HP Business Service Management

Software Version: 9.26

BSM Installation Guide

Document Release Date: September 2016
Software Release Date: September 2016

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

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 Installation Guide. This guide provides a detailed workflow for installing BSM.

This guide is for customers who do not have any version of BSM.

If you have a previous version of BSM, see the BSM Upgrade Guides.

How This Guide is Organized

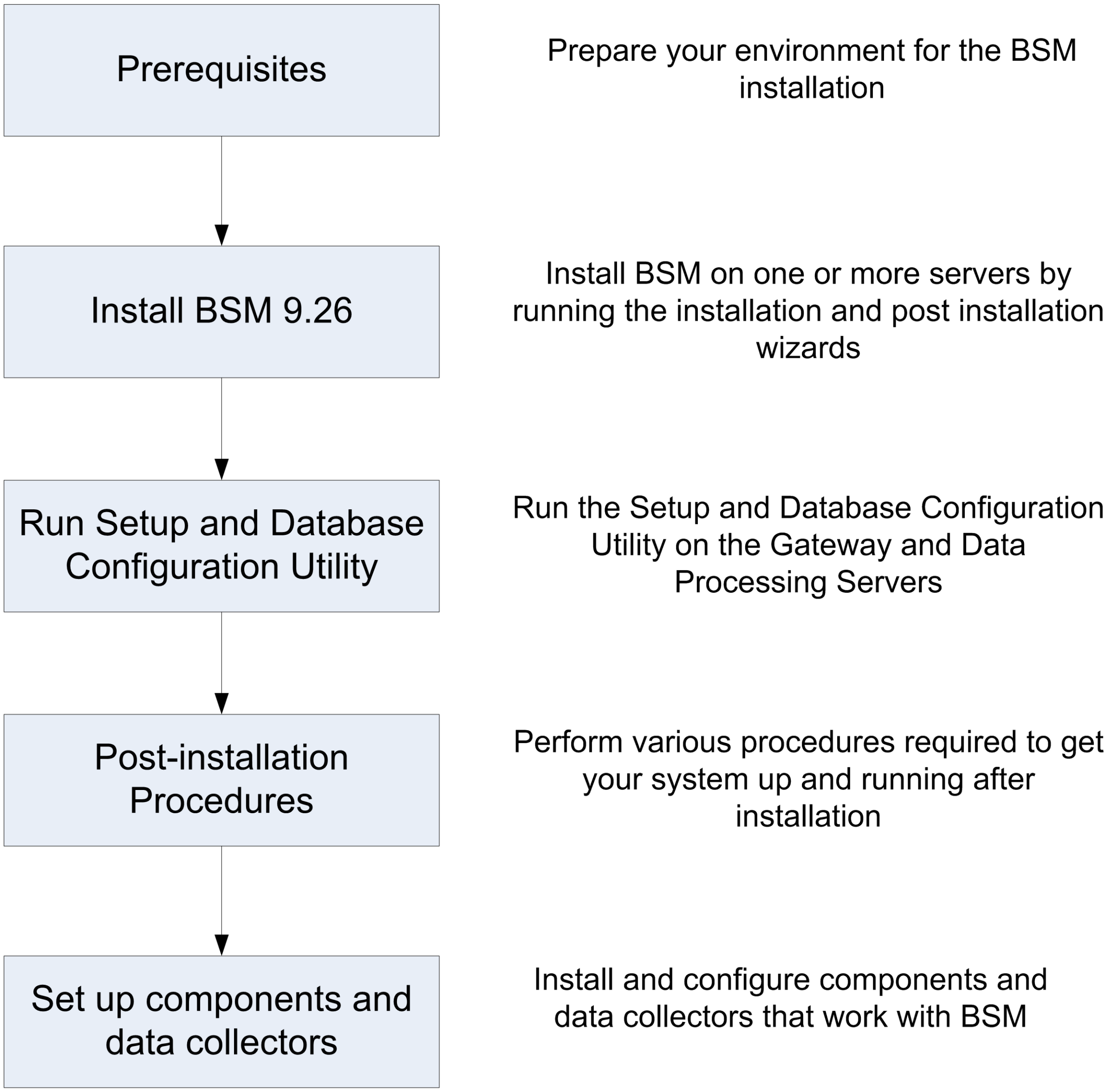
This book is divided into two parts:

- Part I contains the step-by-step workflow for installing BSM.
- Part II, the appendix, contains reference information and optional procedures.

Part I: Installation Workflow

Chapter 1: BSM 9.26 Installation Overview

The installation of BSM 9.26 involves the following main steps:



Prerequisites

Prepare your environment for the BSM installation

Install BSM 9.26

Install BSM on one or more servers by running the installation and post installation wizards

Run Setup and Database Configuration Utility

Run the Setup and Database Configuration Utility on the Gateway and Data Processing Servers

Post-installation Procedures

Perform various procedures required to get your system up and running after installation

Set up components and data collectors

Install and configure components and data collectors that work with BSM

Chapter 2: General Prerequisites

Perform the following steps before starting the installation process:

1. Create a 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. 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).

3. Prepare hardware

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

4. Set up web server (optional)

BSM installs the Apache web server on all BSM Gateway servers during the installation. If you want to use the Apache web server and you have already installed IIS web server, stop the **IIS Web Server** service before installing BSM. Do not change the **Startup Type** setting of this service. Do not remove **IIS Web Server** as a role. If you want to use the IIS web server, install and enable it on all Gateway servers before installing BSM.

> **Note:** There can only be one running Web server on a server machine that uses the same port as BSM. For example, if you use the 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. For more information, see:
>
> - For Linux: "Working with the Web Server" on page 68
> - For Windows: "Working with the Web Server" on page 75

5. Requirements for Monitoring Automation

- **Run-time Service Model (RTSM)** – RTSM Content Pack 11.09 or higher.
- **HP Operations Agent** (if used) – Version 11.12 or higher.
- **HP SiteScope** (if used) – Version 11.22 or higher. SiteScope must *not* be hosted on the BSM server, but requires its own server.
- **HP ArcSight Logger** (if used) – Version 5.30 or higher.

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 75.

- 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.

- 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 unless you are installing BSM in silent mode. For details, see "Installing BSM Silently" on page 91.

- 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.

Chapter 3: Install BSM 9.26

Install BSM 9.26 on a set of 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 directs you as to when to begin installation on the Gateway Server.

The installation wizard guides you to run the post installation wizard. After running the post-installation wizard, you have the option of running the setup and database utility automatically now, or running it later.

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

Note: If the host system for the BSM installation is preinstalled with an HP Operations Agent, you must configure the agent to run under the same user as BSM. You must install BSM using a user with root (Linux) or administrative privileges (Windows). If necessary, switch the user under which the agent is running to the root user (Linux) or the user with administrative privileges that is being used to install BSM (Windows).

Note: If you are installing BSM 9.26 on Windows Server 2008 R2 or 20012 R2:

1. In **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system** locate **Enable LUA** and change the value to **0**.

2. Reboot the machine.

To installation BSM 9.26:

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. 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 BSM 9.26 package and save it locally.

   f. Launch the relevant setup file to install BSM 9.26.

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

Alternatively, you can run these wizards in silent mode. For details, see "Installing BSM Silently" on page 91.

For more details, see the following sections:

- "Installing BSM on a Linux Platform" on page 66
- "Installing BSM on a Windows Platform" on page 72

Note: HP recommends that after you install BSM 9.26, clean the JBoss cache:

1. Stop the JBoss process.
2. Remove the **HPBSM/jboss-as/standalone/tmp** folder.
3. Start the JBoss process.

Chapter 4: Post-Installation Procedures

This chapter contains the following topics:

General Post-Installation Procedures

Perform these tasks to complete the installation 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.

- ## Configure Event Traffic when using OM Agent

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

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

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

- ## Create Profile Database

  You create the profile database schema after running the installation wizards. For more information, see "Creating Databases" in the BSM Platform Administration Guide.

- ## Upload additional licenses

  The main BSM license is entered during the main BSM installation. However, a number of BSM applications require additional licenses. To use these applications, you must obtain licenses from HP. For more information visit HP Software Support site (https://softwaresupport.hp.com).

You upload the license files in the License Manager. For more information, see "License Manager Page" in the BSM Platform Administration Guide.

- ## Configure LW-SSO when load balancer is located in separate domain

  If you are using a load balancer and it is not in the same domain as servers integrating with BSM (for example, NNMi, TransactionVision, OO), you need to customize a LW-SSO configuration. For details, see LW-SSO Configuration for Multi-Domain and Nested Domain Installations in the BSM Platform Administration Guide.

- ## Configure load balancer or reverse proxy certificates

  If you are using a Load Balancer or Reverse Proxy in which your data sources are not communicating directly with the BSM Gateway Server, perform the following task:

  > **Note:** Generally, OMi certificates must be exchanged on all nodes (Data Processing Servers, Gateway Servers, manager of manager configurations, and Load balancers). 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, certificate exchange on the Load Balancer node is not required if you are Load Balancing on the recommended OSI layer 2 or 4.

  For details about Reverse Proxy configuration, see the BSM Hardening Guide.

  a. Request server and client certificates from your Certificate Authority for each front-end server (could be a load balancer VIP or a reverse proxy VIP)

     If you do not have a Certificate Authority, you can issue an OMi certificate from the BSM Data Processing server with the following command:

     ```
     ovcm -issue -file <certificate file> -name <Fully Qualified Domain Name of
     load balancer or reverse proxy node> [ -pass <passphrase>]
     ```

  b. Import these certificates to the load balancer or reverse proxy.

  c. Make sure the load balancer/reverse proxy trusts your Certificate Authority (you may need to import the Certificate Authority certificate into the load balancer/reverse proxy).

  d. On the load balancer/reverse proxy add a listener on port 383.

- ## Perform hardening procedures

  If you want to secure the communication between BSM servers, perform the procedures in "Using TLS in BSM” in the BSM Hardening Guide.

- ## Ensure all processes started properly

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

- ## Install and Configure System Health

  System Health enables you to monitor the performance of the servers, databases, and data collectors running on your BSM system and ensure that they are functioning properly. It is recommended that you install and configure System Health after you deploy BSM servers. For details, see the System Health 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).

- ## 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
```

Restart BSM

Restart BSM by disabling and then enabling all servers. For details, see "Starting and Stopping BSM" on the next page.

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 80.

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.

Monitoring Automation

With traditional management tools, monitoring composite applications deployed in the cloud infrastructures that are typical for modern Hybrid IT environments is a complex, time-consuming and often error-prone task. Monitoring Automation enables you to simplify the configuration and deployment process for most monitoring solutions.

Monitoring Automation Features

Monitoring Automation includes the following features:

Aspects - Using aspects enables you to design monitoring solutions that are independent of the application being monitored, and to hide system details for users focused on application health.

Parameters - Using parameters enables you to tune aspects and monitoring templates to the monitoring context.

Automatic Assignments - Using automatic assignment rules allows you to design monitoring solutions that automatically adapt to topology changes.

Configuration Reports - Using configuration reports facilitates auditing system compliance, and greatly reduces the risk of downtime.

OMi Management Packs and Content Packs

Optional management packs and their associated content packs provide customizable management templates, aspects and content.

Install the OMi Management and Content Packs for the systems you want to start monitoring immediately as described in "OMi Management Packs and Content Packs" on the next page.

HP Operations Agent and SiteScope

This section describes the monitoring methods supported by HP BSM.

Using an HP Operations Agent

The HP Operations Agent resides on a server and collects detailed performance data. The agent can be configured to support the following actions:

- Generate alerts.
- Execute an action autonomously if a metric breaches a threshold value.
- Use the collected metrics to adjust the monitoring thresholds.

The HP Operations Agent is available from the HP Operations Agent v11.14 media.

Using SiteScope

HP SiteScope collects performance data centrally from a number of servers across physical, virtual and cloud infrastructures, including HP Cloud Services, removing the need to have an agent on each system to be monitored.

For details about HP SiteScope, visit the following web site:

```
http://www8.hp.com/us/en/software-solutions/software.html?compURI=1174244&jumpid=hpr_r1002_usen_link1#.UZ9QJZz4JrU
```

> **Note:** Licenses for HP Operations Agents and HP SiteScope are not included in the Monitoring Automation license, and must be purchased separately.

OMi Management Packs and Content Packs

You may want to install optional OMi management packs and content packs, which provide the essential Monitoring Automation content enabling you to immediately start monitoring selected systems and applications.

This section describes where to source the software for management and content packs.

> **Note:** Content Packs are not included in the BSM or Monitoring Automation licenses, and must be purchased separately.

- **Management Packs for HP Operations Manager i**

  The management packs for Infrastructure, Hadoop, Vertica and Oracle Database are available from the HP OMi Management Packs media.

For details about obtaining and installing management packs, see the *HP OMi Management Packs Installation Guide*.

- **Content Packs for Infrastructure, Hadoop and Vertica**

  For details about obtaining and installing the Infrastructure, Hadoop and Vertica Content Packs see the *BSM Platform Administration Guide*, section *Importing Content Packs*. Provided your HP Passport identifies you as a customer of Content Packs for BSM, you can download content packs from the following web site:

  `https://hpln.hp.com/group/content-packs-bsm`

- **Content Pack for Oracle Database**

  The Content Pack for Oracle Database is included in the BSM media kit.

To install a Content Pack:

1. Place the content pack file (`*.zip` or `*.xml`) for the Content Pack to be installed in a location accessible from the BSM server.

2. Launch BSM. In BSM, select **Admin > Operations Management > Setup > Content Packs**. The Content Packs screen is shown.

3. Click **Import Content Pack Definitions and Content**. The Import Content Pack dialog is shown.

4. Click **Browse**, browse to the content pack file and click **Import**. The selected content pack is installed and added to the list of content packs in the Contact Pack Definitions pane (left pane).

Connecting an HP Operations Agent

> **Note:** The HP Operations Agent software is not included in the BSM or Monitoring Automation licenses, and must be purchased separately.

For details about installing and verifying correct deployment of an HP Operations Agent, see the following sections in the *HP Operations Agent and HP Operations Smart Plug-ins for Infrastructure Installation and Configuration Guide*:

- *Installing HP Operations Agent Using HP Server Automation* or *Installing HP Operations Agent using Microsoft System Center 2012 Configuration Manager*.

- *Installing the Agent in the Inactive Mode*. This section includes instructions for pre-installation in a virtual machine image.

> **Tip:** To facilitate HP Operations Agent installation, you can consider deploying using one of the

following methods:

- Include the HP Operations Agent installation in your virtual machine cloning process.
- Include the HP Operations Agent software in your general software distribution process.
- Install the HP Operations Agent software remotely using a distribution tool such as SCP.

For details, refer to the HP Operations Agent documentation.

To monitor a system with an HP Operations Agent, you must connect the HP Operations Agent to the Monitoring Automation server:

1. Connect the agent to BSM:

   a. On the system hosting the agent, navigate to the following location:

      Windows: `<OvInstallDir>\bin\win64\OpC\install`

      (Default: `C:\Program Files\HP\HP BTO Software\bin\win64\OpC\install`)

      Linux: `/opt/OV/bin/OpC/install/`

   b. Open a command prompt, and issue the following command:

      Windows: `cscript opcactivate.vbs -srv <OMi_Gateway_Server>`

      Linux: `. /opcactivate -srv <OMi_Gateway_Server>`

2. Grant the required certificates:

   a. Go to the server hosting BSM and launch BSM.

   b. In BSM, select **Admin > Operations Management**. Activate the **Setup** tab and click the link **Certificate Requests**. A list of certificate requests is shown.

   c. Identify the new certificate request issued by the agent. New requests are prefixed with the 🗎 icon. Select the new request and click ✓ **Grant**. The request is granted and prefixed with the ✓ icon.

   For details about granting certificate requests, see the Operations Manager online help.

   Tip: You can grant certificates automatically using pre-configured IP ranges or a groovy script.

3. Check BBC communication in both directions:

a. On the BSM server, open a command prompt and issue the following command:

```
bbcutil -ping https://<FQDN of the host>
```

Make sure the agent responds with the message: `eService=OK`.

b. On the system hosting the agent, open a command prompt and issue the following command:

```
bbcutil -ping https://<OMi_Gateway_Server>
```

Make sure the BSM Server responds with the message: `eService=OK`.

The agent is now installed and connected, and can be deployed using Monitoring Automation.

Connecting a SiteScope Server

Use the SiteScope user interface to verify that the SiteScope server has an HP Operations Agent installed on it. If necessary, install the agent.

Note: If you are using more than one SiteScope server and want to use advanced features for balancing between these servers (for example, based on license points or number of monitors), you have to additionally set up the SiteScope server in the System Availability Management (SAM) section of BSM. SAM is is not included in the BSM or Monitoring Automation licenses, and must be purchased separately.

To monitor a system that is managed by SiteScope, connect SiteScope to the Monitoring Automation server:

1. Ensure that the HP Operations Agent is installed on the SiteScope system. For details, see the *HP SiteScope Deployment Guide*.

2. Connect the agent to BSM:

    a. On the SiteScope system, launch SiteScope and select **Preferences > Integration Preferences**. The Integration Preferences pane is shown.

    b. Click **New Integration** and select HP Operations Manager Integration. The integration is activated, resulting in the HP Operations Agent sending a certificate request to BSM.

    c. Grant the required certificates:

        i. Go to the server hosting BSM and launch BSM.

        ii. In BSM, select **Admin > Operations Management**. Activate the **Setup** tab and click the link **Certificate Requests**. A list of certificate requests is shown.

        iii. Identify the new certificate request issued by the agent. New requests are prefixed with the icon. Select the new request and click ✓ **Grant**. The request is granted and prefixed with the ✓ icon.

For details about granting certificate requests, see the Operations Manager online help.

> **Tip:** You can grant certificates automatically using pre-configured IP ranges or a groovy script.

3. Update the HP SiteScope configuration component `sisconfig`, as follows:

   a. On the BSM Monitoring Automation server, navigate to the following directory:

   ```
   <BSM root directory>/opr/subagents/sitescope
   ```

   b. Open the following archive:

   ```
   sisinstall-<version>.zip
   ```

   <version> is the version of the SiteScope Config component.

   c. Extract the following file from the archive and copy it to a temporary location on the SiteScope server:

   ```
   oprsisconnector.jar
   ```

   d. On the HP SiteScope server, stop the `sisconfig` component with the following command:

   ```
   ovc -stop sisconfig
   ```

   e. Replace the following file with the file you copied from the BSM server:

   Windows: `<OvInstallDir>\java\oprsisconnector.jar`

   Linux: `/opt/OV/java/oprsisconnector.jar`

   The `sisconfig` component is now updated to the version to be used with Monitoring Automation.

   f. Restart the `sisconfig` component with the following command:

   ```
   ovc -start sisconfig
   ```

4. Configure the agent with the SiteScope user credentials:

   a. On the SiteScope system, issue the following command:

   Windows: `<OvInstallDir>\lbin\sisconfig\sisSetCredentials.bat`

   UNIX or Linux: `/opt/OV/lbin/sisconfig/sisSetCredentials.sh`

   The credentials tool is started.

   b. When prompted, enter the following credentials:

      `SiteScope login`: User name for SiteScope.

      `SiteScope password`: Corresponding password.

      `SiteScope port`: SiteScope server port (default: `8080`).

   c. Display and verify the configured credentials with the following command:

      ```
      ovconfget opr.sisconfig
      ```

5. Set the `MANAGER_ID` on the SiteScope system to the BSM Core ID:

   a. Obtain the value of the BSM Core ID on the BSM Gateway Server with the following command:

      ```
      ovcoreid -ovrg server
      ```

   b. Set the correct `MANAGER_ID` on the SiteScope system with the following command:

      ```
      ovconfchg -ns sec.core.auth -set MANAGER_ID <core ID>
      ```

      where *`<core ID>`* is the BSM Core ID from the previous step.

   c. Restart the agent processes on the SiteScope server with the following command:

      ```
      ovc -restart
      ```

   d. Verify that the `MANAGER_ID` is correctly configured with the following command:

      ```
      ovconfget sec.core.auth
      ```

6. Launch BSM and set up the SiteScope system as a connected server in Operations Management:

   a. Select **Admin > Operations Management > Setup > Connected Servers**. The Connected Servers screen is shown.

   b. Click ✳ **New Item**. The Create New Server Connection wizard is shown.

   c. Complete the wizard with the details of the SiteScope server. Click **Finish** to add a new node to the list of monitored nodes.

   d. To verify the node was created correctly, select **Admin > Operations Management > Setup > Monitored Nodes**. The Monitored Nodes screen is shown. Make sure that the list of monitored nodes contains a CI of CI type Node for the SiteScope system.

If the node is missing, add it manually.

7. Configure any required policy templates in SiteScope and import them into BSM. For details about importing policy templates, see *Importing HP SiteScope Templates* in the *Monitoring* section of the *BSM Help*.

> **Note:**
>
> - You cannot create SiteScope policy templates in BSM.
> - After the import, you can edit only the general properties of SiteScope policy templates. The data part is read-only.

SiteScope is now connected to BSM.

t'sManaging a BSM Host System with Monitoring Automation (Optional)

The following HP Operations Agents are supported:

- 11.14 and higher (HP recommends using the latest available agent version).
- 11.11 (Not in conjunction with Monitoring Automation).
- 11.10 (Not in conjunction with Monitoring Automation).

If your BSM system is installed on Windows, contact HP Support and ask for hotfix **QCCR1A147794**.

If you are installing HP Operations Agents 11.10 after installing BSM, install hotfix **QCCR1A149034** before installing HP Operations Agents 11.10.

To install HP Operations Agent on a system where BSM is installed distributed on Gateway and Data Processing Servers, perform the following steps on all Gateway and Data Processing Servers, and enter the Gateway Server or Load Balancer as certificate server:

1. Install a supported HP Operations Agent on the BSM host system. For details, see the HP Operations Agent documentation.

> **Caution:** Do not use the option `-force_config_mode`. This option replaces the client certificate on your BSM server, with the result that several processes will no longer start.

> **Note:** When configuring the HP Operations Agent using the `oainstall -i -a` command,

> use the FQDN of the BSM Gateway Server or the FQDN of the Load Balancer as the value for the `-srv` and `-cert_srv` option. For example:
>
> ```
> oainstall –i –a –srv <FQDN of Gateway Server or Load Balancer> –cert_srv
> <FQDN of Gateway Server or Load Balancer>
> ```

2. Use the following command to check if the agent is configured properly:

   ```
   ovconfget –ovrg server sec.cm.client

   ovconfget –ovrg server sec.core.auth
   ```

   Make sure that the following values are set correctly:

   ```
   [sec.cm.client]

   CERTIFICATE_SERVER=<FQDN of Gateway server or Load Balancer>

   [sec.core.auth]

   MANAGER=<FQDN of Gateway server or Load Balancer>

   MANAGER_ID=<CoreID of OVRG server>
   ```

3. Use the following command to get the CoreID of OVRG:

   ```
   ovcoreid -ovrg server
   ```

4. If the attributes are not set, set them by using the command:

   ```
   ovconfchg -ovrg server –ns <namespace> –set <attr> <value>
   ```

5. Restart the agent and check its status:

   ```
   ovc –kill

   ovc –start

   opcagt -status
   ```

6. Restart the WDE process on all Gateway servers.

7. Before deploying policies to the BSM node, add the BSM server as a monitored node with the Node Editor in the BSM Administration UI:

   a. Select **Admin > Operations Management**.

   b. Select **Setup > Monitored Nodes**.

   c. Select **Predefined Node Filters > All Nodes**.

   d. Click the **New Node** button on the middle pane to create a node.

Using Monitoring Automation

This section lists all access points for Monitoring Automation functionality in BSM, and provides a brief description of the intended use of each feature. For detailed information, see the *Monitoring Automation User Guide* and the online help.

Admin > Operations Management > Monitoring > Management Templates and Aspects

User interface for creating, editing and managing management templates and aspects.

Admin > Operations Management > Monitoring > Policy Templates

User interface for creating, editing and managing policy templates. Policy templates are the foundation building blocks for management templates and aspects.

Admin > Operations Management > Monitoring > Assignments and Tuning

User interface for assigning management templates, aspects and policy templates, and tuning existing assignments.

Admin > Operations Management > Monitoring > Automatic Assignment Rules

User interface for creating automatic assignment rules for management templates and aspects.

Admin > Operations Management > Monitoring > Deployment Jobs

User interface for viewing and managing the deployment jobs triggered by assignments.

Admin > Platform > Setup and Maintenance > Infrastructure Settings, **Application** `Monitoring Automation`

User interface for managing infrastructure settings for Monitoring Automation.

Admin > Operations Management > Setup > Monitored Nodes

User interface for organizing and managing monitored nodes. Nodes are devices in your IT infrastructure that are monitored by an HPOM Agent or SiteScope.

User Engagement

The innovative User Engagement feature applies game dynamics to add extra stimulation to Operations Management users by providing business-enhancing challenges, accelerating operations bridge efficiency and user know-how. Successful progress through the various activities is rewarded with Achievements and real-time notifications of great performance, helping to provide extra motivation to better engage with Operations Management which improves users' performance in their daily work.

Setting Up User Engagement

The following sections describe how to set up User Engagement for first use after completing installation and configuration.

For detailed information about the functionality of User Engagement, see the *User Engagement for HP Operations Manager i User Guide* or the *User Engagement* section in the *BSM online help* (**Help > Application Administration > Operations Management > Additional Configuration > User Engagement**).

Configuring Administrator Privileges

Note:

- BSM administrators are not automatically granted administrator privileges for User Engagement. You must grant administrator privileges to those accounts that require them manually as described below.

- After initial installation, the only user account with administrator privileges for User Engagement is the built-in BSM administrator account. It is not possible to delete or rename this account. (You can, however, change its User Engagement participant details.) For more information about the built-in BSM administrator account, see the *BSM Installation Guide*.

- Users logging on to the User Engagement stand-alone user interface with the built-in BSM administrator account `admin` receive administrator privileges. The default password for this account is `admin`. HP recommends to change the default password to a more secure value as part of setting up BSM for first use. To change the password, follow the procedure below for the participant `admin`.

To grant User Engagement administration privileges to selected participants:

1. Log on to BSM as administrator and select **Admin > Operations Management**. In the **Setup** tab, select **User Engagement**. In the User Engagement screen, select **Participants**. The Participants dialog opens.

2. Click **Edit Participant** for the participant to which you want to grant User Engagement

administrator privileges. The Edit Participant dialog opens.

a. Under **Roles**, select **Administrator**.

b. *Optional*: If necessary, change the participant's password.

c. Click **OK** to close the dialog.

3. Repeat the previous step for all participants to be granted User Engagement administrator privileges.

About New Participants

New participants in User Engagement are created automatically whenever they perform an action in Operations Management which is associated with an achievement or if they open the User Engagement interface from within BSM. There is usually no need to create them manually.

Changing Your Settings as a Participant

To change the User Engagement settings for your account:

1. Log on to BSM and select **Applications > Operations Management**.

2. Select `User Engagement Dashboard` in the drop-down list box in the main toolbar saying `Select Page`. The User Engagement dashboard opens.

3. Click ⚙**Operations Manager i User Engagement Configuration**. The configuration dialog opens.

4. Check the **Participate** check box if you wish to participate or clear it to exclude your account from participation. You can also choose to participate in expert boards and have your email address displayed.

5. Click **OK** to save your changes and close the dialog.

Enabling and Disabling User Engagement

By default, User Engagement is enabled. After installation, it is not necessary to enable it. If required, however, you can change whether User Engagement is enabled or disabled using the *Infrastructure Settings Manager*:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. The *Infrastructure Settings Manager* opens. Select **Applications** and in the list, select **Operations Management**. A number of sections with settings for Operations Management, listed in alphabetical order, appear.

2. Find the section `Operations Management - User Engagement`.

3. Click ✎ **Edit Setting** for the entry `Enable User Engagement`, and enter the value `false` to disable User Engagement , or `true` to enable it.

Enabling and Disabling Achievements

Achievements can be enabled or disabled. When disabled, achievements are not visible to users.

Achievements are enabled according to the following rules:

- After installing User Engagement for the first time, a default set of achievements is enabled. For details, see the *User Engagement for HP Operations Manager i User Guide* or the *User Engagement* section in the *BSM online help* (**Help > Application Administration > Operations Management > User Engagement**).

- Achievements can be enabled or disabled manually by an administrator, as follows:

  a. Log on to BSM as administrator and select **Admin > Operations Management**. In the **Operations Console** tab, select **Achievements**. The *Achievements* page opens.

  b. In the *Achievements* page, click **Run Achievement** for an achievement to be enabled, or **Disable and Revert Achievement** for an achievement to be disabled and its threshold value to be reset to its default. An enabled achievement is visible to all participants.

Chapter 5: Configuring Secure Access to BSM Reverse Proxy

This chapter describes the security ramifications of reverse proxies and contains instructions for using a reverse proxy with BSM.

This chapter discusses only the security aspects of a reverse proxy. It does not discuss other aspects of reverse proxies, such as caching and load balancing.

A reverse proxy is an intermediate server that is positioned between the client machine and the Web server(s). To the client machine, the reverse proxy seems like a standard Web server that serves the client machine’s HTTP or HTTPS protocol requests with no dedicated client configuration required.

The client machine sends ordinary requests for Web content, using the name of the reverse proxy instead of the name of a Web server. The reverse proxy then sends the request to one of the Web servers. Although the response is sent back to the client machine by the Web server through the reverse proxy, it appears to the client machine as if it is being sent by the reverse proxy.

BSM supports a reverse proxy in DMZ architecture. The reverse proxy is an HTTP or HTTPS mediator between the BSM data collectors/application users and the BSM servers.

Your data collectors may access BSM through the same virtual host or a different virtual host as your application users.

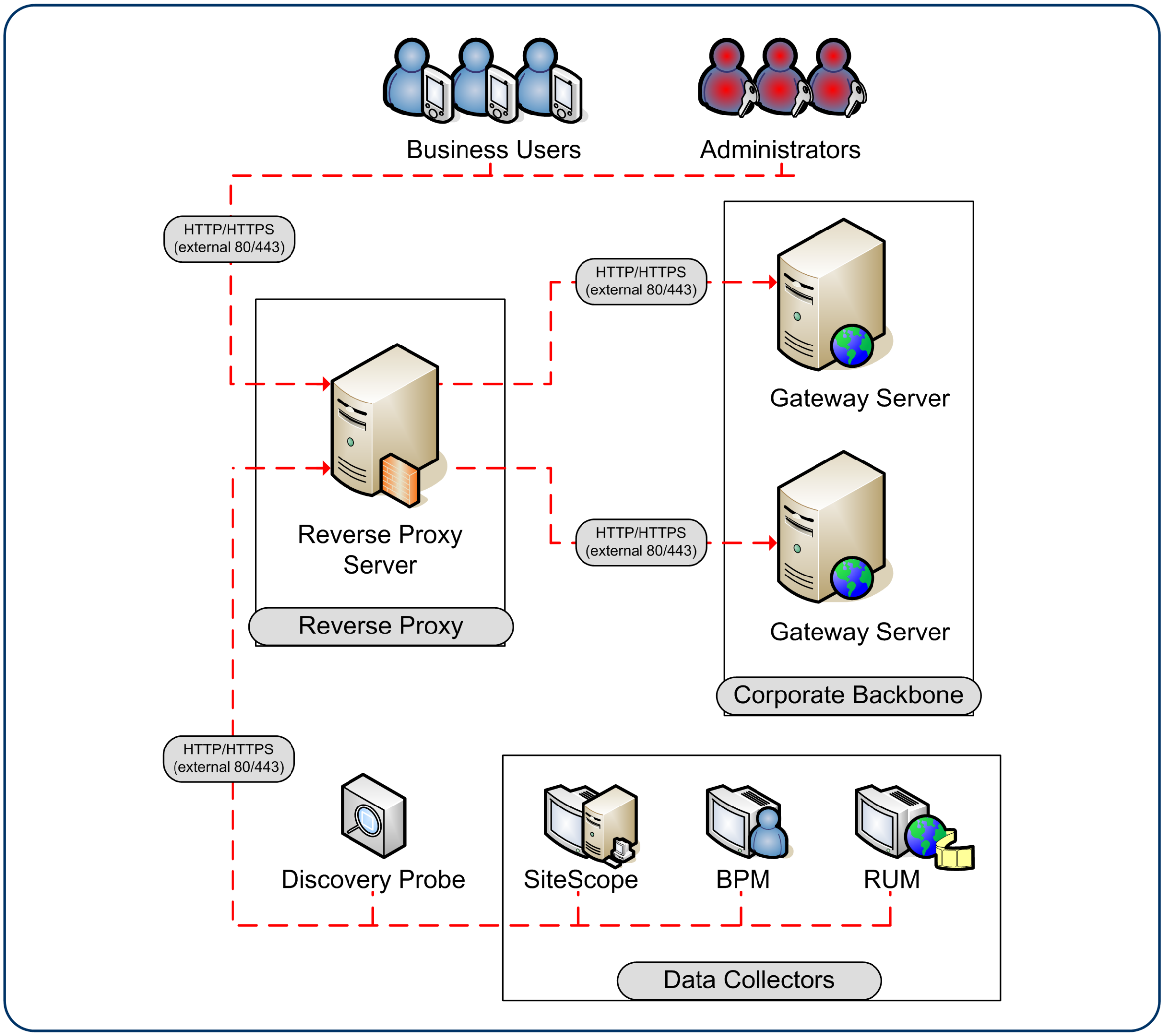
This chapter contains the following topics:

Reverse Proxy Configuration

In this topology, the reverse proxy context is divided into two sections:

- Communication that is redirected to the Virtual Host for Data Collectors.
- Communication that is redirected to the Virtual Host for Application Users.

The use of a reverse proxy is illustrated in the following diagram. Your data collectors may access BSM through the same virtual host or a different virtual host as your application users. For example, your environment may use one load balancer for application users and one load balancer for data collectors.



Reverse proxy BSM support should be configured differently in each of the following cases:

Scenario #	BSM Components Behind the Reverse Proxy
1	Data collectors (Business Process Monitor, Real User Monitor, SiteScope, Data Flow Probe, BSM Connector)
2	Application users
3	Data collectors and application users

Note: When configuring a Reverse Proxy with TransactionVision, only one instance of the TransactionVision UI/Job Server exists, even if there are multiple Gateway Servers in your environment.

Reverse Proxy Configuration Workflow

This section describes the overall workflow for configuring a reverse proxy to work with BSM servers. The procedure differs depending on the web server of your reverse proxy.

1. If you have a load balancer that is functioning as a reverse proxy, you do not need to configure an additional reverse proxy. For details, see "Load Balancing for the Gateway Server" on page 118.

2. Perform the relevant procedure depending on whether your reverse proxy is using the Apache or IIS web server.

   Apache. "Configuring a Reverse Proxy - Apache" on the next page.

   IIS. "Configuring a Reverse Proxy - IIS" on page 54.

3. Configure BSM to support your reverse proxy. For details, see "HP BSM Specific Configuration" on page 60.

4. Configure BSM to support multiple Secure Reverse Proxies. For details, see "Enabling BSM to Configure Multiple Reverse Proxies" on page 62.

Configuring a Reverse Proxy - Apache

This section contains the procedures describing how to configure a reverse proxy using apache web server versions 2.2.x.

> **Note:** Securing access to the reverse proxy should be performed as part of the Hardening Workflow. For details, see *Hardening Workflow* in the Hardening Guide.

This section contains the following topics:

- "Configuring Apache to Work as a Reverse Proxy " below
- "Configuring BBC Port 383 Connection on Reverse Proxy" on page 48
- "Reference - Support for BSM Application Users" on page 50.
- "Reference - Support for BSM Data Collectors" on page 53.

Configuring Apache to Work as a Reverse Proxy

> **Note:** Securing access to the reverse proxy should be performed as part of the Hardening Workflow. For details, see *Hardening Workflow* in the Hardening Guide.

1. Configure Apache to work as a reverse proxy.

   Apache must be manually configured to function as a reverse proxy.

   For example:

   a. Open the <Apache installation directory>\Webserver\conf\httpd.conf file.

   b. Enable the following modules:

      - LoadModule proxy_module modules/mod_proxy.so
      - LoadModule proxy_http_module modules/mod_proxy_http.so

   c. Add the following lines:

```
ProxyRequests off

<Proxy *>
       Order deny,allow
       Deny from all
```

```
            Allow from all
     </Proxy>
     ProxyTimeout 300
```

2. Add support for application users and data collectors as seen in the following example. For more details, see "Reference - Support for BSM Application Users" on page 50 and "Reference - Support for BSM Data Collectors" on page 53.

Data Collectors:

```
ProxyPass              /ext                    http://DATA/ext
ProxyPassReverse       /ext                    http://DATA/ext
ProxyPass              /topaz/topaz_api        http://DATA/topaz/topaz_api
ProxyPassReverse       /topaz/topaz_api        http://DATA/topaz/topaz_api
ProxyPass              /mam-collectors         http://DATA/mam-collectors
ProxyPassReverse       /mam-collectors         http://DATA/mam-collectors
```

Application Users:

```
ProxyPass              /mercuryam              http://USERS/mercuryam
ProxyPassReverse       /mercuryam              http://USERS/mercuryam
ProxyPass              /hpbsm                  http://USERS/hpbsm
ProxyPassReverse       /hpbsm                  http://USERS/hpbsm
ProxyPass              /topaz                  http://USERS/topaz
ProxyPassReverse       /topaz                  http://USERS/topaz
ProxyPass              /webinfra               http://USERS/webinfra
ProxyPassReverse       /webinfra               http://USERS/webinfra
ProxyPass              /filters                http://USERS/filters
ProxyPassReverse       /filters                http://USERS/filters
ProxyPass              /TopazSettings          http://USERS/TopazSettings
ProxyPassReverse       /TopazSettings          http://USERS/TopazSettings
ProxyPass              /opal                   http://USERS/opal
ProxyPassReverse       /opal                   http://USERS/opal
ProxyPass              /mam                    http://USERS/mam
ProxyPassReverse       /mam                    http://USERS/mam
ProxyPass              /mam_images             http://USERS/mam_images
ProxyPassReverse       /mam_images             http://USERS/mam_images
ProxyPass              /mcrs                   http://USERS/mcrs
ProxyPassReverse       /mcrs                   http://USERS/mcrs
ProxyPass              /rumproxy               http://USERS/rumproxy
ProxyPassReverse       /rumproxy               http://USERS/rumproxy

ProxyPass              /odb                    http://USERS/odb
ProxyPassReverse       /odb                    http://USERS/odb
ProxyPass              /uim                    http://USERS/uim
ProxyPassReverse       /uim                    http://USERS/uim
ProxyPass              /ucmdb-api              http://USERS/ucmdb-api
```

```
ProxyPassReverse       /ucmdb-api              http://USERS/ucmdb-api
ProxyPass              /ucmdb-ui               http://USERS/ucmdb-ui
       connectiontimeout=1000 timeout=1000
ProxyPassReverse       /ucmdb-ui               http://USERS/ucmdb-ui
ProxyPass              /tv                     http://USERS/tv
ProxyPassReverse       /tv                     http://USERS/tv
ProxyPass              /tvb                    http://USERS/tvb
ProxyPassReverse       /tvb                    http://USERS/tvb
ProxyPass              /opr-admin-server/messagebroker/amfsecure
               http://USERS/opr-admin-server/messagebroker/amf
ProxyPassReverse       /opr-admin-server/messagebroker/amfsecure
               http://USERS/opr-admin-server/messagebroker/amf
ProxyPass              /opr-admin-server/messagebroker/amfpollingsecure
               http://USERS/opr-admin-server/messagebroker/amfpolling
ProxyPassReverse       /opr-admin-server/messagebroker/amfpollingsecure
               http://USERS/opr-admin-server/messagebroker/amfpolling
ProxyPass              /opr-console/messagebroker/amfsecure
               http://USERS/opr-console/messagebroker/amf
ProxyPassReverse       /opr-console/messagebroker/amfsecure
               http://USERS/opr-console/messagebroker/amf
ProxyPass              /opr-admin-server       http://USERS/opr-admin-server
ProxyPassReverse       /opr-admin-server       http://USERS/opr-admin-server
ProxyPass              /opr-console            http://USERS/opr-console
ProxyPassReverse       /opr-console            http://USERS/opr-console
ProxyPass              /opr-gateway            http://USERS/opr-gateway
ProxyPassReverse       /opr-gateway            http://USERS/opr-gateway
ProxyPass              /opr-web                http://USERS/opr-web
ProxyPassReverse       /opr-web                http://USERS/opr-web
ProxyPass              /opr-config-server      http://USERS/opr-config-server
ProxyPassReverse       /opr-config-server      http://USERS/opr-config-server
ProxyPass              /opr-pm                 http://USERS/opr-pm
ProxyPassReverse       /opr-pm                 http://USERS/opr-pm
ProxyPass              /excite-runtime         http://USERS/excite-runtime
ProxyPassReverse       /excite-runtime         http://USERS/excite-runtime
ProxyPass              /excite                 http://USERS/excite
ProxyPassReverse       /excite                 http://USERS/excite
ProxyPass              /OVPM                   http://USERS/OVPM
ProxyPassReverse       /OVPM                   http://USERS/OVPM
ProxyPass              /topaz/sitescope        http://USERS/topaz/sitescope
ProxyPassReverse       /topaz/sitescope        http://USERS/topaz/sitescope
ProxyPass              /cm                     http://USERS/cm
ProxyPassReverse       /cm                     http://USERS/cm
```

> **Note:** If you are using IDM-SSO, you may need to add the following lines (replace siteminderagent in the syntax below with the name of your IDM-SSO vendor):
>
> ```
> ProxyPass         /siteminderagent    http://USERS/siteminderagent
> ProxyPassReverse  /siteminderagent    http://USERS/siteminderagent
> ```

3. Verify reverse proxy points to BSM

   - Restart Apache
   - Go to http://<RP>/topaz - verify that you see the BSM login page. At this point, if you enter your credentials you would see an empty page because BSM is not yet configured to work with a reverse proxy.

Configuring BBC Port 383 Connection on Reverse Proxy

For all products/components using a BBC channel for communication to be able to forward events to the HP BSM server in the reverse proxy environment, port 383 used by the BBC protocol must be configured on the reverse proxy.

The following general steps use Apache as an example:

1. Before beginning this procedure, perform the steps in the "How to Establish a Trust Relationship for an HPOM Server Connection" chapter in the BSM - Operations Manager Integration Guide.

2. Make sure you have established the trust relationship between the HPOM server and the BSM servers as described in the section "How to Establish a Trust Relationship for an HPOM Server Connection" of the BSM - Operations Manager Integration Guide.

   If you add an additional trust relationship to BSM after performing the following procedure, you must issue the certificate for the ReverseProxy node and run this procedure again.

3. Use the utility below to issue a certificate for the ReverseProxy node. This can be done from the BSM processing server or any HPOM server, but not from the BSM gateway server.

   For example:

   ```
   ovcm -issue -file <certificate_file> -name <FQDN (fully qualified domain name)
   of Reverse Proxy> [-pass <passphrase>]
   ```

4. Use openssl to convert it for use by Apache reverse proxy, as in the following:

   SSLCertificateFile:
   ```
   openssl pkcs12 -in <certificate_file> -out oprcl.crt
   ```

   SSLCertificateKeyFile:
   ```
   openssl rsa -in oprcl.crt -out oprcl.pem
   ```

SSLProxyMachineCertificateFile:
`openssl pkcs12 -in <certificate_file> -out oprcl.p12 -nodes -clcerts`

SSLCACertificateFile:
`ovcert -exporttrusted -file trusts.cer`

5. Copy the files to the following directories:

   SSLCertificateFile:
   <Apache_Install_Dir>/Apache2.2/conf/oprcl.crt

   SSLCertificateKeyFile:
   <Apache_Install_Dir>/Apache2.2/conf/oprcl.pem

   SSLProxyMachineCertificateFile:
   <Apache_Install_Dir>/Apache2.2/conf/oprcl.p12

   SSLCACertificateFile:
   <Apache_Install_Dir>/Apache2.2/conf/trusts.cer

6. Modify <BSM Gateway Installation Directory>/WebServer/conf/extra/httpd-ssl.conf file:

   a. Add the following line after the line Listen 443:

   ```
   Listen 383
   ```

   For example:

   ```
   #
   Listen 443
   Listen 383
   #
   ```

   b. Add a virtual host section for port 383 before the SSL Virtual Host Context section.

   Note: In the following, replace **<FQDN of Reverse Proxy>** with the fully qualified domain name of the reverse proxy. For example:
   <VirtualHost bsmgwdualip.test.net:383>

   ```
   <VirtualHost <FQDN of Reverse Proxy>:383>

   ServerName <value of "friendlyName" in oprcl.crt>
   ServerAlias <hostname of RP>
   ServerAdmin <admin email>
   DocumentRoot "<Apache_Install_Dir>/Apache2.2/htdocs"
   ```

```
ErrorLog "<Apache_Install_Dir>/Apache2.2/logs/<FQDN of Reverse Proxy>-
error.log"
TransferLog "<Apache_Install_Dir>/Apache2.2/logs/<FQDN of Reverse
Proxy>-access.log"
ProxyRequests Off
SSLProxyEngine on
SSLEngine on
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile "<Apache_Install_Dir>/Apache2.2/conf/oprcl.crt"
SSLCertificateKeyFile "<Apache_Install_Dir>/Apache2.2/conf/oprcl.pem"
SSLProxyMachineCertificateFile "<Apache_Install_
Dir>/Apache2.2/conf/oprcl.p12"
SSLCACertificateFile "<Apache_Install_Dir>/Apache2.2/conf/trusts.cer"
<Proxy *>
Order deny,allow
Allow from "<DomainName> e.g. .devlab.ad"
</Proxy>
ProxyPass / "https://<FQDN of BSM Gateway>:383/"
ProxyPassReverse / "https://<FQDN of BSM Gateway>:383/"
</VirtualHost>
```

Reference - Support for BSM Application Users

The following table can be used as a reference for application users to connect through the reverse proxy.

Requests for … on the Reverse Proxy Server	**Proxy Request to be Served by:**
/hpbsm/*	http://[Virtual Host for Application Users]/hpbsm/* https://[Virtual Host for Application Users]/hpbsm/*
/excite/*	http://[Virtual Host for Application Users]/excite/* https://[Virtual Host for Application Users]/excite/*
/excite-runtime/*	http://[Virtual Host for Application Users]/excite-runtime/* https://[Virtual Host for Application Users]/excite-runtime/*
/filters/*	http://[Virtual Host for Application Users]/filters/* https://[Virtual Host for Application Users]/filters/*
/mam/*	http://[Virtual Host for Application Users]/mam/* https://[Virtual Host for Application Users]/mam/*
/mam_images/*	http://[Virtual Host for Application Users]/mam_images/* https://[Virtual Host for Application Users]/mam_images/*

Requests for … on the Reverse Proxy Server	Proxy Request to be Served by:
/mcrs/*	http://[Virtual Host for Application Users]/mcrs/* https://[Virtual Host for Application Users]/mcrs/*
/mercuryam/*	http://[Virtual Host for Application Users]/mercuryam/* https://[Virtual Host for Application Users]/mercuryam/*
/odb/*	http://[Virtual Host for Application Users]/odb/* https://[Virtual Host for Application users]/odb/*
/opal/*	http://[Virtual Host for Application Users]/opal/* https://[Virtual Host for Application Users]/opal/*
/opr-admin-server/ messagebroker/amfpolling/*	http://[Virtual Host for Application Users]/opr-admin-server/ messagebroker/amfpolling/* https://[Virtual Host for Application Users]/opr-admin-server/ messagebroker/amfpolling**secure**/* **Note:** Append the word secure to each resource URL when using https.
/opr-admin-server/ messagebroker/amf/*	http://[Virtual Host for Application Users]/opr-admin-server/ messagebroker/amf/* https://[Virtual Host for Application Users]/opr-admin-server/ messagebroker/amf**secure**/* **Note:** Append the word secure to each resource URL when using https.
/opr-console/ messagebroker/amf/*	http://[Virtual Host for Application Users]/opr-console/ messagebroker/amf/* https://[Virtual Host for Application Users]/opr-console/ messagebroker/amf**secure**/* **Note:** Append the word secure to each resource URL when using https.
/opr-admin-server/*	http://[Virtual Host for Application Users]/opr-admin-server/* https://[Virtual Host for Application Users]/opr-admin-server/*
/opr-config-server/*	http://[Virtual Host for Application Users]/opr-config-server/* https://[Virtual Host for Application Users]/opr-config-server/*
/opr-console/*	http://[Virtual Host for Application Users]/opr-console/* https://[Virtual Host for Application Users]/opr-console/*
/opr-gateway/*	http://[Virtual Host for Application Users]/opr-gateway/* https://[Virtual Host for Application Users]/opr-gateway/*
/opr-pm/*	http://[Virtual Host for Application Users]/opr-pm/* https://[Virtual Host for Application Users]/opr-pm/*

Requests for … on the Reverse Proxy Server	**Proxy Request to be Served by:**
/opr-web/*	http://[Virtual Host for Application Users]/opr-web/* https://[Virtual Host for Application Users]/opr-web/*
/OVPM/*	http://[Virtual Host for Application Users]/OVPM/* https://[Virtual Host for Application Users]/OVPM/*
/rumproxy/*	http://[Virtual Host for Application Users]/rumproxy/* https://[Virtual Host for Application Users]/rumproxy/*
/topaz/*	http://[Virtual Host for Application Users]/topaz/* https://[Virtual Host for Application Users]/topaz/*
/TopazSettings/*	http://[Virtual Host for Application Users]/TopazSettings/* https://[Virtual Host for Application Users]/TopazSettings/*
/tv/*	http://[Virtual Host for Application Users]/tv/* https://[Virtual Host for Application Users]/tv/*
/tvb/*	http://[Virtual Host for Application Users]/tvb/* https://[Virtual Host for Application Users]/tvb/*
/ucmdb-api/*	http://[Virtual Host for Application Users]/ucmdb-api/* https://[Virtual Host for Application users]/ucmdb-api/*
/ucmdb-ui/*	http://[Virtual Host for Application Users]/ucmdb-ui/* https://[Virtual Host for Application users]/ucmdb-ui/* Note: If you are using a Reverse Proxy and you have an integration with HP Universal CMDB, make sure your reverse proxy timeout setting is at least 1000 seconds. For example, in your reverse proxy http.conf file, modify the line that starts with ProxyPass as follows: ProxyPass /ucmdb-ui http://<my BSM GW server>/ucmdb-ui connectiontimeout=1000 timeout=1000
/uim/*	http://[Virtual Host for Application Users]/uim/* https://[Virtual Host for Application Users]/uim/*
/webinfra/*	http://[Virtual Host for Application Users]/webinfra/* https://[Virtual Host for Application Users]/webinfra/*

Reference - Support for BSM Data Collectors

The following table can be used as a reference for data collectors to connect through the reverse proxy.

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/topaz/topaz_api/*	http://[Virtual Host for Data Collectors]/topaz/topaz_api/* https://[Virtual Host for Data Collectors]/topaz/topaz_api/*
/topaz/sitescope/*	http://[Virtual Host for Data Collectors]/topaz/sitescope/* https://[Virtual Host for Data Collectors]/topaz/sitescope/*
/ext/*	http://[Virtual Host for Data Collectors]/ext/* https://[Virtual Host for Data Collectors]/ext/*
/cm/*	http://[Virtual Host for Data Collectors]/cm/* https://[Virtual Host for Data Collectors]/cm/*
/mam-collectors/*	http://[Virtual Host for Data Collectors]/mam-collectors/* https://[Virtual Host for Data Collectors]/mam-collectors/*
/tv/*	http://[HP TransactionVision UI/Job Server]: 21000/tv/* https://[HP TransactionVision UI/Job Server]: 21001/tv/* **Note:** If you want to use AJP to enable the Reverse Proxy server to communicate with the HP TransactionVision UI/Job Server, use the following: http://[HP TransactionVision UI/Job Server]: 21002/tv/*
/axis2/*	http://[Virtual Host for Data Collectors]/axis2/* https://[Virtual Host for Data Collectors]/axis2/* **Note:** Required if SOAP adaptor is used with embedded Run-time Service Model (RTSM) for replication into secure BSM via reverse proxy.

Note:

- Make sure your reverse proxy supports priority handling logic, which enables a specific expression to be handled before a more generic one, if required. For example, the **/topaz/topaz_api/*** expression must be handled before the **/topaz/*** expression.
- For some reverse proxies, a reverse pass is also required. The reverse pass changes the HTTP or HTTPS headers returned from the server to relative headers. For an example of a reverse pass, see "Configuring Apache to Work as a Reverse Proxy " on page 45.

Configuring a Reverse Proxy - IIS

This section contains the procedure describing how to configure a reverse proxy using an IIS web server. Procedures describing steps that are performed in products other than BSM are only for example purposes.

Note: Securing access to the reverse proxy should be performed as part of the Hardening Workflow. For details, see *Hardening Workflow* in the Hardening Guide.

This section contains:

Configure IIS to Work as a Reverse Proxy

This procedure may differ depending on your version of IIS.

For example:

1. Install the Application Request Routing (ARR) extension. For details, see http://www.iis.net/downloads/microsoft/application-request-routing.
2. Open the IIS Manager.
3. Create a new IIS web site, or use the default web site.
4. Create a new IIS Server Farm named BSM.
   a. Add a new server to the farm with the IP of your BSM Gateway server.
   b. When prompted, allow it to create a URL rewrite rule.
5. Enable IIS to function as a proxy.
   a. Select the main tree node (server name) > Application Request Routing Cache > Server Proxy Settings.
   b. Check the **Enable proxy** box.
   c. Set the **HTTP version** to **Pass through**.

   d. Check the **Reverse rewrite host in response headers** box.

   e. Click **Apply**.

6. Verify reverse proxy points to BSM

   Go to http://<Reverse Proxy FQDN>/topaz - verify that you see the BSM login page. At this point, if you enter your credentials you would see an empty page because BSM is not yet configured to work with a reverse proxy.

Configure IIS Reverse Proxy to Work with SSL

Note: Securing access to the reverse proxy should be performed as part of the Hardening Workflow. For details, see *Hardening Workflow* in the Hardening Guide.

1. Establish trust on the reverse proxy to the CA that issued the server certificate.

   Import the CA root certificate of the authority that issued the server certificate for this server into the computer truststore using mmc.

   For example:

   a. From the reverse proxy, open the Microsoft Management Console (**Run > mmc**).

   b. Add a snapin (**File > Add / Remove snapin**).

   c. Select Certificates and click **Add**.

   d. Select Computer Account and click **Next**.

   e. Select Local Computer and click **Finish**.

   f. Click **OK**.

   g. Import the certificate.

      Import ca.cer into the Trusted Root Certificate Authorities list.

2. Import the server certificate to the Microsoft Management Console.

   Import the server certificate you obtained earlier into Personal > Certificates in the Microsoft Management Console.

3. Enable SSL on IIS

For example:

a. In the IIS Manager, select your web site.

b. In the actions pane, select **Bindings**

c. Add an HTTPS binding for port 443

d. Specify your server certificate in the SSL Certificate field.

4. Configure the Reverse Proxy to Require SSL.

   For example:

   a. In the IIS Manager, select your web site, and select **SSL settings**.

   b. Check the **Require SSL** checkbox.

5. Configure SSL Offloading.

   If your SSL terminates on the reverse proxy, perform the following steps:

   a. Run the following command to configure IIS to allow large data samples (1 MB) to pass through:

      C:\Windows\System32\inetsrv>appcmd.exe set config -section:system.webserver/serverruntime /uploadreadaheadsize:1048576 /commit:apphost

   b. In the ISS Manager, Select the main tree node (server name) > Application Request Routing Cache > Server Proxy Settings.

   c. Check the **enable SSL offloading** checkbox.

Configure IIS to Require Client Authentication – Optional

1. Recreate the SSL binding to enable client negotiation.

   The previous binding will function, but may have performance issues. This binding enables negotiation, thereby increasing performance when using client authentication.

   a. Remove the current binding using the IIS manager user interface.

   b. Run the following commands from the IIS server:

      c:\windows\system32\inetsrv\appcmd set site /site.name:"Default Web Site" /+bindings.[protocol='https',bindingInformation='*:443:']

netsh http add sslcert ipport=0.0.0.0:443 certhash=<your server certificate hash> appid={00112233-4455-6677-8899-AABBCCDDEEFF} clientcertnegotiation=enable

> **Note:** You can find the certificate hash from mmc by viewing the thumbprint in the details of the certificate.

2. Configure the Reverse Proxy to Require a Client Certificate.

   For example:

   a. In the IIS Manager, select your web site, and select **SSL settings**.

   b. In **Client certificates**, select **Require**.

3. Specify the header the reverse proxy passes to BSM for client certificate authentication in base64 format.

   For example:

   a. From the IIS manager, select your farm and select **Proxy**.

   b. Select the checkbox **Reverse rewrite host in response header**.

   c. In the field **forward encoded client certificate in the following header**, enter the header name **CLIENT_CERT_HEADER**.

   d. Click **Apply**.

Additional Required Configurations for some Data Connections

1. Install Visuall C++ redistributable package.

   Install Visual C++ redistributable package on the reverse proxy. For details, see http://answers.microsoft.com/en-us/windows/forum/windows_7-windows_programs/trying-to-open-computer-management-the-program/5c9d301a-2191-4edb-916e-5e4958558090.

2. Install L-Core/BBC on the IIS SRP:

   Copy HPSharedComp.msi from the packages folder on the BSM installation media to the SRP system and install by double-clicking.

3. On the IIS SRP run the following command:

   ovc –start

4. On the IIS SRP run the following command:

   ```
   netstat –an
   ```

   Select a port NOT in use. This selected free port is referenced in the next lines as **<port>**.

5. In a command shell on the IIS SRP run the following command:

   ```
   ovconfchg –ns sec.cm.client –set CERTIFICATE_SERVER <FQDN of BSM GW Server or Load Balancer if you have one>
   ```

6. In a command shell on the IIS SRP run the following command:

   ```
   ovcert –certreq
   ```

7. On BSM grant the certificate request:

   a. In the BSM UI navigate to **Admin > Operations Management > Setup > Certificate Requests** and grant the certificate request from the IIS SRP.

      Alternatively you can perform this procedure in the command line as follows:

      On the DPS run **ovcm -listpending**. Then run **ovcm –grant <ID>** where **<ID>** is the result of the previous command.

   b. Verify that the certificate is installed correctly by running the following command on the IIS SRP:

      ```
      ovcert –list
      ```

      If the list is not empty the certificate was installed successfully.

8. On the IIS SRP, run the following commands where <RCP IP address> is the IP address of the IIS SRP server:

   ```
   ovconfchg -ns bbc.rcp -SERVER_PORT <port>
   ```

   For example: ovconfchg -ns bbc.rcp -set SERVER_PORT 9383

   ```
   ovconfchg -ns bbc.http -set PROXY <RCP IP address>:<port>+(*)-(<RCP IP address>)
   ```

   For example: ovconfchg -ns bbc.http -set PROXY 192.168.254.5:9383+(*)-(192.168.254.5)

   Note: Use the same port as the previous command.

   ```
   ovcreg -add "%OVDATADIR%\conf\bbc\ovbbcrcp.xml"
   ```

   ```
   ovc -start
   ```

9. On all BSM GW servers, run the following commands:

   ```
   ovconfchg -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS true
   ```

   ```
   ovconfchg -ns bbc.cb -set RC_CHANNELS <RCP IP address>:<port>
   ```

   ```
   ovconfchg -ns bbc.http -set PROXY <RCP IP address>:<port>+(*)-(<RCP IP address>,<DPS FQDN>,<DPS short hostname>)
   ```

   > **Note:** Use the same port as the previous steps.

10. On every server that will remotely connect to the BSM environment (agents, Diagnostics server, SiteScope server using event integration, HPOM, other BSM/OMi, etc.), run the following commands:

    ```
    ovconfchg -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS true
    ```

    ```
    ovconfchg -ns bbc.cb -set RC_CHANNELS <RCP IP address>:<port>
    ```

    ```
    ovconfchg -ns bbc.http -set PROXY <RCP IP address>:<port>+(*)-(<RCP IP address>)
    ```

    Configure the agent according to the relevant documentation (SiS, Diagnostics, BSM Connector, Integration Adapter, …) to get the relevant certificates. If this does not work out, use the following procedure to manually install the certificates on the agent system:

    a. On the agent node run the following command:

       ```
       ovcoreid
       ```

       Remember the output. We will refer to the output in the next few steps as <coreid>.

    b. On the BSM DPS run the following command:

       ```
       ovcm –issue –file <nodename>.cer –node <FQDN of agent node> -coreid <coreid>
       ```

       Select a password and remember it.

    c. Copy the created file to the agent node.

    d. On the agent node run the following command:

       ```
       ovcert –importcert –file <nodename>.cer
       ```

       Provide the password you selected earlier.

    All message targets on these systems should target the Load Balancer if it exists, or specify one BSM GW server.

For example, the message target in the flex manager forwarding policy of the HPOM system the forwarding target must be: ‘OPCMGR IP 0.0.0.0 "<BSM GW Server>", or “<LoadBalancer>, if available.

11. Verify that the configuration was successful.

    a. On a BSM GW server run the following command:

       bbcutil –ping <FQDN of SiS, Diag, BSMC, HPOM, HPOM Agent> - ovrg server

    b. On a remote system (SiS, Diag, BSMC, HPOM, HPOM Agent) run the following command:

       bbcutil –ping <FQDNof BSM GW server or Load Balancer if used>

    Each command should return **eServiceOK** if the configuration was successful.

HP BSM Specific Configuration

In addition to configuring the reverse proxy to work with BSM, you must configure BSM to work with the reverse proxy.

Note: BSM must be configured only if application users are connected via a reverse proxy to BSM. If the reverse proxy is being used for data collectors only, skip the instructions in this section.

To configure BSM to work with the reverse proxy:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. Click **Foundations** and select the **Platform Administration** context from the drop-down box.

2. In the Platform Administration - Host Configuration pane, set the following parameters:

   - **Default Virtual Gateway Server for Application Users URL and Default Virtual Gateway Server for Data Collectors URL.** Verify that these parameters represent the URL of the machine (reverse proxy, load balancer, or other type of machine) used to access the Gateway server machine. For example, `http://my_reverse_proxy.example.com:80`.

     If you are using a NAT device to access the Gateway server, enter the full URL of the NAT device. For example, `http://nat_device.example.com:80`.

     Local Virtual Gateway Server for Application Users URL and Local Virtual Gateway Server for Data Collectors URL (optional). If you must use more than one URL (the ones defined for the Default Virtual Server URLs, above) to access the Gateway server machine, define a Local Server URL for each machine through which you want to access the Gateway server machine. For example, `http://my_specific_virtual_server.example.com:80`.

If the **Local Virtual Services Server URL** parameter is defined for a specific machine, this URL is used instead of the **Default Virtual Services URL** for the specifically-defined machine.

- **Direct Gateway Server for Application Users Server URL**. Click the **Edit** button and delete the URL in the **value** field.
- **Direct Gateway Server for Data Collectors URL**. Click the **Edit** button and delete the URL in the **value** field.

3. In the Reverse Proxy Configuration pane, set the following parameters:

    - **Enable Reverse Proxy**. Set this parameter to true. Note that this must be done after the above parameters have been configured.
    - **HTTP or HTTPS Reverse Proxy IPs** . Enter the internal IPs the reverse proxies or load balancers used to communicate with the Gateway server machine.

        - If the IP address of the reverse proxy sending the HTTP/S request is included, the URL returned to the client is either the Default Virtual Server URL or the Local Virtual Server URL (when defined).
        - If no IP addresses are defined for this parameter (not recommended), BSM works in Generic Mode. This means that you will only be able to log into BSM using the Virtual URL and not directly to the Gateway.

    > **Note:** If your reverse proxy and BSM Gateway Servers are not in the same domain, you must add the IP of the reverse proxy to the **HTTP or HTTPS Reverse Proxy IPs** parameter. For more details, see "LW-SSO Configuration for Multi-Domain and Nested Domain Installations" in the BSM Platform Administration Guide.

    To find the internal IP of your reverse proxy or load balancer:

    - Log in to BSM through the reverse proxy or load balancer.
    - Open the log in the following location **<BSM Gateway Server>\log\EJBContainer\UserActionsServlet.log**.
    - The IP that appears in the latest **login** line in this log is the reverse proxy or load balancer IP. The entry should have your user name.

4. Increase the reverse proxy timeout.
5. Restart the HP BSM service on the BSM Gateway and Data Processing servers.

> **Note:** After you change the BSM base URL, it is assumed that the client is initiating HTTP or HTTPS sessions using the new base URL. You must therefore ensure that the HTTP or HTTPS channel from the client to the new URL is enabled.

Enabling BSM to Configure Multiple Reverse Proxies

To enable BSM to configure multiple reverse proxies:

1. In BSM, select **Admin > Platform > Setup and Maintenance >Infrastructure Settings**.
2. Select > **Foundations**.
3. Select **Platform Administration**.
4. In the Platform Administration - Host Configuration table, locate **Default Virtual Gateway Server for Application Users URL** and edit the value by adding a list of reverse proxy URLs with their port number. Separate the items in this list with semicolons.
5. Click **Save**.
6. In the Platform Administration - Reverse Proxy Configuration table, locate **HTTP Reverse Proxy IPs** and edit the value to list all the reverse proxy IP addresses separated by semicolons. If a specific reverse proxy has more than one IP address, list all of its IP addresses separated by commas.

   For example:

   <RevProxy1_IP1,RevProxy1_IP2;RevProxy2_IP1,RevProxy2_IP2;...;RevProxyN_IP1,RevProxyN_IP2>

   In this example, different delimiters (comma or semicolon) are used to indicate whether an IP address belongs to the same reverse proxy or to the next one.
7. Click **Save**.
8. In the Platform Administration - Reverse Proxy Configuration table, locate **Enable Reverse Proxy** and set the value to **true**.
9. Click **Save**.
10. Restart BSM.

Notes and Limitations

BSM requires your reverse proxy to have a timeout of at least 300 seconds. This is the default for some versions of Apache, but it may have been reduced. For some processes such as installing a content pack, the timeout should be as high as 1000 seconds (see "Configuring Apache to Work as a Reverse Proxy " on page 45).

If you configured BSM to work in Generic Mode, all the BSM clients must access the BSM machine via the reverse proxy.

Specific and Generic Reverse Proxy Mode Support for BSM

BSM servers reply to application users by sending a base URL that is used to calculate the correct references in the HTML requested by the user. When a reverse proxy is used, BSM must be configured to return the reverse proxy base URL, instead of the BSM base URL, in the HTML with which it responds to the user.

If the reverse proxy is being used for data collectors only, configuration is required only on the data collectors and reverse proxy, and not on the BSM server(s).

There are two proxy modes that control user access to BSM servers:

- "Specific Mode" below.
- "Generic Mode" below.

Specific Mode

This mode should be used if you want to concurrently access BSM servers through specific reverse proxies and by direct access. Accessing the server directly means that you are bypassing the firewall and proxy because you are working within your intranet.

If you are working in this mode, each time an application user's HTTP/S request causes BSM to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Gateway Server URL** or the **Local Virtual Gateway Server URL** (when defined), if the HTTP/S request came through one of the IP addresses defined for the **HTTP** or **HTTPS Reverse Proxy IPs** parameter. If the HTTP/S request did not come through one of these IP addresses, the base URL that BSM receives in the HTTP/S request is the base URL that is returned to the client.

Generic Mode

This mode is used when you try to access the Gateway server via the reverse proxy. Any URLs requested are rewritten and sent back with the virtual IP of the Gateway server.

If you are working in this mode, each time an HTTP/S request causes the BSM application to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Gateway Server URL** or the **Local Virtual Gateway Server URL** (when defined).

Note that when using this mode, you must ensure that all BSM clients are accessing the BSM servers via the URL defined for the **Default Virtual Gateway Server URL** or the **Local Virtual Gateway Server URL** parameters.

Chapter 6: Install and Configure Additional Components

For an end-to-end, high-level workflow for setting up BSM, as well as details about BSM components and concepts, see the BSM Getting Started Guide, available as part of the BSM Help.

Use the following references to install and configure additional components:

Item	Resource
BSM Platform	To configure the BSM platform, see the BSM Platform Administration Guide, available as part of the BSM Help.
BSM Integrations	Information about integrations between BSM and other products can be found on the HP Software Integrations site: http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3.
BSM Components	• **Real User Monitor:** See the Real User Monitor Installation and Upgrade Guide. • **Business Process Monitor:** See the Business Process Monitor Deployment Guide. • **SiteScope:** See the HP SiteScope Deployment Guide. • **TransactionVision:** See the TransactionVision Deployment Guide. • **Diagnostics:** See the Diagnostics Installation and Configuration Guide. • **Service Health Analyzer PA/NNM Data Collector:** See the Service Health Analyzer PA/NNM Data Collector Installation Guide. • **System Health:** See the System Health Guide. • **BSM Connector:** See the BSM Connector Installation and Upgrade Guide. • **Data Flow Probe:** See the Data Flow Probe Installation Guide.

You can access the above resources in the following locations:

- The Planning and Deployment Guides page: Can be found on the BSM installation root directory (**Get_documentation.htm**), or from BSM, go to **Help > Planning and Deployment Guides**.
- The Downloads Page: **Admin> Platform > Setup and Maintenance > Downloads**.
- The HP Software Support site https://softwaresupport.hp.com.

Part II: Appendixes

Appendix A: 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 91.

> **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 B: 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 91.

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 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 26.

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 84.

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 138. 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 91.

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 26.

   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 26.

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.

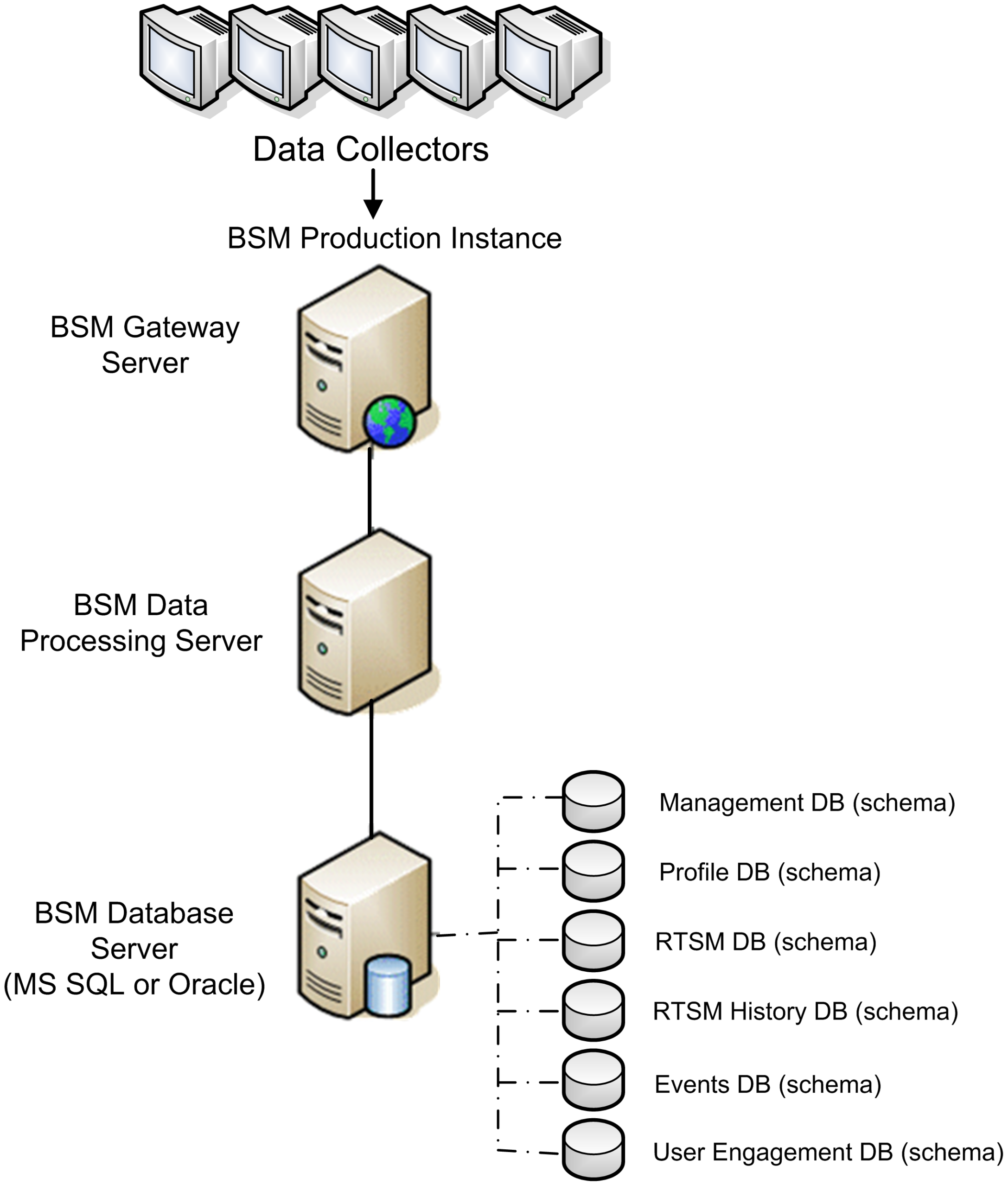
To remove password encryption, enter the passwords in the response file normally and set the value of **IsEncrypted="false"**.

Chapter E: Disaster Recovery for BSM

Introduction to Disaster Recovery for BSM

You can set up and activate (when necessary) a Disaster Recovery system for your BSM system.

The following describes the basic principles and guidelines on how to set up a Disaster Recovery system, and the required steps to make the Secondary BSM system become the new Primary BSM system.



Note:

- Disaster Recovery involves manual steps in moving various configuration files and updates to the BSM database schemas. This procedure requires at least one BSM Administrator and one database administrator, who is familiar with the BSM databases and schemas.
- There are a number of different possible deployment and configurations for BSM. To validate that the disaster recovery scenario works in a particular environment, it should be thoroughly tested and documented. You should contact HP Professional Services to ensure best practices are used in the design and failover workflow for any disaster recovery scenario.
- A disaster recovery machine must use the same operating system and root directory as the original environment.

Preparing the Disaster Recovery Environment

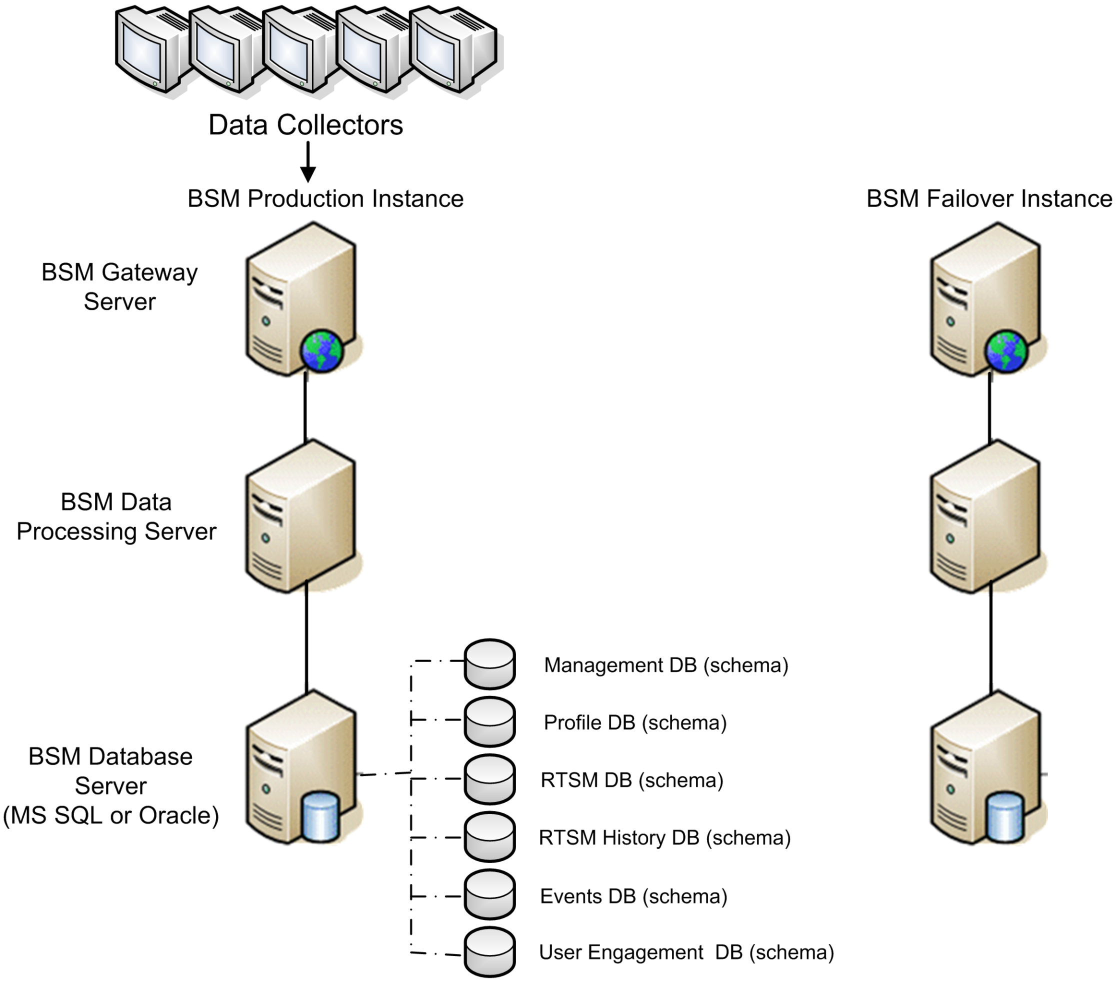
Preparing the Disaster Recovery environment by performing the following steps:

1. Install a set of BSM servers

   Install a second instance of BSM that matches your current production environment.

   - Install exactly the same version of BSM in your backup environment as that used in your production environment.
   - The backup environment should be the same as your production environment (for example, one- or two-machine deployment, similar hardware), unless you have more than one GW or DPS in your production environment. In that case, you only need to create one set of BSM servers (one GW and one DPS or one one-machine) as your disaster recovery environment.
   - The backup environment must use the same operating system and installation directory as the original environment.
   - Do not run the Server and Database Configuration utility and do not create any databases or enable the servers.

   The following diagram shows a typical BSM environment with a Failover system also installed:



2. Copy configuration files from the original system

Copy files you manually modified in any of the following directories from the BSM Production instance to the same server type in the Failover instance:

- odb/conf
- odb/content/
- BLE/rules/<custom rules>.jar

If you used User Reports to create Excel reports, you must manually copy these to the Failover Instance. The reports are stored in the **<Gateway Server>\HPBSM\AppServer\webapps\site.war\openapi\excels\** directory in folders for each customer ID.

Also copy any other files or directories in the system that you have customized.

> **Note:** It is recommended to have at least daily backups of BSM servers. Depending on the amount and interval of configuration changes, it may be necessary to incorporate a faster interval to prevent a large loss of configuration changes in the event of losing the Production instance.

3. Configure the Backup database

Replicate the original database. The original database can now be used as a backup, and the replicated database will be used as the primary database.

> **Note:** HP recommends that only an experienced database administrator perform this phase of the Disaster Recovery scenario.

- **Microsoft SQL–configure database logfile shipping**

  To provide the most up to date monitoring and configuration data, it is critical to enable log file shipping to minimize the time in data gaps. By using log file shipping you can create an exact duplicate of the original database – out of date only by the delay in the copy-and-load process. You then have the ability to make the standby database server a new primary database server, if the original primary database server becomes unavailable. When the original primary server becomes available again, you can make it a new standby server, effectively reversing the servers roles.

  The log file shipping needs to be configured for the following BSM databases:

  - Management
  - RTSM
  - RTSM History
  - Event
  - User Engagement Schema
  - Profile (all databases)
  - Analytic (if it exists)

  For details about how to configure log file shipping for Microsoft SQL, refer to the appropriate Microsoft SQL documentation.

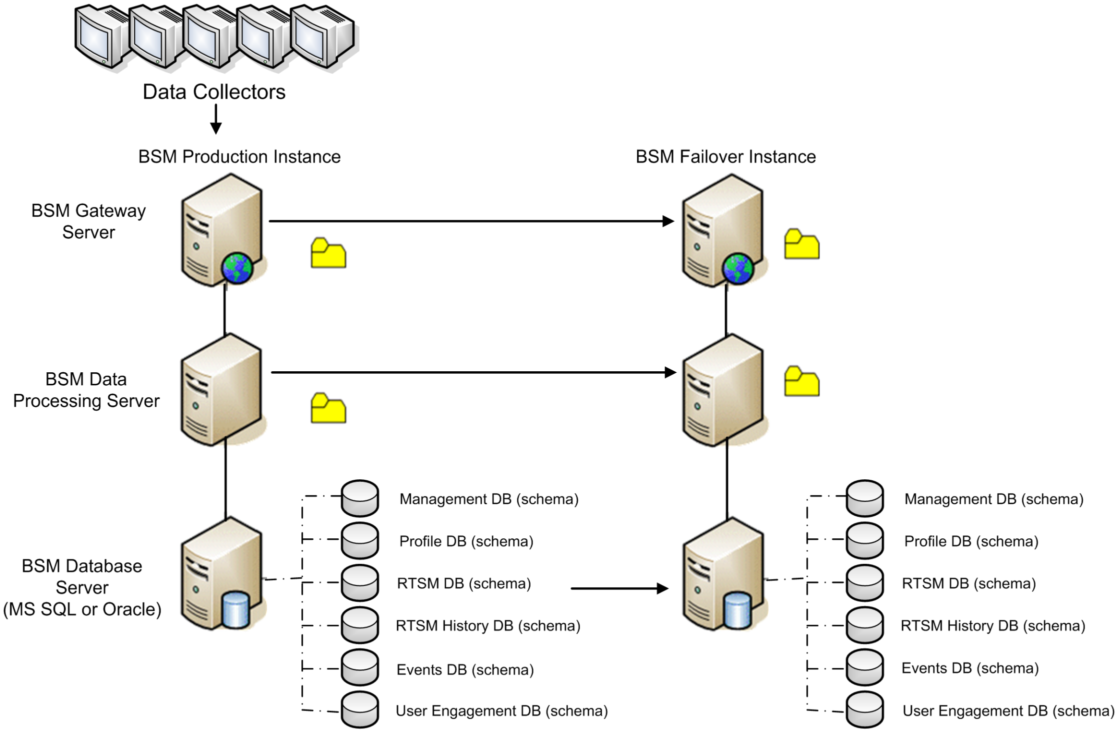
- **Oracle–configure the Standby database (Data Guard)**

Oracle does not have logs for each schema, but only on a database level, which means that you cannot make a standby database on the schema level and must create copies of the production system databases on your backup system.

For details about how to configure a Standby database, refer to the appropriate Oracle documentation.

Upon successful completion of the Backup database configuration, the BSM Failover Database should be in sync with the BSM Production Database.

The following diagram shows the production and Failover systems with database logfile shipping enabled:



Cleanup Procedure

Now that you have replicated the original environment, certain settings must be manually modified to avoid confusion between the original environment and the new environment. This procedure cleans up all the machine-specific references in the configurations from the Production instance.

> **Note:**
>
> - Before starting the activation procedures, the BSM Administrator should ensure that the appropriate license has been applied to the Failover instance and that all the available data collectors can communicate with the Failover instance.
> - HP recommends that an experienced database administrator perform the SQL statements included in this procedure.
> - The SQL statements below to be run against the management database except for the last 2 steps. The SQL statements in the last 2 steps needs to be run against the RTSM database and the Event database respectively.

1. Delete old information from High Availability (HA) tables.

   Run the following queries on the management database of the disaster recovery environment:

   - **delete from HA_ACTIVE_SESS**
   - **delete from HA_BACKUP_PROCESSES**
   - **delete from HA_PROC_ALWD_SERVICES**
   - **delete from HA_PROCESSES**
   - **delete from HA_SRV_ALLWD_GRPS**
   - **delete from HA_SERVICES_DEP**
   - **delete from HA_SERVICES**
   - **delete from HA_SERVICE_GRPS**
   - **delete from HA_TASKS**
   - **delete from HA_SERVERS**

2. Run the following query on the management database of the DR environment:

   Delete from PROPERTIES where NAME = 'HAServiceControllerUpgrade'

3. Switch references in the Sessions table on the management database of the DR environment to the backup databases.

   a. Run the following query to retrieve all database names:

      SELECT * FROM SESSIONS

      where SESSION_NAME like '%Unassigned%'

   b. Update the following columns in each received row with the following values:

      - **SESSION_NAME:** Replace with the new restored database name (only where SESSION_NAME is like '%Unassigned%'). Use the following script:

        UPDATE SESSIONS set SESSION_NAME='Unassigned<NEW_DB_Server_name><NEW_schema_name><DB_User_name>'

        WHERE SESSION_NAME='Unassigned<OLD_DB_Server_name><OLD_schema_name><old_DB_User_name>'

      - **SESSION_DB_NAME:** Replace with the new restored schema name. Use the following script:

        UPDATE SESSIONS set SESSION_DB_NAME='<<NEW_schema_name>'

        WHERE SESSION_DB_NAME='<OLD_schema_name>'

      - **SESSION_DB_HOST:** Replace with the new restored database host name. Use the following script:

        UPDATE SESSIONS set SESSION_DB_HOST='<<NEW_host_name>'

        WHERE SESSION_DB_HOST='<OLD_host_name>'

      - **SESSION_DB_PORT:** Replace with the new restored port name. Use the following script:

        UPDATE SESSIONS set SESSION_DB_PORT='<NEW_port_name>'

        WHERE SESSION_DB_PORT='<OLD_port_name>'

      - **SESSION_DB_SID:** Replace with the new restored session ID name. Use the following script:

        UPDATE SESSIONS set SESSION_DB_SID='<<<NEW_SID_name>>>'

        WHERE SESSION_DB_SID='<<<OLD_SID_name>>>'

- **SESSION_DB_UID:** Replace with the new restored name. Use the following script:

  ```
  UPDATE SESSIONS set SESSION_DB_UID='<NEW_UID_name>'

  WHERE SESSION_DB_UID='<OLD_UID_name>'
  ```

- **SESSION_DB_SERVER:** Replace with the new restored server name. Use the following script:

  ```
  UPDATE SESSIONS set SESSION_DB_SERVER='<NEW_server_name>'

  WHERE SESSION_DB_SERVER='<OLD_server_name>'
  ```

4. Switch references in the Analytics table on the management database to the backup databases.

   a. Run the following query to retrieve all database names:

      SELECT * FROM ANALYTICS_DATABASES

   b. Update the following columns in each received row with the following values:

      - **DB_HOST:** Replace with the new restored database host name. Use the following script:

        ```
        update ANALYTICS_DATABASES set DB_HOST=”NEWDatabasehostname’ where DB_HOST=”OLDDatabasehostname”;
        ```

      - **DB_SERVER:** Replace with the new restored server name. Use the following script:

        ```
        update ANALYTICS_DATABASES set DB_SERVER=’ NEWDatabaseServerName” where DB_SERVER=’ OLDDatabaseServerName’’
        ```

      - **DB_SID:** Replace with the new restored session ID name. Use the following script:

        ```
        update ANALYTICS_DATABASES set DB_SID =’NEWSID’’ where DB_SID='OLDSID';
        ```

      - **DB_PORT:** Replace with the new restored port name. Use the following script:

        ```
        update ANALYTICS_DATABASES set DB_PORT= NewPort where DB_PORT=OldPort
        ```

5. Delete bus cluster info from PROPERTIES table on the management database.

   Run the following query:

   Delete from PROPERTIES where

   NAMESPACE='MessageBroker' or NAMESPACE='SonicMQ_Namespace' or NAMESPACE='BrokerName' or NAMESPACE like 'hornetq-%'

6. Delete machines from Deployment table on the management database.

   Run the following query:

   DELETE from DEPLOY_HW

7. Setting Manager Values of **SETTING_PARAMETERS** table on the management database.

   Update the URLS and LDAP Server in the SETTING_PARAMETERS table.

   The following table shows the keys in the Setting Manager table that need to be updated if they are present:

SP_CONTEXT	SP_NAME	Description
opr	opr.cs.host	IP address of the new primary Data Processing server (used to handle certificate requests)
platform	settings.smtp.server	Name of the SMTP server used for the alert engine
scheduledreports	settings.smtp.server	Name of the SMTP server used for scheduled reports
platform	default.core.server.url	The URL used by data collectors to access the Gateway server in BSM
platform	default.centers.server.url	The URL used by users to access BSM
opr	opr.db.connection.dbname	Name of the event schema. The login and password for this database should be reconfigured during database configuration via the Configuration Server wizard.
opr	opr.db.connection.host	Host name where event schema is located. The login and password for this database should be reconfigured during database configuration via the Configuration Server wizard.
opr	opr.exc.db.connection.dbname	Name of the User Engagement schema. The login and password for this database should be reconfigured during database configuration via the Configuration Server wizard.

SP_CONTEXT	SP_NAME	Description
opr	opr.exc.db.connection.host	Host name where User Engagement schema is located. The login and password for this database should be reconfigured during database configuration via the Configuration Server wizard.
platform	virtual.centers.server.url	
platform	virtual.core.server.url	

For each key in the table, modify and run the following query:

update SETTING_PARAMETERS set SP_VALUE='<new value>'

where SP_CONTEXT='<context value>' and SP_NAME='<name value>'

As follows:

- update SETTING_PARAMETERS set SP_VALUE='<IP of new primary DPS>' where SP_CONTEXT='opr' and SP_NAME='opr.cs.host'
- update SETTING_PARAMETERS set SP_VALUE='<newmachinename>' where SP_CONTEXT='platform' and SP_NAME='settings.smtp.server'
- update SETTING_PARAMETERS set SP_VALUE='<newmachinename>' where SP_CONTEXT='scheduledreports' and SP_NAME='settings.smtp.server'
- update SETTING_PARAMETERS set SP_VALUE='http://<newmachinename>:80' where SP_CONTEXT='platform' and SP_NAME='default.core.server.url'
- update SETTING_PARAMETERS set SP_VALUE='http://<newmachinename>:80' where SP_CONTEXT='platform' and SP_NAME='default.centers.server.url'

The last two settings in the table above do not need to be updated unless you are using a load balancer or a reverse proxy. In that case, update the settings as follows:

- update SETTING_PARAMETERS set SP_VALUE='http://<Load Balancer or Reverse Proxy>:80' where SP_CONTEXT='platform' and SP_NAME='virtual.centers.server.url'
- update SETTING_PARAMETERS set SP_VALUE='http://<Load Balancer or Reverse Proxy>:80' where SP_CONTEXT='platform' and SP_NAME='virtual.core.server.url'

8. Update SYSTEM Keys.

   Update the following keys in the SYSTEM table on the management database:

AdminServerURL	http://<DPS1>:port	By default, there is no port number.
GraphServerURL	http://<GW1>/topaz/	
GraphServerURL4.5.0.0	http://<GW1>/topaz/	
application.tac.path	http://<GW1>:port/AdminCenter	By default, the port number is 80.
application.flipper.path	http://<GW1>:port/monitoring	By default, the port number is 80.

For each value in the table, modify and run the following query:

update SYSTEM set SYS_VALUE='<new value>' where SYS_NAME='<key>'

where **<new value>** is the new URL in the format of the original URL.

For example:

update SYSTEM set SYS_VALUE='http://<newmachine>:port' where SYS_NAME='AdminServerURL'

Note: The default port number is 80.

9. Empty and update tables on the RTSM database.

   This procedure cleans up all the machine-specific references in the RTSM configuration tables.

   Run the following SQL statements against the RTSM database:

   - **update CUSTOMER_REGISTRATION set CLUSTER_ID=null**
   - **truncate table CLUSTER_SERVER**
   - **truncate table SERVER**
   - **truncate table CLUSTERS**

10. Delete old server information from the Certificate Server Authority tables.

    Run the following query on the Event database:

    delete from CSA_SERVERS

11. Delete the old server information from the User Engagement Runtime Server table on the User Engagement database by running the following query on the User Engagement database:

    Delete from EXC_RUNTIME_SERVER

Configure the New Environment

1. ## Run the Server and Database Configuration utility

   Run the Server and Database Configuration utility on each machine to re-initialize the needed tables in the database. To run the Server and Database Configuration utility, select **Start > Programs > HP Business Service Management > Administration > Configure HP Business Service Management.**

   > **Note:** When running the Server and Database Configuration utility, make sure to reconnect to the same databases that were created for the Failover environment (that is, the one to which the backup data was shipped). Possible complete loss of configuration data will result if trying to run this on the Production instance.
   >
   > Run the Server and Database Configuration utility on the machines in the same order that BSM was originally installed in the failover environment.

2. ## Enable BSM

   Enable BSM on the new servers.

3. ## Run the Post Startup Cleanup procedure to disable any obsolete hosts that are not part of the Failover instance

   To disable obsolete hosts:

   a. In BSM, go to **Admin > Platform > Seup and Maintenance > Server Deployment** and select **To Disable Machine**.

   b. Disable any obsolete hosts.

4. ## Repeat Hardening Procedures (optional)

   If your original environment was hardened, you need to repeat the hardening procedures on the new environment.

   The reverse proxy procedures do not have to be repeated.

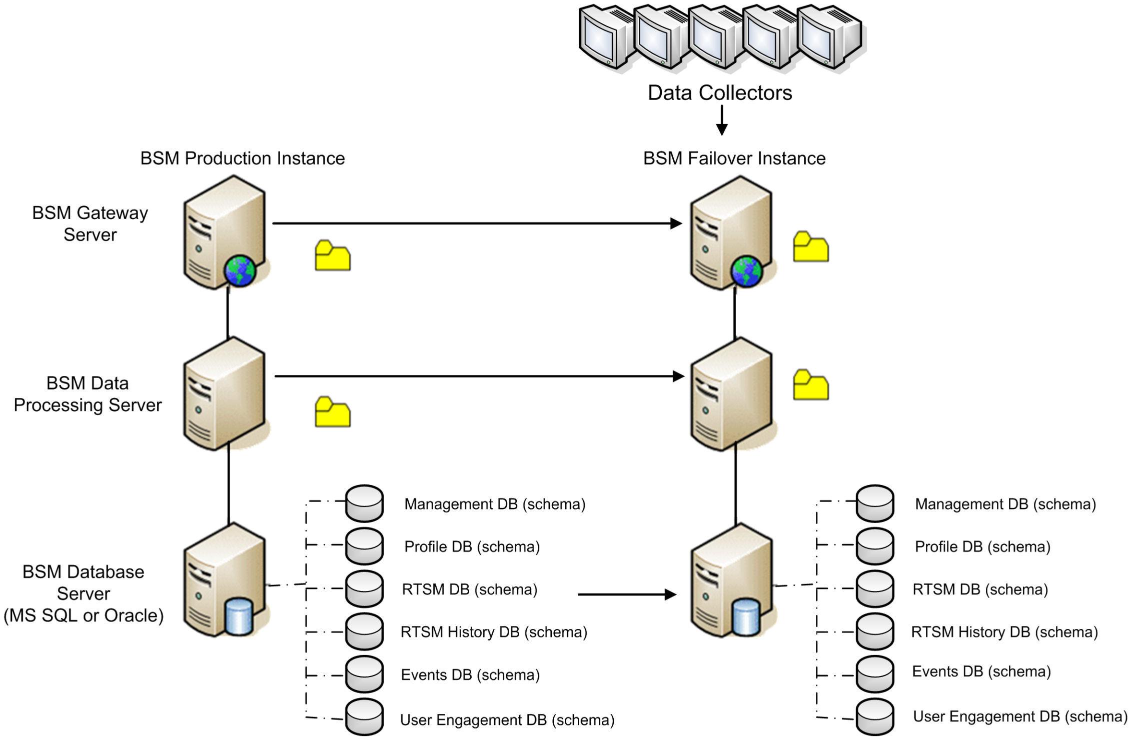
   For details, see the BSM Hardening Guide.

Configure Data Collectors

1. **Configure data collectors.**

   Configure all the data collectors, including Business Process Monitor agents, Real User Monitor engines, SiteScopes, TransactionVision, HPOM, Service Manager, and Operations Orchestration (if installed on a separate server) to work with the Failover instance. For details, see the relevant documentation for each data collector.

The following diagram shows a fully activated Failover instance:



2. **Configuring failover data collector connections.**

   If any of the data collectors also experienced a failure and were moved to different machines, the new URLs must be communicated to the BSM servers. This is done in various applications in BSM. For example:

Data Collector	Procedure
SiteScope	Reconnect the SiteScope servers to the BSM server from the SiteScope console.
Business Process Monitor	Reconnect the BPM servers to the BSM server from the BPM console.
Real User Monitor	Reconnect the RUM servers to the BSM server from the RUM console.
Operations Manager	- Exchange certificates between your HPOM and BSM systems. - In BSM, go to the Infrastructure Settings for Operations Management: **Administration > Platform > Infrastructure Settings > Applications > Operations Management** In the **Operations Management – Certificate Server Settings** section, enter the IP address of the new primary Data Processing Server. In the **Operations Management – HPOM Topology Synchronization Connection Settings** section, check the connection settings for HPOM. If you switched your HPOM server, reconfigure all entries to reflect the details of the new HPOM server. If no settings are recorded, leave these fields empty, and go to the next step. - Open the Connected Servers manager and check the HPOM server connections as follows: **Administration > Operations Management >Tune Operations Management > Connected Servers** If you switched your HPOM server, reconfigure all entries to reflect the details of the new HPOM server. Use the **Test Connection** button to validate communication for the current settings, even if they have not been changed.

Data Collector	Procedure
Operations Manager (continued)	- In HPOM, change the Flexible Management Server Forwarding policy to specify the new BSM server as the target and deploy the new version to your HPOM management server node. - Change the destination server for receiving discovery (topology) data. For details, see described in "Topology Synchronization" in the OMi part of the BSM User Guide. - Restart the service, and in a Command Prompt window on the HPOM management server system, execute the command: **ovagtrep -publish** Topology data from the HPOM system should now be available in Operations Management. - Delete the buffered messages on the HPOM system for the old BSM server. It is not possible to re-direct these messages to the new BSM server, and these cannot be synchronized. Note: All messages currently in the buffer are deleted. It is not possible to distinguish between different targets and messages for other targets are also deleted.

Data Collector	Procedure
Operations Manager (continued)	**To delete the forwarding buffer files on HPOM for Windows:** a. Stop the server processes: **vpstat -3 -r STOP** b. Delete all files and folders contained within the following directories: **<OvDataDir>\shared\server\datafiles\bbc\snf\data** **<OvDataDir>\shared\server\datafiles\bbc\snf\OvEpMessageActionServer** c. Restart the server processes: **vpstat -3 -r START** **To delete the forwarding buffer files on HPOM for UNIX:** a. Stop the server processes: **ovc -kill** b. Delete all files and folders contained within the following directories: **/var/opt/OV/shared/server/datafiles/bbc/snf/data** **/var/opt/OV/share/tmp/OpC/mgmt_sv/snf/opcforwm** c. Restart the server processes: **ovc -start** **Note:** If the messages are left in the forwarding buffer, there may be some performance degradation as the system regularly tries to deliver them without success. They also consume some disk space.
HP Operations Orchestration	On the HP Operations Orchestration server, adopt the configuration to reflect the new BSM server according to the procedure described in the Solutions and Integrations guide.
HP Service Manager	On the HP Service Manager server, adopt the configuration to reflect the new BSM server according to the procedure described in the Solutions and Integrations guide.
TransactionVision	You must configure in both of the following: ■ Go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Applications** > **TransactionVision**. Change the setting of the URL that BSM uses to communicate with TransactionVision. ■ Go to **Admin > TransactionVision > HP Business Service Management Settings** page. Change the URL, protocol, and port that TransactionVision uses to communicate to BSM.

Data Collector	Procedure
SHA PA/NNM data collector	Reconnect the SHA PA/NNM data collector by re-running the configuration-wizard.

Appendix F: High Availability for BSM

This appendix contains the following topics:

Overview of High Availability Options

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

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

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

High availability is implemented in two layers:

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

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

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

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

Load Balancing for the Gateway Server

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

> **Note:** We recommend installing BSM behind a load balancer or reverse proxy. This enables additional security options and can simplify disaster recovery and upgrade procedures.

This section includes the following topics:

"Configuring Load Balancing" below

"Notes and Limitations" on page 120

Configuring Load Balancing

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

   The first host name is for accessing the BSM Web site on the Gateway Server. This URL can be distributed to BSM users. The second host name is for the data collectors to access the Gateway Server. This URL must be used when configuring data collectors to communicate with BSM.

2. Enter the relevant load balancer host names in the Infrastructure Settings for the virtual servers. To do so, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Foundations**, select **Platform Administration - Host Configuration table**:

   - **Default Virtual Gateway Server for Application Users URL.** Virtual host name for the BSM Web site. The Gateway Server you are working on must be able to resolve this Virtual IP address. This means that **nslookup** for the **virtual host name for the application users** should return name and IP address when executed on this Gateway Server.

   - **Default Virtual Gateway Server for Data Collectors URL.** Virtual host name for Data Collectors. All data collectors must be able to resolve this Virtual IP address. This means that **nslookup** for the **virtual host name for the Data Collectors** should return name and IP address when executed on data collector server.

3. In the Reverse Proxy Configuration pane, set the following parameters:

   - **Enable Reverse Proxy parameter = true.**

   - **HTTP Reverse Proxy IPs**

Add the internal IP addresses of the Load Balancers to this setting.

- If the IP address of the load balancer sending the HTTP/S request is included, the URL returned to the client is either the Default Virtual Server URL or the Local Virtual Server URL (when defined).

- If no IP addresses are defined for this parameter (not recommended), BSM works in Generic Mode. This means that you will only be able to log into BSM using the Virtual URL and not directly to the Gateway.

> **Note:** If your load balancer and BSM Gateway Servers are not in the same domain, you must add the IP of the reverse proxy to the **HTTP or HTTPS Reverse Proxy IPs** parameter. For more details, see "LW-SSO Configuration for Multi-Domain and Nested Domain Installations" in the BSM Platform Administration Guide.

To determine the internal IP of your load balancer:

a. Log in to BSM through the load balancer.

b. Open the log in the following location **<BSM Gateway Server>\log\EJBContainer\UserActionsServlet.log**.

c. The IP that appears in the latest login line in this log is the internal load balancer IP. The entry should have your user name.

4. After changing the reverse proxy settings, restart the HP BSM service on the BSM Gateway and Data Processing servers.

> **Note:** If your load balancer allows you to choose between Full-NAT and Half-NAT topologies, choose **Full-NAT**.

5. Configure the load balancer for data collector access. All data collectors must be able to access the Virtual IP of the Load Balancer. Use the standard settings for the load balancer, but set the following:

   - We recommend using a round robin algorithm in order to balance the load on all BSM gateway servers.

   - Use the following KeepAlive URI:

     - Send String: **GET /ext/mod_mdrv_wrap.dll?type=test**

     - Receive String: **Web Data Entry is up**

6. Configure the load balancer for user access.

- Use the standard settings for the load balancer, but set persistency to **stickiness by session enabled** or **Destination Address Affinity** (depending on the Load Balancer). If neither of these options are available and the choice is between **Cookie based** stickiness and **IP based** stickiness, then we recommend trying **IP based** stickiness. If this is not done properly, you may experience intermittent user interface failures.

- Use the following KeepAlive URI:

  - Send String: **GET /topaz/topaz_api/loadBalancerVerify_centers.jsp**

  - Receive String: **Success**

7. Configure the load balancer for BBC channel on port 383.

   - Port 383 needs to be open in both directions (meaning from the data collector through the load balancer to the gateway, and from the gateway and data processing server (not necessarily through the load balancer) to the data collectors).

   - The load balancing method should be “sticky session by IP address” for port 383.

   - Traffic on port 383 should be passed through on network layer 4 (not layer 7, no SSL offloading on the load balancer).

   - The load balancer's data connector address used for load balancing must be reachable and resolvable from all the BSM servers (gateway and data processing server) as well.

Notes and Limitations

- BSM supports hardware and virtual appliance based load balancers. A hardware load balancer solution is preferred for performance reasons.All load balancers must be able to configure sticky session for users and being able to configure URL based health monitors.

- If you use two load balancers for failover, you must ensure that you configure the hostnames of both load balancers on the DNS server machine. You can then specify the machine name, hostname’s FQDN, or URL of either load balancer when this information is required for the data collectors, or in the browser to open the BSM site.

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

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

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

- When a load balancer or reverse proxy is configured, ensure that it can .be reached from all BSM servers (Gateway and Data Processing Servers) with the virtual addresses specified for the connections.

High Availability for the Gateway Server

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

Protected Delivery for Incoming Data

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

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

BSM supports the following mechanisms to help ensure high availability for the raw data:

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

High Availability for Service Health

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

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

The load balancer for the Gateway Server must be set with **stickiness by session enabled**. For details, see "Configuring Load Balancing" on page 118.

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

High Availability for the Data Processing Server

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

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

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

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

Note: When deploying a new BSM installation, the first Data Processing Server started becomes the default server for the assigned Data Processing Server services—that is, it becomes the primary Data Processing Server. If a second Data Processing Server is started, you can assign it to act as a backup server. For details, see "Understanding Service Reassignment" in the BSM Platform Administration Guide.

This section includes the following topics:

Services Assigned to the Server

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

To view services via the JMX Web console:

1. In a Web browser, open:

   http://<Data Processing Server machine name>:29000/jmx-console

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

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

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

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

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

Column Name	Description
Service	The name of the assigned service.
Customer	The ID of the customer to which the service is assigned. The default customer ID for an individual BSM system (one not managed by HP Software-as-a-Service) is 1. A service with a customer id of -1 is a global service used by all customers in a SaaS deployment.
Process	The name of the Data Processing Server and the name of the JVM process handling the service. The length of time the server has been running and the last time it was pinged are also displayed.
Assigned	Whether the service assignment is currently active or not, the date the service was assigned, and the length of time it has been assigned are displayed.

Column Name	Description
State	The current state of the service. Valid states are: 1 – Stopped 2 – Starting 3 – Stopping 4 – Running -1 – Failed -2 – Failed to stop -3 – Failed to start The date that the service acquired the state, and the length of time that it has been in the state are displayed.
Srv. Sign	Server signature.
State Sign	State signature (should match the server signature).

Services Managed by the High Availability Controller (HAC)

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

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

JVM Process Name	HAC Process Name	Service Name	Description of Service Location of Log File
Mercury AS	mercury _as	KPI_ ENRICHMENT	KPI_Enrichment service is responsible for adding dashboard KPIs to CIs that were added to the model by external monitoring systems. The KPIs to add and the CIs to which the KPIs are added are configurable.
		BSM_DT	BSM_DT handles the configured downtimes in the system. Downtimes can be configured onto CIs and can be configured to affect alerts, events, reports, KPI calculations, and monitoring.
		VERTICALS	Verticals service is for SAP that ensures compatibility with BSM. SAP service links data retrieved from SiteScope and Business Process Monitors to SAP related entities brought from the RTSM.
		EUM_ADMIN	EUM_ADMIN handles End User Management Administration where Business Process Monitors and Real User Monitors are configured for monitoring.
mercury_ odb	odb	BSM_ODB	The RTSM is a central repository for configuration information that is gathered from the various BSM and third-party applications and tools. This information is used to build BSM views.
hpbsm_ bizImpact	businessimpact_ service	BIZ_IMPACT	The Business Impact component enables you to see the business CIs and SLAs that are impacted by another CI in Service Health.
		LIV_SERVICE	Local Impact View enables you to also create local impact views in Service Health. These are independent of all other views. When you modify indicator definitions on a CI within a local impact view, this has no effect on this CI in all other views.
hpbsm _offline _engine	offline_ engine	NOA	The New Offline Aggregator service validates and synchronizes new tasks for the offline aggregator on an hourly or daily basis.

JVM Process Name	HAC Process Name	Service Name	Description of Service Location of Log File
hpbsm _marble _ supervisor	marble_ supervisor	DASHBOARD	Dashboard service on the Data Processing Server is responsible for online business logic calculations for Service Health.
hpbsm_ pmanager	pmanager	PM	The Partition and Purging Manager splits fast-growing tables into partitions at defined time intervals. After a defined amount of time has elapsed, data in a partition is no longer accessible for use in BSM reports. After an additional, defined amount of time, that partition is purged from the profile database.
hpbsm_ opr_ backend	opr_backend	OPR	Responsible for the Operations Management application.
hpbsm_ pi_engine	pi_engine	PI_ENGINE	The Service Health Analyzer engine component searches for anomalies over the baseline behavior of the system.
hpbsm_ basel_ engine	basel_engine	BASELVALIDATOR	The baseline validator validates baseline tasks against metadata and add/removes tasks if needed.

Configuring Automatic Failover

You can configure automatic reassignment of services running on a primary Data Processing Server to a backup Data Processing Server. To configure the automatic reassignment of services running on a primary Data Processing Server to a backup Data Processing Server, you must:

- Define a backup Data Processing Server in the JMX console.
- Enable automatic failover.

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

Defining a Backup Server

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

To use the JMX console to define a backup server:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000/jmx-console

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

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

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

   - **primaryServerName**. The name of the primary server.

   - **backupServerName**. The name of the backup server.

   Use the machine name (not the FQDN) for both these parameters. If you are unsure of the machine name, you can use the **listservers** method described below to retrieve the name of the machines already configured.

4. Click **Invoke**.

To remove a backup server:

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

2. Locate removeBackupServer and enter the following value:

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

3. Click **Invoke**.

To view your high availability configuration:

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

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

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

Enabling Automatic Failover

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

To enable automatic failure in Infrastructure Settings:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings.**
2. Choose **Foundations**, select **High Availability Controller**, and locate the **Automatic Failover Enabled** entry in the General Properties table.
3. Modify the value to **true**. The change takes effect immediately.
4. Specify the other parameters in the table according to your needs. The details of each parameter are in the table.

To enable automatic failover in the JMX:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000/jmx-console

   When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
2. In the **Topaz** section, select **service=hac-backup.**
3. Locate **void setAutomaticFailoverEnabled ()**, select **True**, and click **Invoke**.

To check whether automatic failover has been configured:

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

Reassigning Services with JMX Console

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

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

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

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000/jmx-console

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

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

3. Locate **moveServices()** and enter the following values:

   - **customerId.** The default customer ID for a regular BSM installation is **1**. HP Software-as-a-Service customers should use their customer ID.

   - **srcServer**. The name of the source server from where you are moving services.

   - **dstServer**. The name of the destination server to where you are moving the services.

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

   - **groupName**. Leave this parameter value blank.

4. Click **Invoke**. All services running on the source server are moved to the destination server.

5. Restart the online engine (MARBLE) processes after moving them to the destination server to ensure that the model remains synchronized.

Manually Reassigning Services

> **Caution:** This section is for advanced users only.

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

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

> **Tip:** You can check that services have been reassigned, activated, or inactivated correctly by viewing the service status in the JMX Web console. For details, see "Services Assigned to the Server" on page 123.

Removing a Service's Assignment

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

To remove a service's current assignment:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000/jmx-console

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

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

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

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

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

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

   - **serverName.** The name of the Data Processing Server to which the service is currently assigned.

   - **processName.** The name of the process (such as **mercury_as**, **mercury_online_engine**, **mercury_offline_engine**, **topaz_pm**).

4. Click **Invoke**. The assignment for the service is removed from the specified Data Processing Server.

Changing the Status of an Assigned Service

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

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

To change the assigned value of an existing assignment:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000/jmx-console

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

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

3. Under **changeAssignment()**, enter the following data:

- **customerId.** The default customer ID for a regular BSM installation is **1**. HP Software-as-a-Service customers should use their customer ID.

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

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

4. Click **Invoke**. The assignment for the service is changed according to the **assignValue** entered.

Adding an Assignment for a Service

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

To add a new assignment for a service:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000/jmx-console

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

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

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

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

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

   - **serviceName.** The name of the service you are assigning.
   - **serverName.** The name of the new Data Processing Server to which the service is being

assigned.

- **processName.** The name of the process.
- **assignValue.** The assigned value for the assignment. Any number between -9 and 9 is valid. The value **1** makes the assignment active and any other number makes it inactive.

4. Click **Invoke**. The assignment for the service is added for the specified Data Processing Server.

Manually Disabling Data Aggregator Services

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

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

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

Configuring BSM Data Collectors in a Distributed Environment

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

Business Process Monitor and Real User Monitor

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

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

Specify the Gateway Server address as follows:

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

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

SiteScope

For SiteScopes to perform their work, you must specify the Gateway Server URL in each SiteScope profile, using BSM System Availability Management (**Admin > System Availability Management**). For details, refer to "Configuring the Connection" in the SAM part of the BSM User Guide.

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

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

Appendix G: Uninstalling BSM Servers

If you plan to install BSM 9.26 on a machine where a previous BSM 9.2x version already exists you must completely remove the BSM 9.2x installation first.

Note: The standard BSM uninstall process can take several hours, depending on the number of installed patches. In order to speed up the uninstall process, you can run the BSM 9.2x Uninstall Tool. This tool significantly reduces the BSM uninstall time to several minutes using standard operating system tools to clean up the existing BSM installation.

To access the BSM Uninstall Tool:

1. Go to the HPE Software Support web site (https://softwaresupport.hp.com) and sign in.
2. Click **Patches**.
3. Search for **BSM 9.2x Uninstall Tool.**
4. For Windows, select **BSM 9.2x Uninstall Tool for Windows**.

   For Linux, select **BSM 9.2x Uninstall Tool for Linux**.
5. After the BSM Uninstall Tool finishes running, perform steps 3 and 4 from *Uninstalling BSM servers in a Windows environment* below. These steps provide instructions about the IIS Web Server and Windows Registry.

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.

3. If you are running BSM with Microsoft IIS, open the IIS Internet Services Manager and check the following:

a. Under the **Default Web Site**, check that the following virtual directories have been removed and remove them if they still appear:

- bsm
- ext
- HPBSM
- jakarta
- mam_images
- mercuryam
- odb
- topaz
- tvb
- ucmdb-ui
- uim

b. Right-click the server machine name in the tree, and select **Properties**. In the Properties dialog box, with **WWW Service** displayed in the Master Properties list, click **Edit**. Select the **ISAPI Filters** tab. If the **jakartaFilter** filter still appears, remove it.

> **Note:** If you plan to uninstall BSM and then reinstall it to a different directory on the server

> machine, there is no need to remove the **jakartaFilter** filter. However, you will need to update the path for the filter. For details, see "After uninstalling BSM and reinstalling to a different directory, BSM does not work" on page 146.

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

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

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

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

Uninstalling BSM servers in a Linux environment

1. Log in to the server as user **root**.

2. To access the uninstall program, type: **cd /opt/HP/BSM/installation/bin**

3. 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.

Appendix H: 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 I: Switching Web Servers

If you have already installed BSM, and want to switch your web server type, perform the procedure below.

Note: If you have enabled smart card authentication and want to switch your web server from Apache to IIS or vise versa, you need to first disable smart card authentication. You can re-enable smart card authentication after you have switched web servers. For details on how to enable and disable smart card authentication, see "Smart Card Authentication" in the BSM Platform Administration Guide.

1. Stop all BSM Gateway and Data Processing servers. For details, see "Starting and Stopping BSM" on page 26.

2. If you are moving from IIS to Apache, stop the IIS service or select a different port in the post-installation wizard in the next step.

3. If you are moving from Apache to IIS, configure IIS. For more information, see:

   For Linux: "Working with the Web Server" on page 68

   For Windows: "Working with the Web Server" on page 75

4. Run the Post-Installation wizard and select the new web server type on the appropriate screen.

   The post-installation wizard can be run from the following location: **<HPBSM root directory>\bin\postinstall.bat**. However, if the wizard was closed before completion, use the following file instead <**HPBSM root directory>\bin\ovii-postinstall.bat**.

5. Start all BSM Gateway and Data Processing servers.

Appendix J: Troubleshooting

This appendix contains the following topics:

Troubleshooting Resources

- **Installation log files.** For details, see "Check installation log files" on page 24.

- **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.

After installing BSM 9.26, RTSM is not accessible

After installing BSM 9.26, when you try to access RTSM, you might encounter an internal server error. If you encounter such an error, restart BSM.

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 75.

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.

User Engagement Troubleshooting

This section recommends solutions to problems you may encounter when installing User Engagement.

The User Engagement components in the BSM user interface show an error 404 instead of content.

This may be a result of not upgrading the User Engagement database schema to version 9.26.

Recommended Solution:

Manually upgrade the database by running the following script:

Oracle:
`<BSM root directory>/AppServer/webapps/site.war/DataBases/ORA_DB_Utils/exc_ora_dbobjects_update_923.sql`

SQL Server:
`/AppServer/webapps/site.war/DataBases/SQL_Svr_DB_Utils/exc_sql_dbobjects_update_923.sql`

The User Engagement administration user interfaces shows the following error message: `Sorry, you're not authorized to view this page`.

The BSM user account you used to log on does not have administrative privileges for User Engagement.

Recommended Solution:

Grant administrative privileges to the account as described in "Setting Up User Engagement" on page 39.

Event Stream Correlation Master achievements not displayed in the Achievements list.

The Event Stream Correlation Master achievement is not displayed in the Achievements tab in the User Engagement Dashboard, although it is active in the Achievements administrative UI. Participants can create new Stream-based Event Correlation rules but the activities are not awarded.

Recommended Solution:

Disable the Event Stream Correlation Master achievement and enable the SBEC Master achievement, which awards the same activity.

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 Installation Guide (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@hp.com.

We appreciate your feedback!