Because some of the icons have changed in 9.1x, from a BSM 9.1x Gateway Server host system, make a backup copy of all the files in the following directory and subdirectories:

- Windows: **%TOPAZ_HOME%\AppServer\webapps\site.war\images\gui\severities**
- Linux: **/opt/HP/BSM/AppServer/webapps/site.war/images/gui/severities**

b. Copy the custom icon files that you saved from your OMi 8.10 installation in the step "OMi Pre-Upgrade Procedure" on page 88 to the following location on the BSM 9.1x Gateway Server host system:

- Windows: **%TOPAZ_HOME%\AppServer\webapps\site.war\images\gui\severities**
- Linux: **/opt/HP/BSM/AppServer/webapps/site.war/images/gui/severities**

5. Import Security Certificates to JRE Truststore

Secure environments only: To re-enable the trust relationship between the Java Runtime Environment (JRE) and the LDAP server, you must import the LDAP trusted certificate to the JRE truststore.

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

- **<Gateway Server installation directory>/JRE/lib/security/cacerts**
- **<Gateway Server installation directory>/JRE64/lib/security/cacerts**

6. Upgrade Wizard Notes

Migrated OMi 8.10 content and 9.1x content is uploaded using the create mode. The overwrite mode is not used and the OMi 8.10 content is retained to support the SPI DVD release 2008.1 SPIs.

The upgrade wizard first uploads the content packs for the locale set for the system, followed by English-language content packs that were not uploaded during the first upload phase. For example, if the locale is set to Japanese, Japanese-language content packs will be uploaded first, followed by English-language content packs. This can result in mixed-language content.

Note: If the OprUpgrader component partially fails during the configuration upgrade, check the opr-admin.log file to make sure that the HPOprInf, HPOprJEE, HPOprMss, and HPOprOra content packs are loaded successfully:

- Windows: **%TOPAZ_HOME%\log\EJBContainer\opr-admin.log**
- Linux: **/opt/HP/BSM/log/EJBContainer/opr-admin.log**

If these content packs are loaded successfully, you can click Pass Upgrade and continue with the upgrade. If one of these content packs is not upgraded successfully, you must first correct the problem. Otherwise the subsequent SiSConfigurationEnrichment upgrade fails.

Chapter 20: 9.1x Upgrade Wizard

Run the BSM 9.1x upgrade wizard on all 9.1x machines to transfer your data from the original 8.0x format to the 9.1x format. The SDR and Data Transfer Tool must not be executed yet. When the upgrade wizard reaches the screen instructing you to run the SDR, select external SDR in order to continue with the wizard without running the SDR.

On the last screen of the wizard, select the option to **Perform cleanup now**. The upgrade wizard runs a second time in completion mode and finalizes the upgrade process.

Note: When running this wizard, you must create a new Event database schema. Do not use the pre-existing schema as this may cause the upgrade to fail.

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.bat

- Linux:

  /opt/HP/BSM/bin/upgrade_wizard_run.sh

When the wizard is finished, start all BSM servers. For details, see "Starting and Stopping BSM" on page 147.

For details about the upgrade wizard, see "Upgrade Wizard" on page 186.

Chapter 21: Configuration Procedures

Follow the procedures in this chapter. Note that some procedures depend on your specific BSM environment and are not required in all BSM upgrade scenarios.

OMi Post-Upgrade Procedure

If you were using OMi with BSM 8.0x, perform this procedure after running the upgrade wizard when upgrading from BAC 8.x to BSM 9.1x.

1. Update the Key Attribute of CI Collections Synchronized from HPOM

   With BSM 9.10 a new key attribute was introduced for the CI collection CI type.

   If you have previously synchronized HPOM node groups with BSM 8.x or BSM 9.0x, create an enrichment rule that copies the value of the Name attribute to the CI Collection ID attribute.

   To update the CI Collection ID attribute, complete the following steps:

   a. In the Enrichment manager, create a new active enrichment rule based on a new TQL as follows:

      i. Select **Admin -> RTSM Administration -> Enrichment manager**

      ii. Right-click in the **Enrichment Rules** pane and click **New**.

      iii. In the enrichment rule wizard, specify a name and description for the rule.

      iv. Select **Rule is active** and click **Next**.

      v. For the Base Query Type, select **Base the Enrichment on a new query**.

      vi. Click **Finish** to save the enrichment rule.

   b. Drag the CI type **Ci Collection** to the editing pane of the newly created enrichment rule.

   c. Right-click **Ci Collection** in the editing pane and select **Query Node Properties**.

   d. In the **Query Node Properties** window, clear **Include subtypes**.

   e. Add a new attribute condition ().

   f. Select the new condition, and from the **Attribute name:** drop-down list select **Ci Collection ID - (string)**.

   g. From the **Operator:** drop-down list, select **Is null**. (The **Value** field remains empty.)

   h. Add another new attribute condition (). Check that this condition is linked with **AND** to the previous condition.

   i. Select the new condition, and from the **Attribute name:** drop-down list select **Monitored By - (string_list)**.

j. From the **Operator:** drop-down list, select **Contains**.

k. In the Value field, enter OM.

l. Click **OK** to save the query node properties.

m. *Optional:* Calculate the query results.

n. Change **Query Mode** to **Enrichment Mode** (first field, top-left corner of the editing pane).

o. Right-click the **Ci Collection** icon in the editing pane and select **Update Query Node**.

p. In the Query Node Definition dialog, select the **CI Collection ID** attribute from the **Name** column.

q. Select the **By Attribute** radio button. The string name **CI Collection** appears in the first drop-down list next to the **By Attribute** button.

   To specify the attribute to be taken, select the **Name** attribute in the dropdown list to the right of the CI Collection attribute field.

   Click the **Save** icon.

r. Click **OK**.

s. Navigate to the Scheduler:

   Admin > RTSM Administration > Scheduler

t. Add a new job condition ( ).

   Specify a name and a definition in the Job Definition dialog box.

u. Add an action to the job (under Actions in the Job Definition dialog box).

v. In the Action Definition dialog box, select **Run an Enrichment rule** and click **Next**.

w. Select the enrichment rule that you created in Step 1 and click **Finish**.

x. In the Job Definition dialog box, under **Scheduler**, select **Once** and specify the current time.

y. Click **OK** to save the job definition and close the dialog box.

z. Wait for the enrichment to finish. Check that the enrichment query created in Step 1 no longer matches any hosts.

   For more information about enrichment rules and scheduling, see the Model Management section in the BSM online help.

2. Configure the HPOM Message Forwarding Policy for the BSM 9.1x Installation Only - Optional

   Remove the entry for the obsoleted OMi 8.10 installation from all HPOM message forwarding policies.

3. Exchange Certificates Between HPOM and BSM

   Establish a trust relationship between the systems. For details, see "How to Establish a Trust Relationship for a Server Connection" on page 204

4. Manage BSM Nodes in HPOM

   In HPOM, update the nodes that represent the BSM systems.

   To enable communication between HPOM and OMi 8.10, the BAC 8.x servers were set up as managed nodes in HPOM (but no HP Operations Agent software installed). After the migration, the managed nodes that represent the BAC 8.x servers are no longer needed in HPOM and you can delete them. For details, see "Deleting BAC 8.x Managed Nodes in HPOM" below. (The BSM 9.1x servers do not need to be added to HPOM to enable communication.)

   Do not delete the BAC 8.x managed nodes if the HP Operations Agent software is installed and HPOM monitors the BAC 8.x servers for the purpose of system and performance management:

   - For direct upgrades, if this is the case, you must update the nodes' core IDs in HPOM because the systems have received new certificates. For details, see "OMi Post-Upgrade Procedure" on page 112 and "OMi Post-Upgrade Procedure" on page 112.
   - If you are performing a staging upgrade and you want to monitor the new BSM 9.1x systems with HPOM, add the 9.1x systems as new managed nodes to HPOM and install the HP Operations Agent software to these nodes. For details, see the HPOM documentation.

Deleting BAC 8.x Managed Nodes in HPOM

To enable communication between HPOM and OMi 8.10, the BAC 8.x servers were set up as managed nodes in HPOM (but no agent software installed). After the migration, the managed nodes that represent the BAC 8.x servers are no longer needed in HPOM and you can delete them.

Note: Do not delete the BAC 8.x managed nodes if the HP Operations Agent software is installed and HPOM monitors the BAC 8.x servers for the purpose of system and performance management.

To delete the BAC 8.x managed nodes in HPOM for Windows, complete the following steps:

a. Open the Configure Nodes dialog, right-click the **Nodes** folder in the console tree and select **Configure > Nodes**.

b. Select the nodes that represent the BAC 8.x servers and press the **Delete** key.

c. Click **Yes** to confirm that you want to delete the nodes.

d. Close the Configure Nodes dialog.

To delete the BAC 8.x managed nodes in HPOM for UNIX or Linux, complete the following step:

On the HPOM for UNIX or Linux management server, use the opcnode command line tool to delete the nodes, type:

 # opcnode -del_node node_name=<node_name> \net_type=< network_type>

<node_name>: Name of the managed node that you want to remove from the HPOM database.

<network_type>: Type of managed node, for example: Non IP, IP (Network), or External (Node).

The opcnode command also ensures that the managed node's assignment to any node groups is removed. For more information about the opcnode command and its parameters and options, see the *opcnode(1m)* manual page.

5. Configure Dynamic Topology Synchronization

Before configuring forwarding of topology (node and service) data to Operations Management from Operations Manager management servers, perform the procedure "How to Run Dynamic Topology Synchronization" on page 207.

6. Validate Event Synchronization

Validate event synchronization and test the connection between HPOM and OMi.

To verify message forwarding from HPOM to OMi complete the following steps:

In this section, you check whether the message forwarding policy for sending messages from HPOM to OMi is correctly configured. To do so, complete the following steps:

a. Make sure the BSM platform is running.

b. Make sure at least one open message interface policy is deployed on your HPOM system. For instructions and details, see the HPOM documentation.

c. On the HPOM system, open a command or a shell prompt.

d. Create a new message by executing the following command:

   - On the HPOM for Windows system:

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

   - On the HPOM for UNIX and HPOM for Linux system:

     /opt/OV/bin/OpC/opcmsg a=App o=Obj msg_text="Hello"

If you have correctly configured the server-based flexible management, the message arrives at the HPOM management server and is forwarded to OMi. You can view the events with the Operations Management Event Browser.

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

To verify the synchronization of HP OMi events with HPOM messages, complete the following steps:

a. Make sure the BSM platform is running.

b. Log on to the BSM platform management console.

c. Click **Applications > Operations Management**.

d. In the Event Browser, select an event that has been synchronized in HPOM and OMi earlier.

e. In the Event Details pane, click the Edit button of the General tab.

f. From the Severity drop-down list, choose another severity (for example, major) and click **Save** to change it to the selected severity.

g. In HPOM, verify the severity of this event and make sure it has been set to the new severity value.

7. Validate Topology Synchronization

If you have modified the out-of-the-box topology synchronization packages, you must manually recreate your changes in the 9.1x topology synchronization packages.

If you have created and saved your own custom topology synchronization packages in OMi 8.10, copy the saved custom packages to the BSM 9.1x installation. If these custom synchronization packages use out-of-the-box CI types, make sure that your synchronization packages still produce the desired results in BSM 9.1x, complete the following steps.

To validate topology synchronization, complete the following steps:

a. Copy the custom topology synchronization rules that you saved from your OMi 8.10 installation in the step "OMi Pre-Upgrade Procedure" on page 88 to the following location on the BSM 9.1x Data Processing Server host system:

   - Windows: **%TOPAZ_HOME%\conf\opr\topology-sync\sync-packages**
   - Linux: **/opt/HP/BSM/conf/opr/topology-sync/sync-packages**

b. On the BSM 9.1x Data Processing Server host system, run basic topology synchronization. Open a command prompt or shell and type:

   - Windows: **%TOPAZ_HOME%\bin\opr-startTopologySync.bat**
   - Linux: **/opt/HP/BSM/bin/opr-startTopologySync.sh**

c. If out-of-the-box CI types have changed in BSM 9.1x, the synchronization process ends with errors. Check the synchronization log file:

   - Windows: **%TOPAZ_HOME%\log\opr-topologysync**
   - Linux: **/opt/HP/BSM/log/opr-topologysync**

d. Enable the data dump option and verify the CI attributes:

   i. Navigate to the HPOM Topology Synchronization settings in the Infrastructure Settings Manager:

      Infrastructure Settings > Applications > Operations Management > Operations Management - HPOM Topology Synchronization Settings > Dump data

   ii. Change the value of **Dump data** to **true**.

   iii. Run the Topology Sync tool with the following command:

- Windows: **<HPBSM root directory>\bin\opr-startTopologySync.bat**
- Linux: **<HPBSM root directory>/bin/opr-startTopologySync.sh**

iv. Check if the file in the following directory contains all expected attributes for the CIs of your synchronization package:

- Windows: **%TOPAZ_HOME%\opr\tmp\datadump\postenrichment**
- Linux: **/opt/HP/BSM/opr/tmp/datadump/postenrichment**

e. Use the BSM 9.1x CI Type Manager to find changed CI types, adapt your mapping rules, and run topology synchronization again.

Repeat this process until all mapping errors have been resolved.

For more information about topology synchronization, see the HP Operations Manager i *Extensibility Guide*.

8. Recreate Your OMi 8.10 Modifications in 9.1x - Optional

If you upgraded the SPIs to SPI DVD release 2010 before the migration, you must manually recreate the modifications that you applied to the OMi 8.10 content in your 9.1x installation. Refer to your notes taken in "Make a Note of Each Modification to the OMi 8.10 Content Packs" on page 89.

Alternatively, if you exported and converted a custom content pack, upload the custom content pack in create mode after the migration.

To recreate upload the custom content pack in create mode, complete the following steps:

a. Change to the temporary location on the BSM 9.1x Gateway Server host system, where the converted custom content pack resides, for example:

- Windows: **%TEMP%\migration**
- Linux: **/tmp/migration**

b. Upload the custom content pack in create mode, enter the following command:

<HPBSM Install Directory>/opr/bin/ContentManager -username admin -password admin -i <converted custom content pack>

Where the administrator account must have read and write access to the Content Manager.

c. Verify the uploaded content pack in the Content Packs Manager.

9. Re-import the 9.1x Content - Optional

If you did *not* upgrade the SPIs to the SPI DVD 2010 release before the migration, but rather decide to switch to the new SPIs after the migration, you must reimport the 9.1x content with overwrite mode. However, the overwrite mode will overwrite *all* of your modifications. You must then manually recreate your OMi 8.10 modifications in the 9.1x content.

To reimport 9.1x content, complete the following steps:

a. Upgrade the HP Operations SPIs to SPI DVD release 2010 as described in the documentation provided with the SPIs.

b. Reimport the 9.1x content in overwrite mode, enter the following command:

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

c. Manually recreate your OMi 8.10 modifications in the 9.1x content. Refer to the notes taken in "Make a Note of Each Modification to the OMi 8.10 Content Packs" on page 89.

General Configuration Procedures

Perform the following procedures:

- Upgrading Customized Service Health KPIs

  In BSM 9.2x, the internal format of the KPI parameter “KPI is critical if” was changed. As a result, this value may be incorrect following upgrade, if you have created or customized KPIs.

  To fix this, perform the following:

  a. Access the JMX console on the Gateway Server via http://<Gateway Server name>:29000/jmx-console, and enter your user name and password.

  b. Click **service=repositories-manager** in the Topaz section.

  c. Locate the **upgradeCriticalIf()** operation.

  d. Click **Invoke**.

- Service Health and SLM repository post-upgrade procedure

  When you installed BSM 9.1x, content that was imported using out-of-the-box content packs was categorized in the Service Health and SLM repositories as **Custom** or **Predefined (Customized)**, rather than as **Predefined**.

  After you install BSM 9.2x, 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>:29000/jmx-console**, and enter your 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 9.2x, 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 9.2x:

  - **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 9.2x using Baselining

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

  BSM 9.2x 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 9.2x to Work with Baselining" on page 214.

- 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 Etl 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://<FQDN of BSM Gateway server>:29000/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.

- Back up files

  Back up the following files from the BSM 9.1x 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)

- 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.

Pre-Upgrade Tool

The pre-upgrade tool temporarily stores some configuration and certificates in the BSM database to help migrate them to 9.2x. It should be run on all BSM Gateway and the active DPS servers.

1. **Run the Pre-Upgrade Tool on all BSM Gateway servers**

   On all BSM Gateway servers, 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 9.2x 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 9.2x installation.
- Events from your BSM 9.1x environment may be lost.

In this case, you should execute the following steps manually on your BSM 9.2x 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 22: 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. Uninstall BSM via the Windows user interface or silently.
    a. Uninstall BSM Using the Windows user interface:
        i. On the machine from which you are uninstalling HP Business Service Management, select **Start > Control Panel > Programs and Features**. Select **HP Business Service Management**.
        ii. 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).

        iii. 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.
    b. Uninstall BSM silently:
        i. Stop all BSM servers.
        ii. Run the command **<HPBSM Installation Directory>\installation\bin\uninstall.bat -i silent**
2. 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. Stop all BSM servers.

4. Run the following script to uninstall in UI mode: **./uninstall.sh**. To peform this step in silent mode, use the command **./uninstall.sh -i silent**.

5. The BSM uninstall program begins. Follow the on-screen instructions. When the uninstall program is complete, a success message is displayed.

6. Click **Finish**.

7. 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 23: Migrate Database to MS SQL 2012 (optional)

If you would like to use MS SQL 2012, migrate your staging database to a new MS SQL 2012 database. For details, refer to MS SQL documentation.

Chapter 24: Install BSM 9.26

Install BSM 9.26 on one 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.

Note: Do not install more than one set of BSM servers. The upgrade process will use one set of servers to upgrade the database, and you will be directed to install any additional servers towards the end of the upgrade procedure

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.

Go to My software updates (use your HP Passport credentials) and click the BSM 9.26 installation package.

Or

1. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.
2. Click **Search**.
3. For Windows, select **Application Performance Management (BAC) > 9.26> Windows**).

   For Linux, select **Application Performance Management (BAC) > 9.26> Linux**).
4. Under Document Type, select **Patches**.
5. Locate the BSM 9.26 package and save it locally.
6. Launch the relevant setup file to install BSM 9.26.

Alternatively, you can run these wizards in silent mode. For details, see "Installing BSM Silently" on page 180.

For more details, see the following sections:

- "Installing BSM on a Linux Platform" on page 163
- "Installing BSM on a Windows Platform" on page 155

Chapter 25: 9.26 Upgrade Wizard

Run the BSM 9.26 upgrade wizard on the 9.26 BSM servers to transfer your data from the original 8.0x format to the 9.26 format. When this is complete, run the upgrade wizard a second time. The upgrade wizard runs in completion mode and finalizes the upgrade process.

You should only have one set of 9.26 servers installed at this time. Do not run the upgrade wizard on more than one set of 9.26 servers.

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_from80.bat

- Linux:

  /opt/HP/BSM/bin/upgrade_wizard_run_from80.sh

For details about the upgrade wizard, see "Upgrade Wizard" on page 186.

Chapter 26: Staging Mode

The Staging Data Replicator (SDR) takes the data coming into your source environment and copies it to the staging environment. The SDR does not transfer event data.

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 27: Staging Data Replicator

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 BSM 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 file:

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.

In Linux, you can change the installer working directory (default /tmp) by running the following commands:

```
export IATEMPDIR=/new/tmp/dir

export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/directory
```

where `/new/temp` is the new /temp directory.

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 (Standalone)" on page 134.

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 the 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 the 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 139.

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 140.

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 137.

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 138.

Running the Staging Data Replicator (Standalone)

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 137.

2. Run the appropriate replicator file.

   a. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.

   b. Click **Search**.

   c. For Windows, select **Application Performance Management (BAC) > 9.26 > Windows**).

      For Linux, select **Application Performance Management (BAC) > 9.26 > Linux**).

   d. Under Document Type, select **Patches**.

   e. Locate the Staging Data Replicator package and save it locally.

   f. Launch the relevant setup file.

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 any staging Gateway server to the **C:\HPBSMSDR\dat** directory of the standalone SDR server. These directories were created automatically by the Setup and Database Configuration Utility.

   - 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 139.

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 140.

8. Begin running the Staging Data Replicator.

   - Windows: Select **Start > HP BSM Staging Data Replicator > Administration > Enable HP BSM Staging Data Replicator**.

     Verify that the SDR is running by looking for **hpbsmsdr** in the Windows Task Manager.

   - Linux: Run the following command:
     <SDR installation directory>/scripts/run_hpbsmsdr.sh start

     Verify that the SDR is running searching for the hpbsmsdr process (for example: **ps -ef | grep hpbsmsdr**)

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.

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:
      <SDR installation directory>/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 138.

Verifying that the SDR Server Can Communicate with the Production Server

1. Ping the production server.

    a. Ping the production Gateway Server from the SDR server using the Gateway Server's short name. If this works, continue to step 2. If it does not work, continue with step 1 b.

    b. Ping the production Gateway Server from the SDR server using the Gateway Server's fully qualified domain name. If this works, open the relevant **hosts** file for your operating system and add the mapping between the production Gateway Server name and its IP address.

2. Verify connection.

    a. **Production Gateway Server runs Windows:** Run **ipconfig** on the production Gateway Server.

    Production Gateway Server runs Solaris/Linux: Run **ifconfig -a** on the production Gateway Server.

    b. Verify all the listed IP addresses are open to connection to and from the server running the SDR.

    If this is not feasible, contact HP Software Support.

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

Unsubscribing the Staging Data Replicator from the Source Server

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

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

To unsubscribe the SDR:

1. Stop the SDR.
    a. Open the Nanny Manager jmx console from **http://<machine name>:11021**, where **<machine name>** for an embedded SDR is the name of the Load Balancer (if it exists) or destination BSM Gateway Server. For a Standalone SDR, **<machine name>** is **localhost**.
    b. Select **Foundations: type=NannyManager**
    c. Open **showServiceInfoAsHTML**
    d. Stop the **HPBSMSDR-x.x** process.
2. Open the **<Staging Data Replicator root directory>\conf\b2G_translator.xml** file and locate the <Message Selector> element(s).
3. Within the **<Message Selector>** element(s), 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 Manager jmx console from **http://<machine name>:11021**, where **<machine name>** for an embedded SDR is the name of the Load Balancer (if it exists) or destination BSM Gateway Server. For a Standalone SDR, **<machine name>** is **localhost**.
    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. 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\sdreplicator_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 28: Post-Installation Procedures

Perform these tasks to complete the upgrade process:

General Post-Installation Procedures

Perform these tasks to complete the upgrade process:

Note: If you use the IIS web server, stop the **IIS Web Server** service before running the post installation procedure. Do not change the **Startup Type** setting of this service. Do not remove **IIS Web Server** as role.

- ## Disable firewall between BSM Gateway and Data Processing 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 all traffic between all BSM Gateway and DPS servers.

  Additionally, to enable BSM users and data collectors to communicate with the BSM Gateway servers, you must leave open the relevant ports depending on your BSM configuration. The required ports are typically 443 or 80, and 383. For details, see "Port Usage" in the BSM Platform Administration Guide.

- ## Update Data Collectors

  See the System Requirements and Support Matrixes, available from **Help > Planning and Deployment** and the Updated Components section in the HP Business Service Management Release Notes to determine if you must upgrade your data collector to the latest supported version.

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

  Restore the following files to the BSM:

  - <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 and you are upgrading using a staging environment, you need to repeat the hardening procedures described in the BSM Hardening Guide.

  If your original environment was secured with SSL and you are upgrading directly, you need to repeat the following hardening procedures:

  a. If you had previously made changes to **<HP BSM root directory>\EJBContainer\server\mercury\deploy\jboss-web.deployer\server.xml** while performing hardening procedures on your system, repeat the “Securing JBOSS” procedure in the Hardening Guide after the patch installation on all relevant BSM machines.

  b. If you had previously configured SSL on an IIS web server used by BSM, you need to verify HTTPS port binding in IIS is set to the correct port (443).

  c. If you had previously configured SSL on the Apache web server used by BSM, you may need to reapply the changes to httpd.conf and httpd-ssl.conf files as follows:

     - In **<HP BSM root directory>\WebServer\conf\httpd.conf**, uncomment the following two lines:

       LoadModule ssl_module modules/mod_ssl.so

       Include conf/extra/httpd-ssl.conf

     - In **<HP BSM root directory>\WebServer\conf\extra\httpd-ssl.conf**, specify paths to **SSLCertificateFile** and **SSLCertificateKeyFile**

     - Restart the HP BSM Apache web service

- 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.

- 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\<BSM version>** directory.

  In a Linux environment, the logs files are located in the **/tmp/HPOvInstaller/<BSM version>** 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_9.26_2015.10.21_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_BPMPkg_install.log).

- Overwrite custom changes (optional)

  BSM 9.26 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 9.26 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 who value is **predefined (customized)**, this indicates that the artifact was customized and is different from the one delivered with 9.26.

  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 192.

- 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. You can upload them 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" in the BSM Platform Administration Guide.

  Note:

  - The components on the Downloads page are updated for each major and minor release (for example, 9.00 and 9.20). To download updated components for minor minor releases and patches (for example, 9.26), go to the HP Software Support site (https://softwaresupport.hp.com).
  - You can install a component by using the component's setup file directly from the network. 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.

  To install component setup files, 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.

- Enable IPv6 Support (optional)

  BSM by default communicates using IPv4. If your environment uses IPv4 and IPv6, you can choose to use either IPv4 or IPv6, but not both.To enable IPv6, run the following commands on all BSM servers (GW and DPS):

  ovconfchg -ns sec.cm.server -set IsIPV6Enabled TRUE

  ovc -kill

  ovc -start

- **Update the LW-SSO Configuration.**

  You must update the LW-SSO configuration even if you are not using LW-SSO authorization. Be sure to install all patches before performing this step. For instructions, see the BSM 9.26 Build Patch Installation Guide (https://softwaresupport.hpe.com/km/KM02140729).

a. Go to the JMX console – LW-SSO Configuration :

http://<Gateway or Data Processing Server >:29000/mbean?objectname= Topaz%3Aservice%3DLW-SSO+Configuration

where

<Gateway or Data Processing Server name> is the name of the machine on which BSM is running.

b. Search for InitString and copy the value.

c. Access the flat xml file located at:

\HPBSM\conf\settings\SingleSignOn\lwssofmconf.xml.

d. Search for InitString and paste the value you just copied.

e. Go to the JMX console – Infrastructure Settings Manager:

http://<Gateway or Data Processing Server name>:29000/mbean?objectname= Foundations%3Aservice%3DInfrastructure+Settings+Manager

where

<Gateway or Data Processing Server name> is the name of the machine on which BSM is running.

Note: This step must be performed in either Firefox or Chrome.

f. Search for the **setGlobalSettingValue()** method.

g. Enter the following values and invoke the method:

- **contextName:** SingleSignOn
- **settingName:** lw.sso.configuration.xml
- **newValue:** paste the content of the lwssofmconf.xml file

Note: Format the content of the lwssofmconf.xml file on one line.

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 | restart}

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>/mercuryam and http://<server_name>.<domain_name>/topaz

2. Enter the default administrator user ("admin"), and the password specified in the Setup and Database Configuration utility, and click **Log In**. After logging in, the user name appears at the top right.

3. (Recommended) Create additional administrative users to enable BSM administrators to access the system. For details on creating users in the 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.

Adding Additional BSM Servers

After you have a working BSM 9.26 environment, you can add new Gateway and Data Processing servers as desired.

To add new BSM servers to an existing BSM environment:

1. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.
2. Click **Search**.
3. For Windows, select **Application Performance Management (BAC) > 9.26 > Windows**).

   For Linux, select **Application Performance Management (BAC) > 9.26 > Linux**).
4. Under Document Type, select **Patches**.
5. Locate the 9.26 patch and save the package locally.
6. Launch the relevant setup file to install the patch.
7. Run the installation files on all BSM servers (Gateway and Data Processing).
8. 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**. 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**.

   For more details about this utility, see "Server Deployment and Setting Database Parameters" on page 169.
9. Restart all BSM servers.

   After you have installed all additional servers, restart all other BSM servers and data collectors to allow them to recognize the new servers.

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. Update the data collectors to 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. We recommend upgrading each data collector to the latest supported version. For details, see the System Requirements and Support Matrixes, available from **Help > Planning and Deployment**.

2. Restart BPM Agents

   If you have any BPM Agents, you must restart them in order to establish connectivity with the new server.

3. End the SDR and unsubscribe it from the source server. For details, see "Staging Data Replicator" on page 131

4. Exit staging mode

   a. Go to **Admin > Platform > Infrastructure Settings > Foundation – Platform Administration > Platform Administration – HP BSM Evaluation**.

   b. Set **Enable evaluation (staging) mode** to **false**.

   c. Set **Enable evaluation (staging) mode for customer** to **false**.

5. 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 221.

Chapter 29: SiteScope Post-upgrade Procedure

After performing a BSM staging upgrade, you need to configure SiteScope to communicate with the new BSM Gateway Servers. You also need to redirect the HP Operations agent to the Gateway Servers.

1. **Change the Gateway Server to which SiteScope sends data**

   After performing a BSM staging upgrade, you need to configure SiteScope to communicate with the new BSM Gateway Servers. To do so, perform one of the following:

   - In SiteScope's BSM Integration Preferences, enter the new Gateway Server name or IP address in the **Business Service Management machine name/IP address** box. For user interface details, see BSM Integration Preferences Dialog Box in the Using SiteScope Guide in the SiteScope Help.
   - In SAM Administration, update the SiteScope settings with the new Gateway Server name in **Distributed Settings**. For user interface details, see New/Edit SiteScope Page in the BSM Application Administration Guide in the BSM Help.

   Note: This can only be used for changing the Gateway Server for a SiteScope that is already registered with a given BSM installation. It cannot be used to add a new SiteScope, or to connect a SiteScope to a different BSM system.

2. **Redirect SiteScope HP Operations Agent to a different BSM Gateway server**

   You can reconnect the HP Operations agent (which is installed on the SiteScope server) to a different BSM Gateway server by either:

   - Uninstalling and reinstalling the HP Operations agent.
   - Redirecting the HP Operations agent to a different server.

   To uninstall and reinstall the HP Operations agent:

   a. In SiteScope, select **Preferences > Integration Preferences**, and delete the Operations Manager integration.

   b. Uninstall the HP Operations agent from **Start > Settings > Control panel > Add or Remove Programs**, and select the **HP Operations Agent** option.

   c. Reinstall the HP Operations agent from the SiteScope release media DVD (OA 11.14 for 64 bit Windows or OA 11.14 for 64 bit Linux) or from HP Software Support Downloads.

   d. In SiteScope, configure the HP Operations Manager integration with the new BSM server to which you want to connect.

i. Select **Preferences > Integration Preferences** and create a new **HP Operations Manager Integration**, or select an existing integration and click **Edit Integration**.

ii. In the HP Operations Manager Integration dialog box, expand the **HP Operations Manager Integration Main Settings** panel, and enter the following in the **Connection Settings** area:

- **HP Operations Agent installation path**. Path to the HP Operations agent installation on the SiteScope machine.
  - On Windows platforms, the installation path is automatically resolved from the HP Operations agent **InstallDir** key in the registry, and appears in this field. The default path is **C:\Program Files\HP\HP BTO Software**. If the key is not found, the field is left empty, and you must manually enter the agent installation path.
  - On UNIX platforms: SiteScope checks to see if the HP Operations agent is installed in the default **/opt/OV** path. If it is not there, the field is left empty, and you must manually enter the agent installation path.

    Click the **Resolve Path** button to restore the default installation path found by SiteScope if you manually entered a different path.
- **HP Operations Manager/BSM server**. Enter the name or IP address of the BSM server to which you want to connect. If you are connecting to a BSM distributed environment, enter the BSM Gateway Server name or IP address. If your BSM Gateway Servers are behind a load balancer, enter the name or IP address of the load balancer that is configured for data collectors.

iii. Click **Connect** to connect the agent to the BSM server. This sends a connection request from the agent to the specified server.

To redirect the HP Operations agent to a different server:

Note: If you are cloning a machine with an HP Operations agent which usually includes a host name and IP address change, start from a below; otherwise start from d.

a. On the SiteScope server where the HP Operations agent is installed, run the following command to create a new core ID:

```
ovcoreid -create –force
```

b. To remove the certificates, run:

```
ovcert -list
```

For all IDs in the output, run the command:

```
ovcert -remove 'id'
```

c. Adapt the xpl configuration variable OPC_NODENAME by running the command:

```
ovconfchg -ns eaagt -set OPC_NODENAME 'hostname'
```

d. Set the new server host name and core ID by running the commands:

```
ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <new OM server>
ovconfchg -ns sec.core.auth -set MANAGER <new OM server>
ovconfchg -ns sec.core.auth -set MANAGER_ID <new OM server
ovcoreid>
ovconfchg -ns eaagt.lic.mgrs -set general_licmgr <new OM server>
ovcoreid –show
```

> **Tip:** To find the OM server `ovcoreid`, go to the HPOM server (for Operations Management, go to the Data Processing Server) and run the command:
>
> ```
> ovcoreid -show
> ```

If automatic failover has been configured on a BSM distributed environment, you need to change MANAGER_ID on both Data Processing Servers, or assign the same ovcoreid to both Data Processing Servers.

e. Restart the HP Operations agent by running the commands:

```
ovc -kill
ovc –start
```

f. Create a new certificate request by running the command:

```
ovcert –certreq
```

g. Grant a certificate request on the BSM Gateway Server (in case of distributed BSM, grant certificate request on the Data Processing Server).

h. In SiteScope, open the Operations Manager Integration dialog box and perform the following in the **HP Operations Manager Integration Main Settings** panel:

- Change the name or IP address of the BSM server in the **HP Operations Manager / BSM** server box.
- Install the log policies by clicking the **Install Policies** button.

Part III: Appendixes

Appendix A: Installing BSM on a Windows Platform

This appendix contains the following topics:

Preparing 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
  - HP Software Configuration
  - HP Software Deployment
- **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)

- For Microsoft Windows Server 2008 using IIS 7.x Web server, see "Microsoft Windows Server 2008 using IIS 7.x Web Server" below.
- For Microsoft Windows Server 2012 using IIS 8 Web server, see "Microsoft Windows Server 2012 using IIS 8 Web Server" on the next page.

Microsoft Windows Server 2008 using IIS 7.x Web Server

If you are installing on a Microsoft Windows Server 2008 and using the IIS 7.X Web server, 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**.

Microsoft Windows Server 2012 using IIS 8 Web Server

If you are installing on a Microsoft Windows Server 2012 and using the IIS 8 Web server, perform the following procedure:

1. In the **Control Panel**, select **Administrative Tools** > **Server Manager**.
2. Click **Manage** > **Add Roles and Features**.
3. Click **Next**.
4. Select **Role-based or feature-based installation**.
5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Click **Next**.
8. 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.
9. Click **Next** twice.
10. In the Select Role Services panel, select the following roles:
    a. **Common HTTP Features** section:
       - **Static Content** (usually enabled by default)
       - **HTTP Redirection**
    b. **Application Development** section: **ISAPI Extensions** and **ISAPI Filters.**
    c. **Management Tools** section: **IIS Management Scripts and Tools**
11. Click **Next**.
12. Click **Install**.

Installing BSM Servers on a Windows Platform

You install BSM servers—the Gateway Server and Data Processing Server—from 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. If HP Operations Agent is installed on the system and configured to run as non-root user, switch the user under which the agent is running to the user with administrative privileges that is being used to install BSM.

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.

You can also install BSM in silent mode. For details, see "Installing BSM Silently" on page 180.

To install BSM servers:

1. Obtain the installation package.

   Go to My software updates (use your HP Passport credentials) and click the BSM 9.26 installation package.

   or

   a. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.

   b. Click **Search**.

   c. Select **Application Performance Management (BAC) > 9.26 > Windows**).

   d. Under Document Type, select **Patches**.

   e. Locate the BSM 9.26 package and save it locally.

2. From the **Start** menu, select **Run**.

3. Enter the location from which you are installing, followed by HPBsm_9.26_setup.exe. The setup file for BSM servers is located in the **Windows_Setup** directory. For example, enter d:\Windows_Setup\HPBsm_9.26_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.

4. Click **OK**. Setup begins.

5. 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.

     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.

     - 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.

6. 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 Post Install.
   - **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.**

Appendix B: Installing BSM on a Linux Platform

This appendix contains the following topics:

Preparing 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 on a Linux Platform

You can install BSM servers—the Gateway Server and Data Processing Server—from the BSM 9.26 installation 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.

You can also install BSM in silent mode. For details, see "Installing BSM Silently" on page 180.

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.

BSM and HP Operations Agent must always run as the same user. If the host system for the BSM installation is preinstalled with an HP Operations Agent and the HP Operations Agent is configured to run as a non-root user, you must first switch the HP Operations Agent to a root user before calling the BSM installer. At the end of the installation, you can choose if BSM runs as a root user or non-root user. If you choose to run BSM as a non-root user, you must switch the HP Operations Agent to the same non-root user.

To install BSM servers:

1. Log in to the server as user **root**.
2. Obtain the installation package.

   Go to My software updates (use your HP Passport credentials) and click the BSM 9.26 installation package.

   or

   a. Go to the HP Software Support web site (https://softwaresupport.hp.com) and sign in.

   b. Click **Search**.

   c. Select **Application Performance Management (BAC) > 9.26 > Linux**).

   d. Under Document Type, select **Patches**.

   e. Locate the BSM 9.26 package and save it locally.
3. (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.

4. Run the following script:

   ./HPBsm_9.26_setup.bin

5. 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.

6. 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 **<HP BSM root directory>/bin/ovii-postinstall.sh <TOPAZ_HOME>**, where **<TOPAZ_HOME>** is the BSM installation directory (typically /opt/HP/BSM).

Appendix C: Server Deployment and Setting Database Parameters

This appendix contains the following topics:

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. The BSM server on which you are running the utility must be disabled. For details, see "Starting and Stopping BSM" on page 147.

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

Note: Modifying connection parameters for the management, RTSM, RTSM history, 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 the next page and "Required Information for Setting Database Parameters" on page 173.

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 can set connection parameters for the following databases:

- Management
- RTSM
- RTSM History
- Event
- User Engagement Schema

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" on the next page.

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 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 Getting Started 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).

  Note: Database names starting with numbers are not supported.

- **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. Note that a password must be supplied.

  Tip: We recommend not using the default **sa** user for security reasons.

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 192. 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 Managment > Administration > Disable HP Business Service Managment**).
- Use only English characters when entering database parameters.

Note: You can also run this utility in silent mode. For details, see "Installing BSM Silently" on page 180.

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 configuring the databases.
   a. **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.

   b. **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 Getting Started 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.

c. **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 and TransactionVision.

   Note: If you change the **Access to RTSM** password during the BSM installation, you must similarly change the password in Diagnostics, RUM, and TV.

d. **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**.

e. **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.

f. To enable the database connections, you must click **Finish** at the end of the utility.

3. 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 147.

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

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

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

- Copy the contents of the **\loaded** directory into the **\toload** directory. Restart BSM.

Appendix D: Installing BSM Silently

The wizards used to install and configure BSM can be run in silent mode. Silent mode runs the wizards from a command line, without viewing the wizard interface. This allows Linux users without X-windows to run these wizards, however it can be used in windows environments as well.

The instructions have been written for Linux. To run the files for windows environments, replace all .bin file types with .exe and .sh file types with .bat.

Note: Silent mode is not supported for upgrade wizards.

This appendix contains the following topics:

How to Fully Install BSM 9.26 Silently

This procedure describes how to perform a complete installation of BSM silently, including the installation wizard, post-installation wizard, latest minor-minor release, and setup and database configuration utility.

1. Run the BSM 9.26 Installation Wizard silently by running the installation file from the command line with a **-i silent** parameter. The installation file can be found in **<BSM Installation Media>** root folder.

   - To install the Gateway and Data Processing servers on one-machine (typical installation) using the default installation directory, run the following command:

     setup.bin -i silent

   - To install the Gateway and Data Processing Servers on different machines use the following procedure:

     i. Create an empty file called **ovinstallparams.ini** in the same directory as the installation executable file on both servers.

     ii. Copy the following section to the .ini file on the Gateway Server:

     [installer.properties]

     setup=HPBsm

     group=**gateway**

     iii. Run the Installation Wizard in silent mode on the Gateway Server as follows:

     setup.bin -i silent

     iv. Copy the following section to the .ini file on the Data Processing Server:

     [installer.properties]

     setup=HPBsm

     group=**process**

     v. Run the Installation Wizard in silent mode on the Data Processing Server as follows:

     setup.bin -i silent

2. Open the response file in **<BSM Installation Directory>\Temp\emptyRspFile.xml** and complete the values.

3. If you plan to use a non-root BSM configuration, create an appropriate user.
4. Run the post-installation wizard

   silentConfigureBSM.sh <BSM Installation Directory>\temp\emptyRspFile.xml postinstall
5. Log out of and in to Linux (optional). If you are installing BSM in a Linux environment, and you specified a non-root user in the post-installation wizard, log out and log in using the non-root user you selected.
6. Run the Setup and Database Configuration Utility

   silentConfigureBSM.sh <BSM Installation Directory>\temp\emptyRspFile.xml configserver
7. Enable BSM. For details, see "Starting and Stopping BSM" on page 147.
8. Enabling BSM for the first time may take up to an hour. To check the status of BSM, use the following URL:

   http://localhost:11021/invoke?operation=showServiceInfoAsHTML&objectname=Foundations%3Atype%3DNannyManager
9. In BSM, go to **Platform Administration > Setup and Maintenance > Server Deployment** to enable BSM applications.

How to Generate a Response File to Rerun the Post-Installation Wizard and the Setup and Database Configuration Utility Silently

You can create an xml file with the value entries you used when running the Setup and Database Configuration Utility. This file can be used to run the wizard on different machines.

1. Run the Setup and Database Configuration Utility normally on an existing BSM system.
2. The response file is generated and stored in the **<BSM Installation Directory>/temp** directory or in a location you specified. It is automatically filled in with the values you specified when running the Post-Installation Wizard and the Setup and Database Configuration Utility.
3. You can now run the Post-Installation Wizard and the Setup and Database Configuration Utility on any machine silently with the response file using the following syntax:

   silentConfigureBSM.sh <path to response file>/<response file name>.xml

   Note: You can run the two wizards separately by appending the appropriate command as follows:

   silentConfigureBSM.sh <path to response file>/<response file name>.xml [postinstall | configserver]

   The silentConfigureBSM.sh file can be found in the **<BSM Installation Directory>/bin** directory.

How to Configure Windows Authentication When Running the Setup and Database Configuration Utility Silently

The Setup and Database Configuration Utility allows you to configure BSM to take the database schema credentials directly from the windows authentication credentials. To enable this feature when manually creating a response file, leave the UserName and Password keys for each relevant schema blank. The following example shows the Management schema section of the response file formatted to use windows authentication:

```
        <database name="management">
            <!--Enter 'create' to create a new database or 'connect' to connect to
an existing database-->
            <property key="operation" value="connect"/>
            <property key="dbName" value=" "/>
            <property key="hostName" value=""/>
            <property isEncrypted="true" key="password" value=" "/>
            <property key="server" value=" "/>
            <!--'sid' property is  relevant only if you are using an Oracle
database-->
            <property key="sid" value=" "/>
            <property key="UserName" value=" "/>
            <property key="port" value=""/>
            <!--Please enter your Management Database Server Type:'Oracle' or 'SQL
Server'-->
            <property key="dbType" value=" "/>
            <!--The following four items are only relevant if you are using an
Oracle database-->
            <property key="adminUserName" value=" "/>
            <property isEncrypted="true" key="adminPassword" value=" "/>
            <property key="defaultTablespace" value=" "/>
            <property key="temporaryTablespace" value=" "/>
        </database>
```

How to Encrypt Passwords in the Response File

The passwords that are stored in the response file can be encrypted for added security. To do this, run the password encryption tool located in:

<BSM Installation Directory>/bin/encrypt-password.sh

You enter your password and the encryption tool returns a string. Copy the string to the response file where you would have entered your password.

Limitation: encrypted passwords are valid on the machine that ran the encryption tool.

To remove password encryption, enter the passwords in the response file normally and set the value of **IsEncrypted="false"**.

Appendix E: Upgrade Wizard

This appendix provides information about the BSM upgrade wizard and contains the following topics:

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:** upgrade_wizard_run.bat
- **Linux:** upgrade_wizard_run.sh

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

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.

Tracking the BSM 9.1x Configuration Upgrade Progress

The configuration upgrade step of the 9.1x upgrade wizard displays the status of the configuration upgraders as they are executed.

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

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

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

Partially Failed Status

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

Upgrader	Meaning of Partially Failed Status
SampleEnrichmentUpgrade	A partially failed status may happen when an unexpected error occurred in the upgrader while trying to upgrade one of the following entities: • Metrics configuration in profile database • SiteScope monitor CIs in RTSM • Related CIs in RTSM monitored by SiteScope monitors Some possible reasons for failure are: • Database error • CI resolution error • RTSM error • Problems in mapping of measurements to indicators due to missing or corrupted content. When this happens the upgrader will mark the entity as partially failed in the corresponding upgrader log. (i.e sampleEnrich.upgrade.log) If there is at least one entity that was marked as partially failed the final upgrader status will be **Partially Failed**. In this case the user has the option to stop the upgrade or to instruct the wizard to continue. If the user decides to continue with the upgrade it means that **any configuration or data associated with this entity will not be upgraded to the new system**. For example, if a monitor was marked as partially failed and the user decided to continue it means that in the upgraded system this monitor and its related data will not exist - HIs/KPIs will not be assigned to CIs which have failed monitors associated with them.
OprContentUpgrader	At least one content pack failed and at least one succeeded. This could happen if you have customized content. We recommend that you continue with the upgrade. In some cases the SiS Upgrader will fail if a required out-of-the-Box-Contentpack conflicted with a custom content. In this case you will have to resolve the conflict manually and upload the OOTB-Contentpacks manually again.

Upgrader	Meaning of Partially Failed Status
RuleTooltipUpgrader	This happens when you have a Service Health rule that does not have a corresponding tooltip. If you decide to continue it means that the rule will not have a tooltip. A new tooltip can be assigned to the rule in repository 9.1x user interface by editing the rule.
CustomMapViewNameUpgrader	The upgrade updates two tables, one with data regarding the image set to the view, and one with data of CIs set to the image. If only one table upgrade succeeded and the second failed a partially failed status is returned. If you decide to continue it means that the view will not have an image or the view will have an image but with no CIs on the image. A customer can set new image/CIs in the Custom Image user interface in **Admin > Service Health > Custom Image**.
BPM Model and RUM Model Upgraders	A partially failed status in the EUM Admin upgraders may happen when an unexpected error occurred in the upgrader while trying to upgrade one of the following entities: • BPM profile • RUM Application • RUM End User Group • RUM Page • RUM Transaction • RUM event When this happens the upgrader will mark the entity as partially failed in the corresponding upgrader log. In each EUM Admin upgrader, if there is at least one entity that was marked as partially failed the final upgrader status will be **Partially Failed.** In this case, you have the option to stop the upgrade or to instruct the wizard to continue. If you decide to continue with the upgrade, it means that any configuration or data associated with this entity will not be upgraded to the new system. For example, if a profile was marked as partially failed and the user decided to continue it means that in the upgraded system this profile and its related data will not exist. Additionally, any other entity that relates to this profile (E.g. Alerts, SLM, report filters, linked CI, etc) will be detached from this profile or removed completely if it cannot exist by its own.

Appendix F: Changing BSM Service Users

This appendix provides the procedure for how to switch the Windows and Linux users associated with BSM and contains the following topics:

"Switching the Windows User" below

"Switching the Linux User" on the next page

Switching the Windows User

The BSM service, which runs all BSM services and processes, is installed when you run the Setup and Database Configuration utility. By default, this service runs under the local system user. However, you may need to assign a different user to run the service (for example, if you use NTLM authentication).

The user you assign to run the service must have the following permissions:

- Sufficient database permissions (as defined by the database administrator)
- Sufficient network permissions
- Administrator permissions on the local server

Note: When the BSM service is installed, it is installed as a manual service. When you enable BSM for the first time, it becomes an automatic service.

To change the BSM service user:

1. Disable BSM (**Start > Programs > HP Business Service Management > Administration > Disable HP Business Service Management**).
2. In Microsoft's Services window, double-click **HP Business Service Management**. The HP Business Service Management Properties (Local Computer) dialog box opens.
3. Click the **Log On** tab.
4. Select **This account** and browse to choose another user from the list of valid users on the machine.
5. Enter the selected user's Windows password and confirm this password.
6. Click **Apply** to save your settings and **OK** to close the dialog box.
7. Enable BSM (**Start > Programs > HP Business Service Management > Administration > Enable HP Business Service Management**).

Note: This procedure must be repeated if BSM is uninstalled or upgraded.

Switching the Linux User

BSM must be configured to run on linux using a specific user. This user can be either the root or any other user. BSM supports only one user at a time. The user is defined in the post-installation wizard.

To switch the user after BSM is installed:

1. Stop BSM.
2. Rerun the post-installation wizard and specify the new user. The post-installation wizard can be run from the following location: **<HPBSM root directory>\bin\postinstall.bat**.
3. Log out of Linux and log in with the new user.
4. Run the Setup and Database Configuration Utility

   Run the Setup and Database Configuration Utility on the Gateway and Data Processing Servers. You do not have to change any settings. The Setup and Database Configuration Utility can be run from the following location **<HPBSM root directory>\bin\config-server-wizard.bat**.
5. Start BSM.

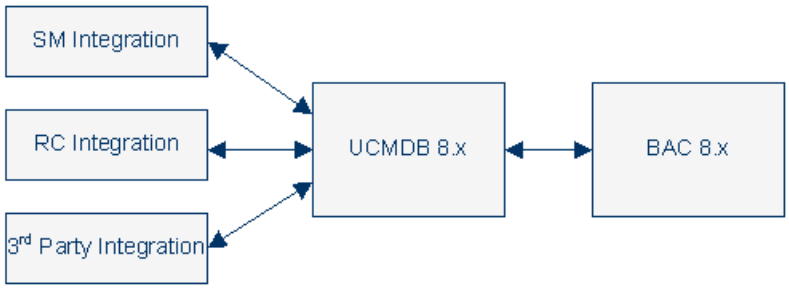
Appendix G: BSM Integrations Upgrade Information

This appendix contains the following topics:

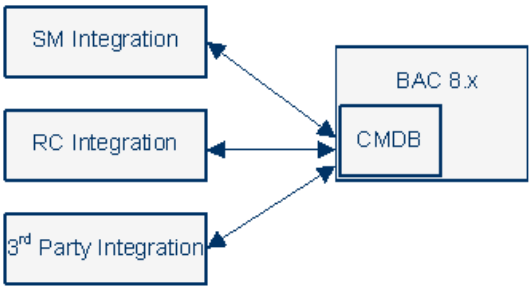
HP Universal CMDB (embedded/external) Upgrade Information

Note: This section is relevant for upgrading integrations in which HP Universal CMDB was being used as a repository for BAC 8.x CI's.

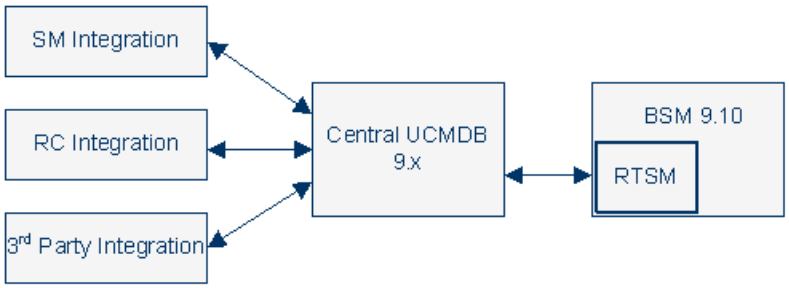
There are a number of different configurations that were possible for integrations between HP Universal CMDB and BAC 8.x. One such configuration was to use an external server for HP Universal CMDB. In this case, you may have configured additional HP and third-party products to integrate with the HP Universal CMDB server, as seen in the example below.



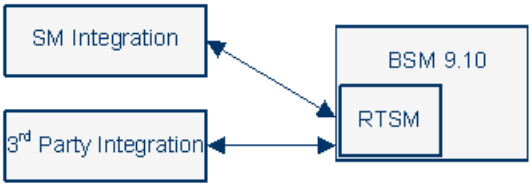
Alternatively, these integrations could also have been configured to communicate directly with the BAC 8.x server via an embedded CMDB.



There are two methods for upgrading HP Universal CMDB and its related integrations. The first method, called **splitting**, involves setting up an external Central UCMDB 9.x server, configuring the HP Universal CMDB integrations to synchronize data with that server, and configuring the Central UCMDB 9.x server to communicate with the embedded RTSM within BSM 9.x.



The second method, called **migrating**, involves reconfiguring any integrations that you had with an external HP Universal CMDB 8.x to communicate with the internal RTSM contained in BSM 9.x. This option is limited in that not every integration can work directly with RTSM (for example Release Control). For more information about RTSM integration recommendations, see the RTSM Best Practices Guide.



Alternatively, if you had an external HP Universal CMDB server with integrations with other products, you can choose to upgrade BSM to 9.x without upgrading HP Universal CMDB or its related integrations. This prevents you from configuring any integrations between BSM and HP Universal CMDB until you upgrade HP Universal CMDB to version 9.x.

RTSM is an embedded version of HP Universal CMDB included in every instance of BSM 9.x. Therefore, if you had an external instance of HP Universal CMDB but did not have any integrations with other products, you no longer need to use an external HP Universal CMDB server. The upgrade will automatically migrate your data from the external server to the embedded RTSM instance.

For more information about working with HP Universal CMDB, see the RTSM Best Practices Guide.

For information about how to upgrade HP Universal CMDB and any integrations associated with it, see "Upgrading HP Universal CMDB Integration - Splitting Procedure" on the next page.

Upgrading HP Universal CMDB Integration - Splitting Procedure

This procedure describes how to migrate UCMDB and its related integrations to integrate with BSM 9.1x by setting up an external Central UCMDB 9.x server. We recommend performing this procedure in two cases:

- If you had integrations between other HP products via HP Universal CMDB
- If your HP Universal CMDB was being used to implement configuration or changes management processes using DDMa, RC, Amber, or other HP or third party products.

For background information about upgrading HP Universal CMDB, see "HP Universal CMDB (embedded/external) Upgrade Information" on page 195.

For more information about working with HP Universal CMDB, see the RTSM Best Practices Guide.

To set up an external Central UCMDB:

1. **Perform this step only if you are performing a direct BSM upgrade and you did not have an exernal instance of CMDB in BAC 8.x.** Begin the BSM 9.1x direct upgrade procedure, but immediately before uninstalling BAC 8.x, stop all connections and integrations into HP Universal CMDB. Continue with the upgrade process of removing BAC 8.x and upgrading to BSM 9.1x.
2. Install new instance of HP Universal CMDB 9.x.
3. If you need to preserve other configurations from the original CMDB, create a custom package, export it, and deploy it in the external CMS. For details, see "Package Manager" in the RTSM Administration Guide. Note that deploying custom packages can overwrite critical class model elements in the CMS environment. Therefore, you should only add modified or user type elements and should not add out of the box or factory type elements.
4. If you need to preserve credentials and IP ranges from the original CMDB, you can export them from the Data Flow Management under RTSM and then import them into the external CMS. For details see "How to Export and Import Credential and Range" in the RTSM Data Flow Management Guide.
5. If you need to preserve the original CMDB IDs of items in the central UCMDB server, perform a one-time synchronization between the central UCMDB server and RTSM. This synchronization is activated from RTSM.

   This synchronization only transfers data. If there are resources such as views, tqls or enrichments that you want to migrate to the new server, it needs to be exported from RTSM and imported to the central UCMDB manually.

After the synchronization, Central UCMDB will have the synchronized CIs with the original CMDB IDs. The Global IDs in the Central UCMDB will be equal to the internal CMDB IDs.

For information about how to perform this procedure, see "How to Perform Initial Synchronization" in the RTSM Data Flow Management Guide.

Note: At this point all configurations and CIs that existed on the external UCMDB are part of RTSM in the upgraded BSM system.

6. Move the integrated products from the original server to the Central UCMDB 9.x server.

7. If you want to continue synchronizing data between the Central UCMDB and RTSM database embedded in the BSM 9.1x server, set up an ongoing synchronization. Choosing not to synchronize these databases may prevent some integrations from working. For information about how to perform this procedure, see "How to Set Up Integrations between CMS and BSM" in the RTSM Data Flow Management Guide.

   - If you had an integration between BSM and Service Manager relating to alerts, make sure that CIs that are part of this integration are included in on-going synchronization.

   - If you were integrating Service Manager planned changes and incidents with BSM Service Health, this step is not optional. The integration will not work unless there is an ongoing sync and a delegation of federation is configured. For more details, see "How to Set Up Integrations between CMS and BSM" in RTSM Data Flow Management Guide.

   - You can view BSM KPI's in an external applications by setting up an adapter. If you configured this type of adapter in BAC 8.x, and you have configured a delegation of federation as part of the ongoing topology synchronization between Central CMDB and BSM, the KPI federation adapter must be deployed on the central UCMDB and not on the RTSM. You must manually move this adapter. For details, see below.

To manually move the adapter used to view KPIs from RTSM to the Central UCMDB server:

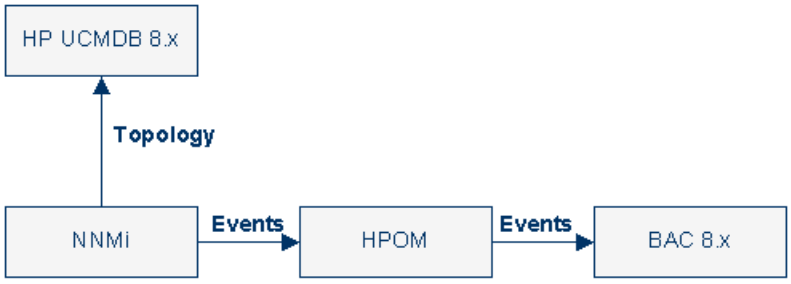
1. Deploy the following package on the central UCMDB server:

   HPBSM\odb\conf\factory_packages\BACKPIsAdapter.zip

2. Perform the configurations described in "Set Up an Adapter to View KPIs in an External Application" in the RTSM Developer Reference Guide.

NNMi Upgrade Information

In BAC 8.x, NNMi had the ability to integrate topology information with CMDB, and events with BAC via HPOM and the OMi application as follows:



NNMi 8.x can continue to function with BSM 9.1x without any changes to configuration or functionality. There is a recommended modification that you can perform if you decided to upgrade to NNMi 9.x and you are synchronizing BSM 9.x with HP UCMDB 9.x. In this case, NNMi can integrate both topology and events directly with BSM 9.10 as seen below. Should you choose to perform this modification, it should be done after the BSM 9.1x upgrade is complete.

Migrating Modified UCMDB Integration (Federation) Adapters

Out-of-the-box adapters: All adapters must be compatible with the new BDM model. If you made changes to existing out-of-the-box adapters, you must make the same changes to the adapter files in the new BSM version. That is, do not copy files from version 8.0x and overwrite the files in the new version. Back up the modified adapters before starting the upgrade process and copy the changes once the upgrade is complete.

Custom adapters: Back up the custom adapters before starting the upgrade process and redeploy them in BSM 9.1x. For details, see "Package Manager" in the RTSM Administration Guide.

Upgrade of the Integration of HP Operations Orchestration

The table describes what changed between BAC 8.x and BSM 9.x.

Topics	BAC 8.x	BSM 9.x
Run books assigned to CIs	Run books assigned to CIs	Run books assigned to CIs: The upgrader automatically handles the following changes due to the topology changes in the RTSM: • CI Types. For example, Host CI is changed into Node CI. • CI attributes. • The mapping of CI types to runbooks in **Admin > Integrations > Operations Orchestration**.
BAC-OO integration (not automatically upgraded)	BAC-OO integration	BSM-OO integration **TO DO:** After the upgrader has run, you must perform the BSM-OO integration. For details on how to reconfigure OO, see the BSM-Operations Orchestration Integration Guide.

Upgrade EMS Integrations

The Show Events context menu that opens a console or event log listing the events relevant to the integration and allows you to delete events is not upgraded.

RTSM Upgrade Limitations

- When upgrading from version 8.0x to version 9.1x, the Data Flow Probe fails to update the server with job results if the Probe's IP address changes (and its identifier remains the same).
- When upgrading from version 9.0x to version 9.1x, if you have a larger History database, the first server startup may take some time to complete. Do not interrupt the server startup process until you have confirmed that the server is up and running.
- LDAP server settings are not upgraded during the upgrade process. You must manually reconfigure the LDAP connection configuration after upgrading to 9.1x (user mappings are upgraded).

How to Establish a Trust Relationship for a Server Connection

For connection and communication between BSM and external servers such as HPOM hosts, other BSM hosts where Operations Management is running, or a BSM Server with an event channel license, you must establish a trust relationship between the systems.

In HPOM Server Pooling, the virtual server must have a certificate which is trusted by all HPOM hosts in the server pool and by all BSM hosts where Operations Management is running.

The trust relationship between Gateway Servers and Data Processing Servers is part of the initial installation and is described in the BSM Installation Guide.

Note: Generally, the trust relationship must be set up on all nodes (Data Processing Servers, Gateway Servers, manager of manager configurations, load balancers, and reverse proxies). However, some load balancer technologies include a by-pass or pass-through functionality for incoming encrypted messages to its pool members. When using such technologies, trust relationship on the load balancer node is not required, if you are load balancing on the recommended OSI level 2 or 4.

To establish a trust relationship between the Data Processing Servers and external servers:

1. *HPOM servers only:*

   Note:

   HPOM for Windows: Starting with patches OMW_00121 (32-bit) and OMW_00122 (64-bit), the **BBCTrustServer** tool is already installed to the folder **%OvInstallDir%\contrib\OVOW** on the HPOM for Windows management server.

   HPOM for UNIX: Starting with patches Patch PHSS_42736 (HP-UX), OML_00050 (Linux), and ITOSOL_00772 (Solaris), the **BBCTrustServer** tool is already installed to the directory **/opt/OV/bin** on the HPOM for UNIX or Linux management server.

   If you have the appropriate patch installed, you can skip this step.

   a. Locate the following files on the BSM Data Processing Server:

      <HPBSM root directory>/opr/lib/cli/opr-cli.jar

      <HPBSM root directory>/opr/bin/BBCTrustServer.bat

      <HPBSM root directory>/opr/bin/BBCTrustServer.sh

   b. *HPOM for Windows only:* Copy the files to the computer that is running the HPOM for

Windows management server.

Copy **opr-cli.jar** to **%OvInstallDir%\java\opr-cli.jar**.

Copy **BBCTrustServer.bat** to **%OvBinDir%\BBCTrustServer.bat**.

c. *HPOM for UNIX or Linux only:* Copy the files to the computer that is running the HPOM for UNIX or Linux management server.

Copy **opr-cli.jar** to **/opt/OV/java/opr-cli.jar**.

Copy **BBCTrustServer.sh** to **/opt/OV/bin/BBCTrustServer.sh**.

Change the permissions of the **BBCTrustServer** tool by entering the following command:

chmod 555 /opt/OV/bin/BBCTrustServer.sh

2. If you are using a load balancer, where your data sources are not communicating directly with the BSM Gateway Servers, make sure that Port 383 is routed through the load balancer to the BSM Gateway Servers.

Only if the load balancer is configured to be the endpoint for secure communication (which is not recommended), then the following prerequisites must also met and perform the following steps.

- The certificate on the load balancer must be installed for port 383 (or the port that you have configured for secure communication).
- Communication between the load balancer and the gateway systems must be secured.
- The load balancer must possess a server certificate for authentication so that external servers such as HPOM can connect successfully. The load balancer must also validate client certificates presented by external clients (for example, HPOM management servers).
- The load balancer must possess a client certificate for authentication with BSM.

a. Issue a certificate for the load balancer from the BSM Data Processing server with the following command:

ovcm -issue -file <*certificate file*> -name <*Fully Qualified Domain Name of Virtual Interface*> [-pass <*passphrase*>]

b. Import these certificates to the load balancer.

3. On the BSM Data Processing Server, execute the following command:

BBCTrustServer[.bat|sh] <*external_server*>

Replace **<*external_server*>** with the DNS name of the external system (for example, `ommgmtsv`).

> **Note:** The value of *<external_server>* should be the virtual name in case of HPOM server pooling.

When asked whether to add the certificate to the trust store, enter: **y**.

The tool informs you if a trusted certificate already exists and asks you whether to overwrite the existing certificate. To replace the existing certificate with the new one, enter: **y**.

4. On the external system, execute the following command:

   BBCTrustServer.[bat|sh] <*load_balancer_or_single_gateway_server_or_RP_or_Server_Pool_Virtual_Interface*>

   When asked whether to add the certificate to the trust store, enter: **y**.

   The tool informs you if a trusted certificate already exists and asks you whether to overwrite the existing certificate. To replace the existing certificate with the new one, enter: **y**.

5. Update new trusts on the Gateway Servers, with the command:

   ovcert -updatetrusted

   > **Note:** During deployment, certificates for Gateway Servers are requested and granted for each Gateway Server. For details, see the BSM Installation Guide.

6. Check the connection between the servers.

How to Run Dynamic Topology Synchronization

Before configuring forwarding of topology (node and service) data to Operations Management from Operations Manager management servers, complete the following configuration steps in Operations Management:

- Add the Operations Manager management server as a connected server in Operations Management. For details, see How to Create a Connection to an HPOM Server in the BSM - Operations Manager Integration Guide.
- Establish a trust relationship between the Data Processing Server and the Operations Manager management server. For details, see How to Establish a Trust Relationship for a Server Connection in the BSM - Operations Manager Integration Guide.
- *Optional:* Use the `opr-sdtool.bat` command-line tool to upload new or changed synchronization packages from the file system to the database. For details, see the Operations Manager i section of the *Extensibility Guide*.

After ensuring that the Operations Manager management server is added in Operations Management as a connected server, configure the forwarding of topology (node and service) data on the Operations Manager management server as described in the following section.

The following sections describe how to configure topology synchronization:

- "How to Configure Dynamic Topology Synchronization on HPOM for Windows Systems" below
- "How to Migrate from Scheduled Synchronization on HPOM for Windows Systems" on the next page
- "How to Configure Dynamic Topology Synchronization on HPOM for UNIX or Linux Systems" on page 210
- "How to Migrate from Scheduled Synchronization on HPOM for UNIX or Linux Systems" on page 211

How to Configure Dynamic Topology Synchronization on HPOM for Windows Systems

This section describes how to configure dynamic topology synchronization on HPOM for Windows management servers. For further details, see the HPOM for Windows documentation.

To forward topology data to Operations Management, complete the following steps on the Operations Manager for Windows management server from which you want to receive topology information:

1. *Prerequisite:* Make sure that the minimum patch level for the HPOM for Windows management server is installed:

- Version 8.16: Patch OMW_00121 or superseding patch.
- Version 9.00: Patch OMW_00122 or superseding patch.

2. *Prerequisite:* Configure trusted certificates for multiple servers.

   In an environment with multiple servers, you must configure each server to trust certificates that the other servers issued.

3. In the console tree, right-click **Operations Manager**, and then click **Configure > Server...**. The Server Configuration dialog box opens.
4. Click **Namespaces**, and then click **Discovery Server**. A list of values appears.
5. Add the hostname of the server 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
   ```

6. Make sure that the value of **Enable discovery WMI listener** is true. This is the default value.
7. Click **OK** to save your changes and close the Server Configuration dialog box.
8. Restart the `OvAutoDiscovery Server` process for your changes to take effect.
9. Start the initial synchronization of topology data:
   a. In the console tree, select **Tools > HP Operations Manager Tools**.
   b. 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.

How to Migrate from Scheduled Synchronization on HPOM for Windows Systems

This section describes how to migrate from scheduled synchronization on HPOM for Windows management servers. For further details, see the HPOM for Windows documentation.

To migrate from scheduled synchronization, complete the following steps on the Operations Manager for Windows management server from which you want to receive topology information:

1. *Prerequisite:* Make sure that the minimum patch level for the HPOM for Windows management server is installed:
   - Version 8.16: Patch OMW_00121 or superseding patch.
   - Version 9.00: Patch OMW_00122 or superseding patch.
2. Clear the agent repository cache on the HPOM management server using the following command:

   ```
   %OvBinDir%\ovagtrep -clearall
   ```
3. Remove the service auto-discovery policies from the HPOM management server node, type:

   ```
   %OvBinDir%\ovpolicy -remove DiscoverOM

   %OvBinDir%\ovpolicy -remove DiscoverOMTypes
   ```
4. Synchronize the policy inventory on the HPOM management server:
   a. In the console tree, right-click the management server.
   b. Select **All Tasks > Synchronize inventory > Policies**.

      The management server creates a deployment job to retrieve the inventory from the local agent.
5. Make sure the listener process is running:
   a. In the console tree, right-click **Operations Manager**, and select **Configure Server.**

      The Server Configuration dialog box opens.
   b. Click **Namespaces**, and select **Discovery Server**.

      A list of values appears.
   c. Set the value of **Enable discovery WMI listener** to true. This is the default value.
   d. Click **OK** to save your changes and close the Server Configuration dialog box.
   e. Restart the OvAutoDiscovery Server process for your changes to take effect using the following commands:

      ```
      net stop "OvAutoDiscovery Server"

      net start "OvAutoDiscovery Server"
      ```
6. Start the initial synchronization of topology data:

a. In the console tree, select **Tools > HP Operations Manager Tools**.

b. 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 servers.

How to Configure Dynamic Topology Synchronization on HPOM for UNIX or Linux Systems

This section describes how to configure dynamic topology synchronization on HPOM for UNIX or Linux management servers. For further details, see the HPOM for UNIX or Linux documentation.

To forward topology data to Operations Management, complete the following steps on the Operations Manager for UNIX or Linux management server from which you want to receive topology information:

1. *Prerequisite:* Make sure that the minimum patch level for the HPOM 9.10 for UNIX or Linux management server is installed:
   - HP-UX: Patch PHSS_42736 or superseding patch.
   - Linux: Patch OML_00050 or superseding patch.
   - Solaris: Patch ITOSOL_00772 or superseding patch.
2. *Prerequisite:* Make sure that the HP Operations Agent version on the HPOM for UNIX or Linux management server is 8.60.500 or higher. (Older agents require the agent hotfix QCCR1A100254 and agtrep must be configured to send complete instance data.)
3. *Prerequisite:* Configure trusted certificates for multiple servers.

   In an environment with multiple servers, you must configure each server to trust certificates that the other servers issued.
4. 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.

   This command restarts the service discovery server. The source management server begins to send any topology data changes immediately.
5. Type the following command to start the initial synchronization of topology data:

   ```
   /opt/OV/bin/OpC/startInitialSync.sh
   ```

How to Migrate from Scheduled Synchronization on HPOM for UNIX or Linux Systems

This section describes how to migrate from scheduled synchronization on HPOM for UNIX or Linux management servers. For further details, see the HPOM for UNIX or Linux documentation.

To migrate from scheduled synchronization, complete the following steps on the Operations Manager for UNIX or Linux management server from which you want to receive topology information:

1. *Prerequisite:* Make sure that the minimum patch level for the HPOM for Windows management server is installed:
   - HP-UX: Patch PHSS_42736 or superseding patch.
   - Linux: Patch OML_00050 or superseding patch.
   - Solaris: Patch ITOSOL_00772 or superseding patch.
2. Clear the agent repository cache on the management server using the following command:

   ```
   /opt/OV/bin/ovagtrep -clearall
   ```
3. Remove the service auto-discovery policies from the management server node using the following command:

   ```
   /opt/OV/bin/ovpolicy -remove DiscoverOM

   /opt/OV/bin/ovpolicy -remove DiscoverOMTypes
   ```
4. Deassign the service auto-discovery policies from the management server node using the following command:

   ```
   /opt/OV/bin/OpC/utils/opcnode -deassign_pol node_name=<management_server> net_
   type=NETWORK_IP pol_name=DiscoverOMTypes
   pol_type=svcdisc

   /opt/OV/bin/OpC/utils/opcnode -deassign_pol node_name=<management_server> net_
   type=NETWORK_IP pol_name=DiscoverOM
   pol_type=svcdisc

   /opt/OV/bin/OpC/opcragt -dist <management_server>
   ```

   Replace <*management_server*> with the name of the management server.
5. Type the following command to enable topology synchronization:

   ```
   /opt/OV/contrib/OpC/enableToposync.sh -online
   ```

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

6. Type the following command to start the initial synchronization of topology data:

   ```
   /opt/OV/bin/OpC/startInitialSync.sh
   ```

Appendix H: Custom Rules

- **Custom Java rules.** If you created custom Java rules and compiled them to create a new .jar file in pre-9.0 versions of BAC (now BSM), contact HP Professional Services for instructions on modifying and packaging them for BSM 9.x **before** upgrading.

  Note that this does not relate to custom rules in the repositories; it is only relevant if you have custom java rule source files.

  > **Note:** To compile and build custom .jars, you must have JDK (Java Development Kit) 6 installed. This can be downloaded from http://www.oracle.com.

- **Custom classpath for calculation rules infrastructure setting.** If you created custom rule .jar files and used the **Custom classpath for calculation rules** infrastructure setting to define them in pre-9.0 BAC, contact HP Professional Services for assistance **before** you upgrade.

- **Text file-based API Rules.** If you created text file-based custom rules using the Rules API, and saved your rules in **<Data Processing Server root directory>\BLE\rules\groovy\rules**, copy your rules to the same location in your 9.x environment, **before** upgrading.

  In addition, edit the text files as follows:

  - Replace lines starting with
    import com.**mercury.am.**platform.processing.ble.calculation with
    import com.**hp.bsm.**platform.ble.calculation.

  - Replace lines starting with
    import com.**mercury.am.**platform.processing.ble.rulesfwk with
    import com.**hp.am.**platform.processing.ble.rulesfwk.

  - Replace lines starting with
    import com.**mercury.am.**platform.processing.ble.groovy.rulefwk with
    import com.**hp.am.**platform.processing.ble.groovy.rulefwk.

  - Replace usage of **RuleTrinityModelAccess** with **RuleBLEModelAccess**.

Appendix I: Upgrading SLAs from BSM 9.x to 9.2x to Work with Baselining

BSM 9.20 introduced 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 9.2x 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.

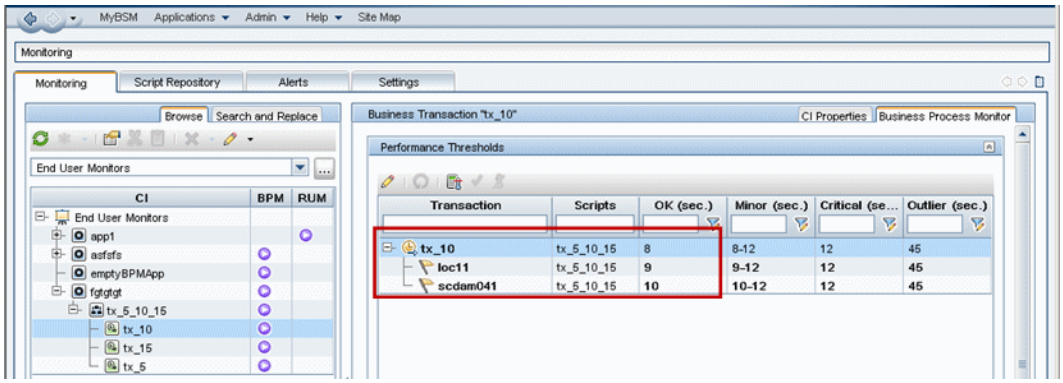
In this procedure you will clone your original SLA (before enabling baselining) to save calculation results; change rules on the cloned SLA to rules that are not influenced by baselining; stop the original SLA; and then configure baselining without it influencing SLA calculation.

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

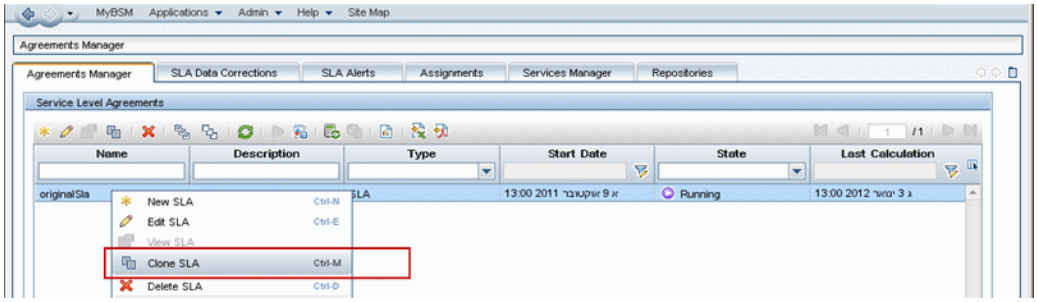
- "To update SLAs with different thresholds in each location:" below.
- "To update SLAs with the same thresholds in each location:" on page 218.

To update SLAs with different thresholds in each location:

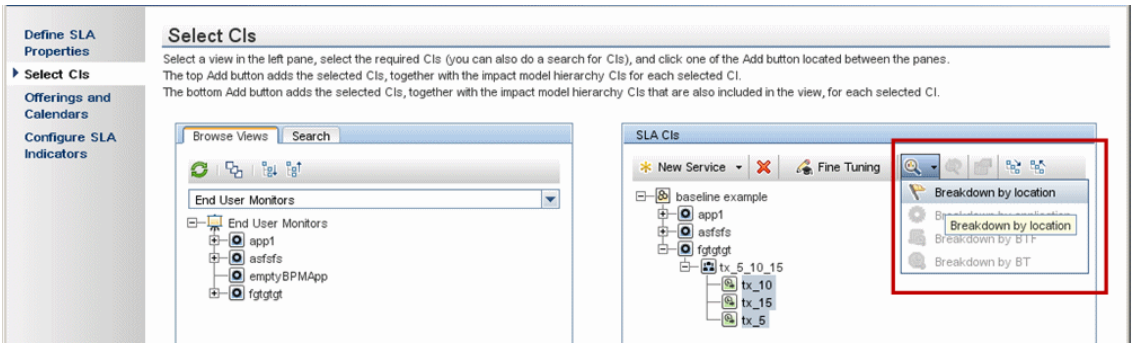
If you have different thresholds for a transaction in each BPM location perform the following procedure:



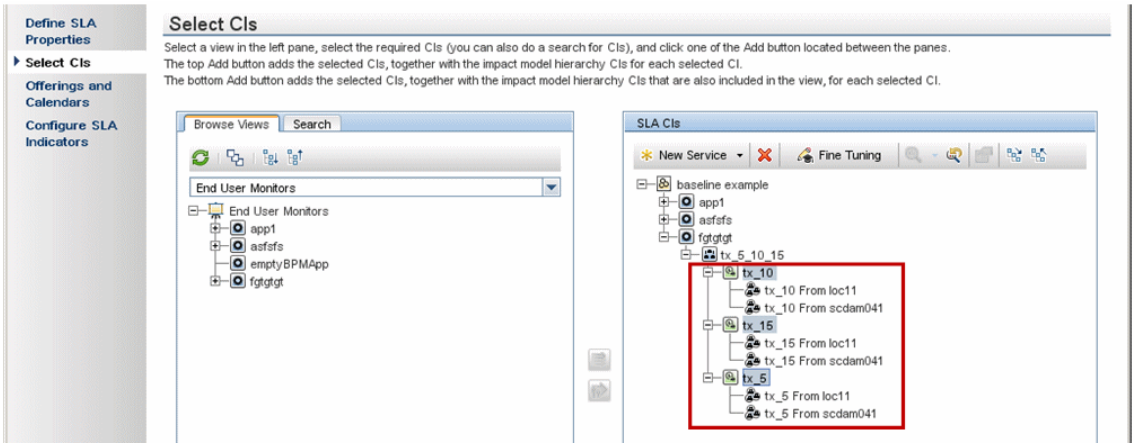
1. Within **Admin > Service Level Management**, clone your SLA; this saves your original SLA with its old calculation results.



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.



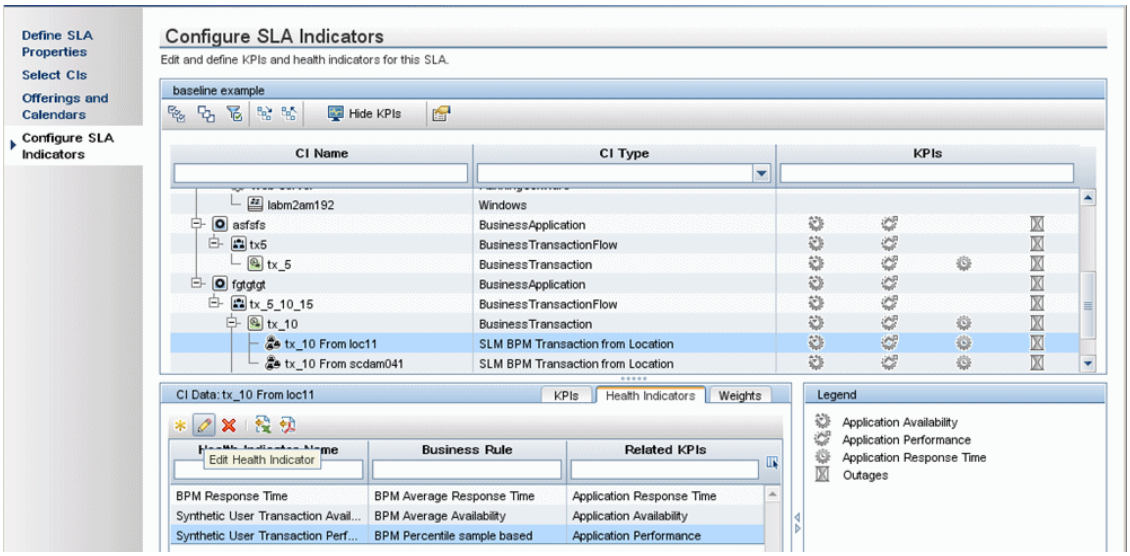
The result is as follows:

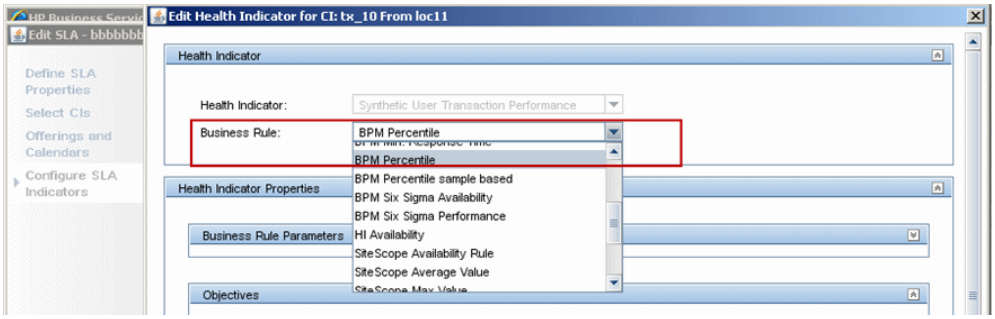


Note: If a new location was added to the application inside the SLA, to add the location to the breakdown you must disable the breakdown for the selected transaction using the **Undo Breakdown** button, and then enable it again.

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.

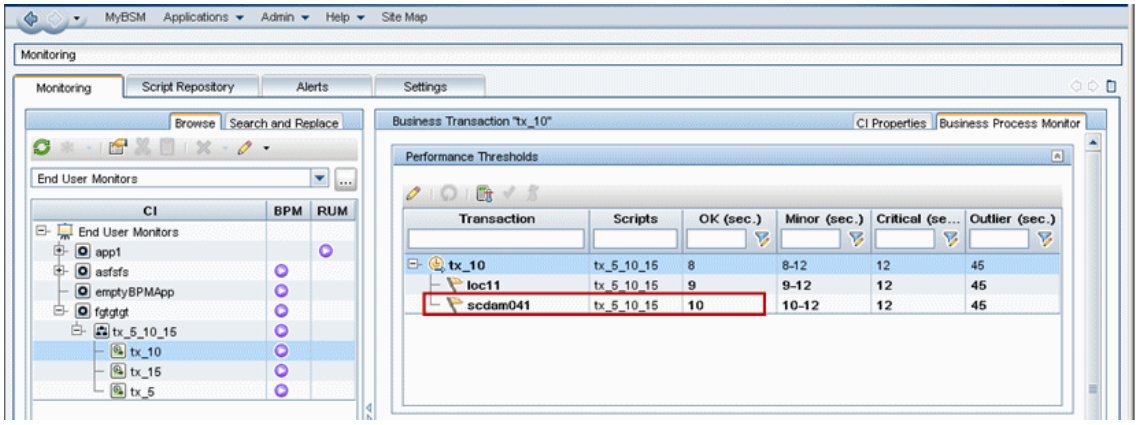
For details on these rules, refer to the list of SLM calculation rules in the the BSM Application Administration Guide.

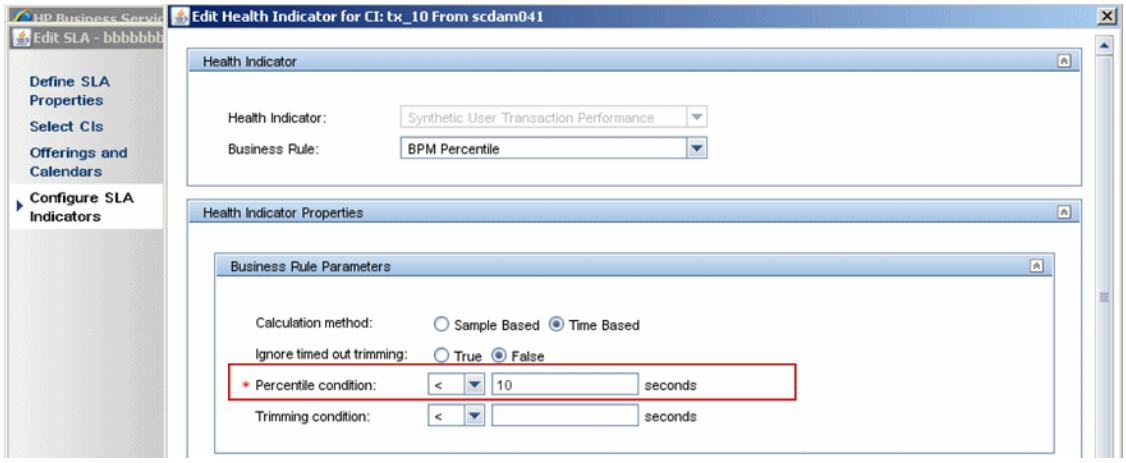




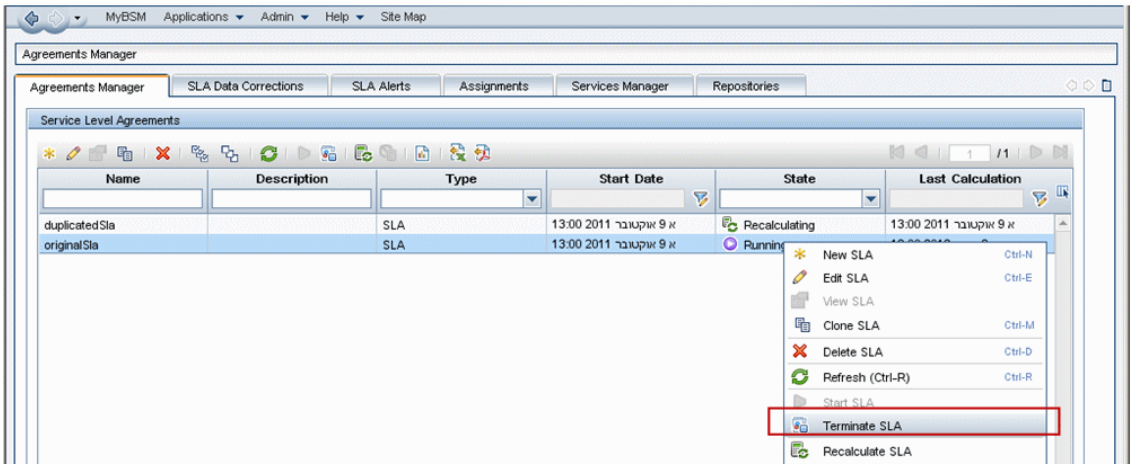
4. For each of the transaction from location CIs whose rule you changed, copy the OK performance threshold defined for the CI in EUM Admin, and use it to define the Percentile Condition rule parameter.

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





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

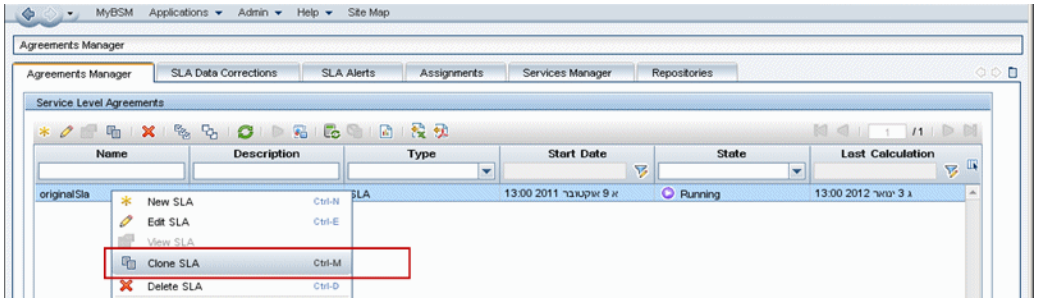


You can now configure baselining without influencing the SLA's calculation.

To update SLAs with the same thresholds in each location:

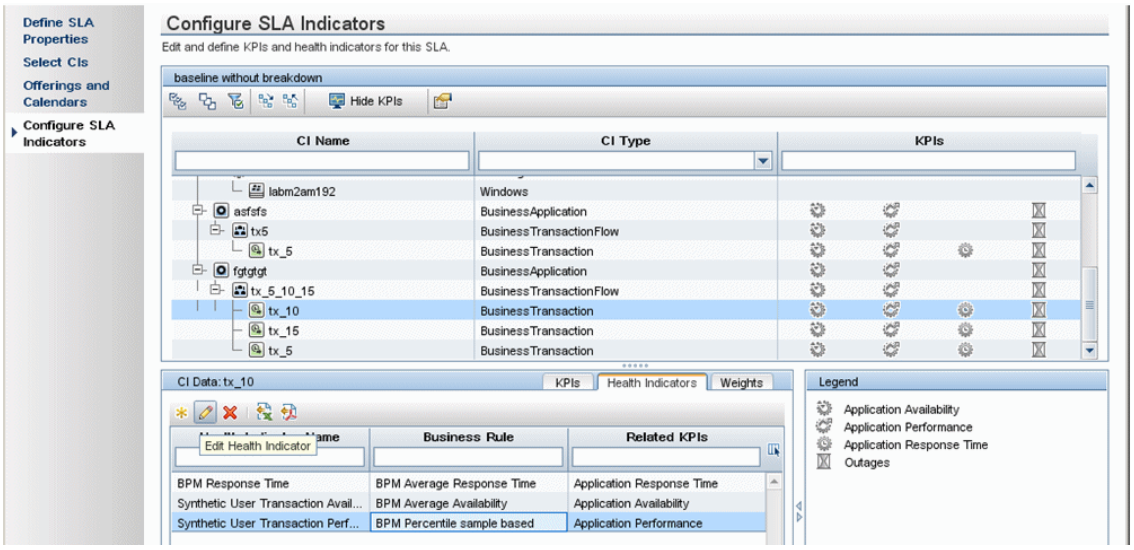
If you have the same threshold for all locations, perform the following procedure:

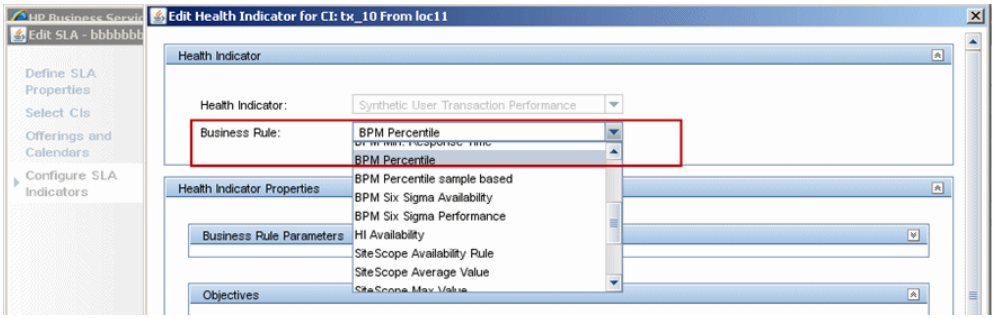
1. Within **Admin > Service Level Management**, clone your SLA; this saves your original SLA with its old calculation results.



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.

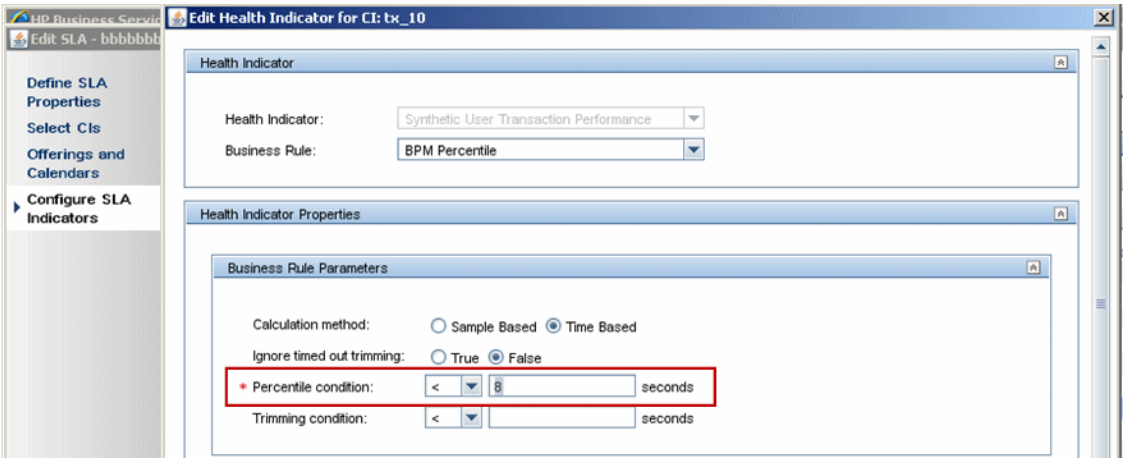
For details on these rules, refer to the list of SLM calculation rules in the the BSM Application Administration Guide.



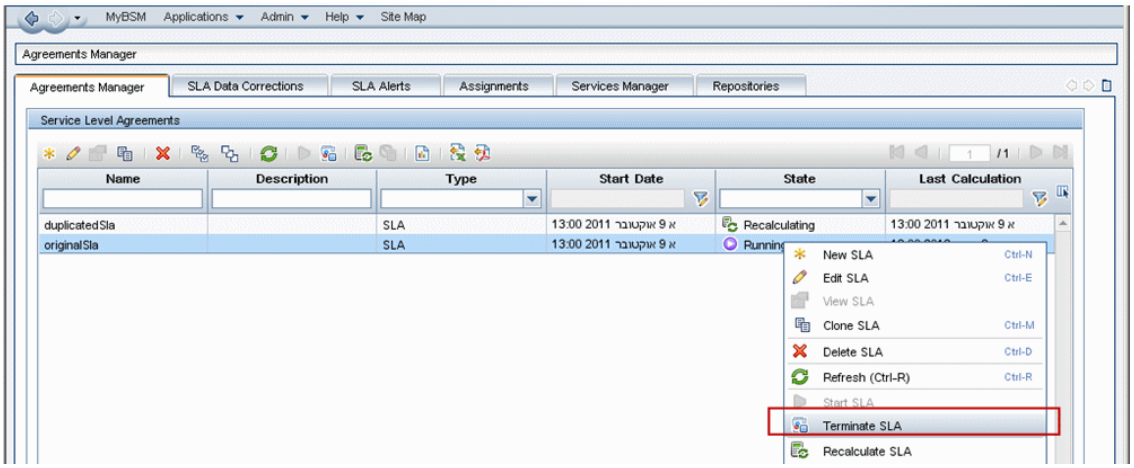


3. For each of the transaction CIs whose rule you changed, copy the OK performance threshold defined for the CI in EUM Admin, and use it to define the Percentile Condition rule parameter.

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.

Appendix J: Troubleshooting

This appendix contains the following topics:

Troubleshooting Resources

- **Installation log files.** For details, see "Check installation log files" on page 144.
- **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 **<HPBSM 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 accessed from the HP Software Support (https://softwaresupport.hp.com).
- **BSM Tools.** You can use BSM tools to assist in troubleshooting the HP Business Service Management environment. You access the tools from **<HPBSM 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.

Unable to access BSM using Internet Explorer with an FQDN that has a two letter domain

Internet Explorer does not support FQDNs with two letters domains for the BSM default virtual URL (for example XXXX.aa).

Workaround:

If FQDN has a two letter domain, use another browser (not Internet Explorer) to access BSM.

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.

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.
  - **Windows:** Select **Start > Settings > Control Panel > System > Advanced tab > Environment Variables**, and edit the path for the **TEMP** variable in the User variables area.
  - **Linux:** Run the following commands:

    ```
    export IATEMPDIR=/new/tmp
    export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp
    ```

    where `/new/tmp` is the new working directory.

Installation fails due to security restrictions of the /tmp directory on Linux

If the /tmp directory has security restrictions that prevent script execution from it, the installation will fail.

Solution:

Set a new /tmp directory not affected by these restrictions, by running the following commands:

```
export IATEMPDIR=/new/tmp
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp
```

where `/new/tmp` is the new working directory.

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 29000 (http://MACHINE _NAME:29000).

   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 158.
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. (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/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 **<HPBSM 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 system. Disable UAC on all BSM servers running Windows.

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**).

Uninstalling BSM results in errors

If you receive a few errors that look like the following:

The package HPOv….can not be uninstalled.

You can ignore these errors. BSM has been uninstalled correctly.

Unreadable Eastern Asian Characters

On some RHEL6.x distributions, when choosing to install BSM in an Eastern Asian locale (Korean, Japanese or Simplified Chinese), the installation UI displays unreadable characters.

Workaround:

Launch the installer with a JRE that supports Eastern Asian Languages.

setup.bin LAX_VM ${PATH_TO_JAVA}

Server is not ready message

If you see the following, it is an indication that JBoss is not starting.

- The status page returns the “Server is not ready” message.
- Processes are not loading.
- The wrapper.log file from the <HPBSM>\log\supervisor folder contains this error: “Error: Password file read access must be restricted: c:\HPBSM/JRE64/lib/management/jmxremote.password”

Workaround:

1. Disable BSM.
2. Navigate to **<HPBSM>\JRE64\lib\management**.
3. Right-click **jmxremote.password** and select **Properties**.
4. Click the **Security** tab..
5. Click **Edit**.
6. Click **Add** and add the **Administrators** group.
7. Allow **Read** and **Write** permissions for the Administrators group.
8. Enable BSM.

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 upgrade Framework.log for the cause of the error. In most cases, restarting the upgrade wizard resolves the problem.
- RUM Engine permissions may be reset during the BSM upgrade. Therefore, it is recommend to ensure that the RUM Engine View permission is selected after upgrading BSM.

  a. In BSM, click **Admin > Platform**.

  b. Click the **Users and Permissions** tab.

  c. Click **User Management**.

  d. In the tree, select an EUM context and click the **Permissions** tab.

  e. Select the RUM Engine instance(s) and click the **Operations** tab.

  f. Enable the **View** option if it is not already selected and if it is not inherited or granted from Group/Roles/Parent.

JBoss does not start when there are two enabled NICs

Description: JBoss does not start when there are two enabled NICs.

Workaround: There is a known issue with JBoss 7 (used by BSM 9.26) when there are multiple NICs (LANs) on the box. To resolve this problem, install the following hotfix on top of BSM 9.26 IP1 **https://patch-central.corp.hpecorp.net/crypt-web/protected/viewContent.do?patchId=QCCR1I118920_HOTFIX**.

Cannot log in to LDAP after upgrade

Description: The upgrade process could not reuse an LDAP configuration created before BSM version 9.25. Therefore, newly created users are not able to log in to LDAP. This is because support for multiple LDAPs was added in BSM version 9.25.

Workaround: After upgrading from BSM version 9.24 or earlier to version 9.25 or later, reconfigure LDAP.

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**.
- If there are no connections, and the schema upgrade step fails or gets stuck, you can skip this validation step. In the file **C:\HPBSM\dbverify\conf\UFupgrade_tasks.xml**, remove or comment out the line **com.mercury.dbverify.tasks.ConnectionTask**.

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 29000, 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 **<HPBSM 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\sdreplicator\sdreplicator.properties**. Modify the **loglevel** to **debug**.

2. Open **<BSM Directory>\>\conf\core\Tools\log4j\sdreplicator\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 **sdreplicator.properties** and **wde.properties** files.

Data Transfer Tool

- Verify that the SDR is working before running the Data Transfer Tool; you can check the SDR log to see that the SDR is working. If you ran the Data Transfer Tool and the SDR did not run, a message will appear when you click Next (SDR initiation Date warning).

- If you exit the wizard (or the wizard crashes) during the data transfer tool sequence of steps, re-run the tool on the same dates it ran earlier (see upgrade_all.log for the exact times).
- If you decide not to run the Data Transfer Tool, you will have missing data. Take this into account when looking at reports.
- If you did not record the time of the database backup, choose a date prior to the date of backup. You will have no data missing, but the Data Transfer Tool will take longer than necessary.
- When you run the Data Transfer Tool for a second time, you must choose a different path for the temporary folder than the one chosen for the first run.
- If you accidentally enter the credentials of the staging DB and not the production DB, you will receive the following error message: **Operation Failed … FileNotFoundException**. Enter the correct details, and continue.
- The UI allows you to pause the Transferred data upgrade, but actually this does not have any effect.

Verifying Digitally Signed HP Files

All HP installation files that are in the format listed below are digitally signed:

- **Windows:** MSI, EXE, DLL, VBS, JS, CPL.
- **Linux:** RPM files only.

To verify that the installation files are original HP-provided code and have not been manipulated by a third party, you can do the following:

For Windows files:

1. Right-click the file and select **Properties**.
2. Select the **Digital Signatures** tab and verify that the name of the signer is Hewlett-Packard.

For Linux files:

Open a command line, and run the following commands:

rpm -v -checksig ${RPM_FILE_NAME}# rpm -v -qi -p ${RPM_FILE_NAME}

For example:

```
# rpm -v --checksig  HPBsmFndCom1-9.10.320-Linux2.6_64.rpm
HPBsmFndCom1-9.10.320-Linux2.6_64.rpm:
    Header V3 DSA signature: OK, key ID 2689b887
    Header SHA1 digest: OK (a4b436a86ca52dde34113c964866d5838b50bbc5)
    MD5 digest: OK (59def5f6719a78eac778324bdb0f6f05)
```

```
    V3 DSA signature: OK, key ID 2689b887


# rpm -v -qi -p  HPBsmFndCom1-9.10.320-Linux2.6_64.rpm
Name        : HPBsmFndCom1                 Relocations: (not relocatable)
Version     : 9.10.320                          Vendor: Hewlett-Packard Company
Release     : 1                             Build Date: Sun 27 Mar 2011 06:15:37
PM IST
Install Date: (not installed)               Build Host: LABM1AMRND02.devlab.ad
Group       : Applications/System           Source RPM: HPBsmFndCom1-9.10.320-
1.src.rpm
Size        : 298420659                        License: Hewlett-Packard
Development Company, L.P.
Signature   : DSA/SHA1, Sun 27 Mar 2011 07:04:03 PM IST, Key ID 527bc53a2689b887
Summary     : HP BSM Foundations Common Components Pack_1
Description :
HP BSM Foundations Common Components Pack_1
```

Limitation

- Search queries defined in **EUM Admin > Search and Replace** for BSM version 9.01 do not work in BSM 9.13 or later .

  Workaround: Recreate the queries in the later BSM version.

- In the staging environment, you cannot retrieve any data for reports that query RUM when RUM is pointing to the BAC side.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on BSM Upgrade Guide - 8.0x to 9.26 (Business Service Management 9.26)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Sw-doc@hpe.com.

We appreciate your feedback!