HPE Business Service Management

Software Version: 9.26

BSM Upgrade Guide - 9.2x to 9.26

Document Release Date: June 2017

Software Release Date: September 2016

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

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

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

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

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

iPod is a trademark of Apple Computer, Inc.

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

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

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=.

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

Support

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

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services

- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to **https://softwaresupport.hp.com** and click **Register**.

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

HP Software Integrations, Solutions and Best Practices

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

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

Contents

Introduction 6

Upgrade Methods 7

Part 1: Method I Upgrade (Direct) 8

Chapter 1: Overview of BSM 9.2x to BSM 9.26 Method I Upgrade (Direct) 9

Chapter 2: Method I Upgrade from BSM 9.2x to BSM 9.26 10

Chapter 3: Uninstall BSM 9.26 (Rolling Back) 18

Part 2: Method II Upgrade (Indirect) 19

Chapter 4: Overview of BSM 9.2x to BSM 9.26 Method II Upgrade (Indirect) 20

Chapter 5: Method II Upgrade from BSM 9.2x to BSM 9.26 21

Chapter 6: Disaster Recovery for BSM 27

Introduction to Disaster Recovery for BSM 28

Preparing the Disaster Recovery Environment 31

Cleanup Procedure 35

Configure the New Environment 42

Configure Data Collectors 43

Chapter 7: Uninstall BSM 9.26 (Rolling Back) 53

Part 3: Method III Upgrade (Staging) 54

Chapter 8: Overview of BSM 9.2x to BSM 9.26 Method III Upgrade (Staging) 55

Chapter 9: Method III Staging Upgrade of BSM 9.2x to BSM 9.26 56

Chapter 10: Disaster Recovery for BSM 62

Introduction to Disaster Recovery for BSM 63

Preparing the Disaster Recovery Environment 65

Cleanup Procedure 69

Configure the New Environment 76

Configure Data Collectors 77

Chapter 11: Staging Mode 87

Chapter 12: Staging Data Replicator 88

Staging Data Replicator - Overview 89

Running the Staging Data Replicator (Standalone) 90

Verifying that the SDR Server Can Communicate with the Production Server 92
Unsubscribing the Staging Data Replicator from the Source Server 93
Running the SDR with Basic Authentication 94
Enable Event Receiving on the Production System 95
SSL Configuration for the Staging Data Replicator 96

Part 4: Troubleshooting 97

Chapter 13: Installation and Connectivity Troubleshooting 98
Cannot log in to LDAP after upgrade 99
JBoss does not start when there are two enabled NICs 99
Server is not ready message 100

Send Documentation Feedback 101

Introduction

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

Note: If you have a RUM data collector, when upgrading BSM, RUM persists the data samples to send to BSM. Persistency is limited by the amount of unsent sample data and by time. To increase the amount of unsent sample data, see Configuring the Amount of Unsent Sample Data to Store in RUM in the Real User Monitor Administration Guide.

This guide is for customers who have version 9.2x of BSM installed and want to upgrade to version 9.26.

How This Guide is Organized

This book is divided into four parts:

- Part 1 contains the workflow for upgrading using Method I (Direct)
- Part 2 contains the workflow for upgrading using Method II (Indirect)
- Part 3 contains the workflow for upgrading using Method III (Staging)
- Part 4 contains troubleshooting information

You should select the workflow that is appropriate for your environment. Whichever workflow is chosen should be read and executed in chronological order where relevant.

Upgrade Methods

There are three possible methods for upgrading from BSM 9.2x to BSM 9.26.

Method I is a **direct** upgrade. Upgrading directly refers to installing BSM 9.26 on the same servers and database schemas as BSM 9.2x. This can only be performed after uninstalling BSM 9.2x (which includes BSM versions 9.20, 9.21, 9.22, 9.23, 9.24, 9.25 and all IPs for these versions) and therefore results in greater downtime.

Method II (**indirect**) involves installing BSM 9.26 on different machines but connecting to the existing database schemas. The original BSM 9.2x servers are shut down while the upgrade is in process. The original BSM 9.2x installation is only removed once the upgrade is successful. If BSM version 9.26 is not functioning as required after connecting to the existing database schemas, you can easily roll back to the previous BSM 9.2x version by reconnecting the BSM 9.2x machine to the database schemas.

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

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

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

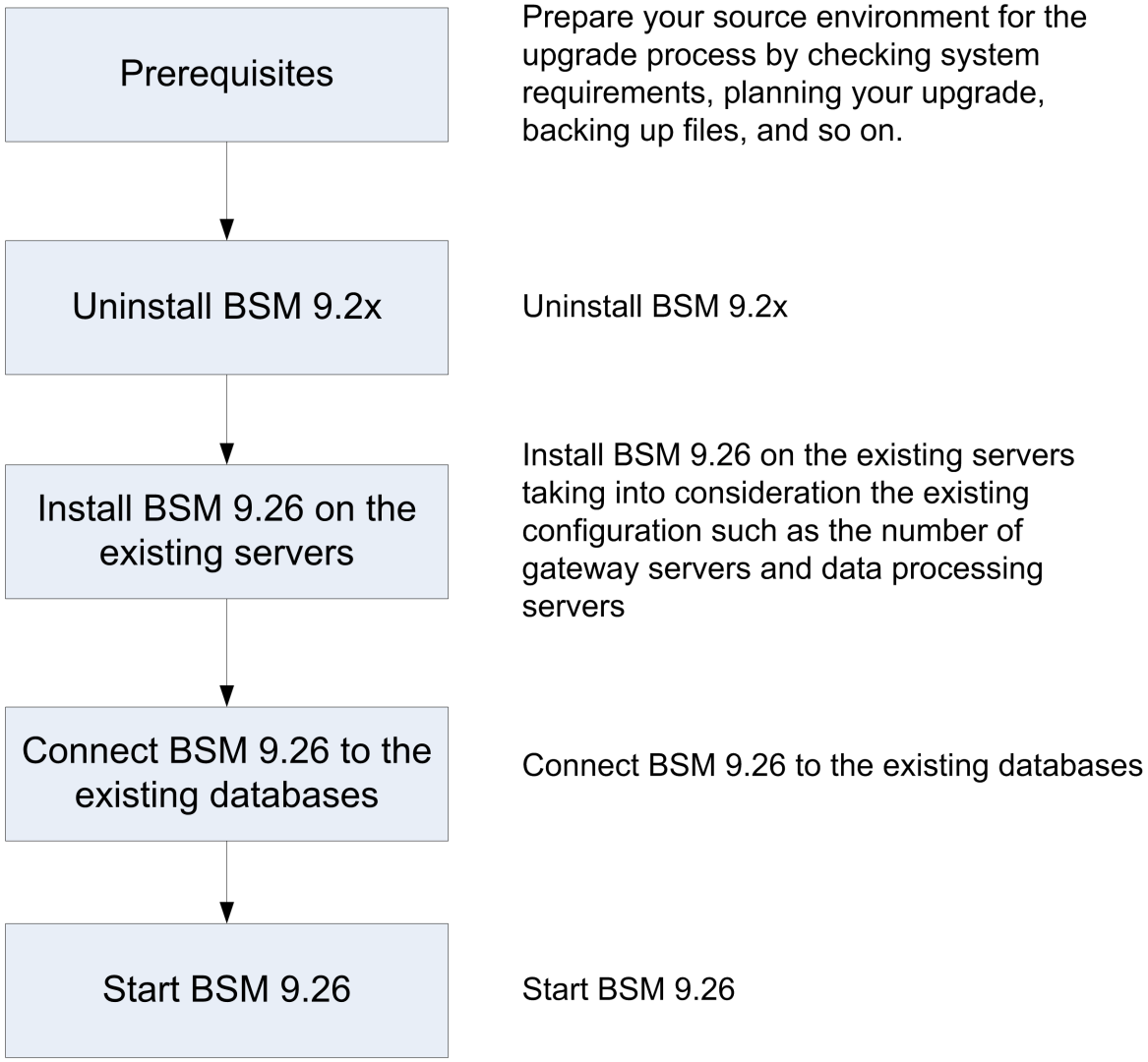
Note:

- If your source and target environments are not running the same operating systems, you must upgrade using the staging method.
- If you are upgrading to BSM 9.26 and are running Red Hat Enterprise Linux 5.x, upgrade your operating system to Red Hat Enterprise Linux 6.x or 7.x and then perform the upgrade using Method I (Direct) or Method II (Indirect).
- Scheduled reports are not sent from the staging servers while in staging mode. For more details, see "Troubleshooting the Upgrade Process" on page 1.
- All BSM machines in the staging environment must be set to the same time zone as the source environment. Incompatible time zone settings can lead to inaccuracies in reporting historical data.
- You must upgrade using a staging environment if you are switching operating systems. In BSM 9.2x, Windows Server 2003 is no longer supported, such users would have to perform a staging upgrade to a supported operating system.

Part 1: Method I Upgrade (Direct)

Chapter 1: Overview of BSM 9.2x to BSM 9.26 Method I Upgrade (Direct)

The upgrade from BSM 9.2x to BSM 9.26 involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Chapter 2: Method I Upgrade from BSM 9.2x to BSM 9.26

Note:

- If any custom configuration changes were made to the IIS web server on the BSM server, this upgrade may fail. For details and troubleshooting instructions, refer to "Installation and Connectivity Troubleshooting" on page 98.
- In this upgrade method, you install BSM 9.26 on the same servers and database schemas as BSM 9.2x. This can only be performed after uninstalling BSM 9.2x (which includes BSM versions 9.20, 9.21, 9.22, 9.23, 9.24, 9.25 and all IPs for these versions). We strongly recommend that before starting this upgrade, you create a complete backup of your BSM environment in case you decide to roll back to the 9.2x version of BSM.
- BSM versions 9.20-9.25 use SonicQ. BSM 9.26 uses HornetQ. Therefore, the internal ports used between the servers (DPSs, GWs) for the messaging cluster have changed. If you configured your firewall to allow the Sonic ports, after upgrading to 9.26, event synchronization will not work. For information on the HornetQ ports, see the Port Usage chapter in the Platform Administration Guide.

1. **Prerequisites**
   - It is recommended that you back up all BSM databases and files you made custom changes to.
   - If you create an SLA in BSM version 9.23, and then upgrade to any newer BSM version, the SLA will not work. This limitation is applicable to SLAs created in BSM version 9.23 only. Before creating SLAs in BSM version 9.23, run patch KM00706628, and then upgrade.
2. **Run the Pre-Upgrade Tool**.

   The Pre-Upgrade Tool temporarily stores some configuration and certificates in the BSM database to help migrate them to 9.26. It should be run on all BSM Gateway and the active DPS servers.

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

      On all BSM Gateway servers, run the PreUpgradeTool using the following command:

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

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

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

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

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

Additional Information

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

The Pre-Upgrade Tool executes the following steps:

- Ensures the Sonic Queue is emptied
- Gives the customer the ability to shorten the upgrade process by choosing to not upgrade closed events

3. **Back up customized Java database connectivity properties (jdbc) - Oracle RAC (optional).**

   If you configured BSM with an Oracle RAC database, and if you have custom modifications in the jdbc.drivers.properties file, back up the file.

4. **Back up configuration files from the original system.**

   Back up files you manually modified in any of the following directories:

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

   If you used User Reports to create Excel reports, you must manually back them up. 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.

5. **If Monitoring Automation 9.2x or User Engagement 9.2x are installed, uninstall them**.

   Uninstall Monitoring Automation 9.2x or User Engagement 9.2x according to the instructions in the Monitoring Automation and User Engagement Installation Guides.

6. **Uninstall BSM 9.2x**. BSM 9.2x includes all IPs for this version.

   Uninstall BSM 9.2x according to the instructions in the BSM Installation Guide.

7. **Reboot the server.**

8. **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.

   Note: On the Summary page of the Post-installation Wizard, click **Exit. Complete the upgrade or installation process at a later time**.

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

10. **Connect BSM 9.26 to the existing databases.**

    To connect BSM 9.26 to the existing databases, run the Configuration Wizard. To access the Configuration Wizard, click:

- **Linux:** Open a terminal command line and launch **/opt/HP/BSM/bin/config-serverwizard.sh**
- **Windows:** Select **Start > Programs > HP Business Service Management > Administration > Configure HP Business Service Management**

Note: The User Engagement schema is mandatory. For information on creating a User Engagement schema, see the BSM 9.26 Installation Guide.

11. **Restore configuration files.**

    Restore all files that you manually backed up in Step 4 "Back up configuration files from the original system." on page 11

12. **Enable BSM.**

    Enable BSM on all servers.

13. **Repeat hardening procedures (optional).**

    If your original environment was secured with SSL, you need to repeat the hardening procedures in “Using TLS in BSM” in the BSM Hardening Guide.

    If SSL/TLS termination is configured on the BSM Gateway and you are using Server Aliases with Subject Alternative Name (SAN) certificate in your environment and your deployment is using Apache as a BSM Gateway Web Server, you need to add the list of all aliases as described in “Using TLS in BSM” in the BSM Hardening Guide.

14. **Upgrade SHA metadata.**

    If you had previously installed SHA on a working version of BSM 9.20, perform this procedure:

    a. If you backed up your SHA analytics metadata (in case you made manual changes), merge any manual changes onto the new files.

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

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

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

        <BSM DPS installation directory>/conf/analytics/metadata/default

    b. Log onto the JMX console on the DPS using the following address:

    http://<BSM_DPS_FQDN>:29924/mbean?objectname=Topaz%3Aservice%3DAnalyticsMetadata

    c. In **java.lang.string.reloadmetadata**, under **Value**, click **True**, and then click Invoke.

d. Restart the analytics loader.

You can do this by restarting the analytics_loader on all BSM Gateway servers (avoiding system downtime), or restart all BSM Gateway servers.

15. **Deploy new RTSM Content Pack**

Deploy the latest RTSM Content Pack using one of the following methods:

- **Using the BSM UI:**
  i. Click **Admin > RTSM Administration > Administration > Package Manager**.
  ii. On the toolbar, click the **Install Content Pack** button ().
  iii. In the Install Content Pack dialog box, select version **11.13** and click **Install**.
- **Using the JMX console:**
  i. Log onto the JMX console on the Data Processing Server using the following address:

  http://<DPS server>:21212/jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=Content Pack Services

  ii. Invoke the **displayAvailableContentPackVersions** method with customerID **1** and copy the version number of the latest Content Pack (without the parenthesis).
  iii. Return to the Content Pack Services page.
  iv. Invoke the **installContentPack** method with customerID **1** and the version number you just copied.

16. **Deploy the Updated Packages**

If you are applying the latest patch to any 9.2x BSM version previous to 9.25, deploy the following packages.

Note: In a distributed environment, the packages are on the Data Processing Server.

<BSM_HOME>/odb/conf/factory_packages/BACKPIsAdapter.zip

<BSM_HOME>/odb/conf/factory_packages/BSMConnector.zip

<BSM_HOME>/odb/conf/factory_packages/BSMDowntime.zip

<BSM_HOME>/odb/conf/factory_packages/BSMDowntimeAdapter.zip

<BSM_HOME>/odb/conf/factory_packages/EUM.zip

<BSM_HOME>/odb/conf/factory_packages/Diagnostics.zip

<BSM_HOME>/odb/conf/factory_packages/Diagnostics_new.zip

<BSM_HOME>/odb/conf/factory_packages/Business.zip

<BSM_HOME>/odb/conf/factory_packages/Sitescope.zip

To deploy a package:

a. In BSM, go to **RTSM Administration > Administration > Package Manager**.

b. Select the **Deploy packages to server (from local disk)** button .

c. Select the **Add** button, and navigate to the package (see the paths above).

d. Select **Deploy**.

17. **Validate BSM Service.**

After the Windows installation, validate that the BSM service is running with the same credentials as before the installation.

Note: The build patch removes and re-installs the HP BSM service. Therefore, all service configurations are reset to the default values.

a. In Microsoft's Services window, double-click **HP Business Service Management**. The HP Business Service Management Properties (Local Computer) dialog box opens.

b. Click the **Log On** tab. In the **This account** field, the credentials of the user running the BSM services is displayed.

Note: There is no need to validate the user in the Linux installation.

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

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

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

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

where

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

b. Search for InitString and copy the value.

c. Access the flat xml file located at:

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

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

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

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

where

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

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

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

g. Enter the following values and invoke the method:

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

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

19. **Update Data Collectors.**

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

20. **Add New REST URLs to LW-SSO configuration.**

a. Launch your Web browser and enter the following address:
http://<server_name>:29000
where **<server_name>** is the name of the machine on which BSM is installed.

b. Under **Foundations**, click **Foundations:service=Infrastructure Settings Manager** to open the JMX MBEAN View page.

c. Locate **addURLToConfigurationFile**

d. Enter the following URL: **.*/topaz.*/omi.*/integration.***

e. Click **Invoke**.

f. Repeat steps a – e for the following URLs:

- **.*/topaz.*/acweb.***
- **.*/topaz.*/personalization.***
- **.*/topaz.*/bsmLight.***
- **.*/topaz.*/ldapContext.***
- .***/topaz.*/bsmLight.*/BPM.***

21. **Enable event receiving on the production system.**

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

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

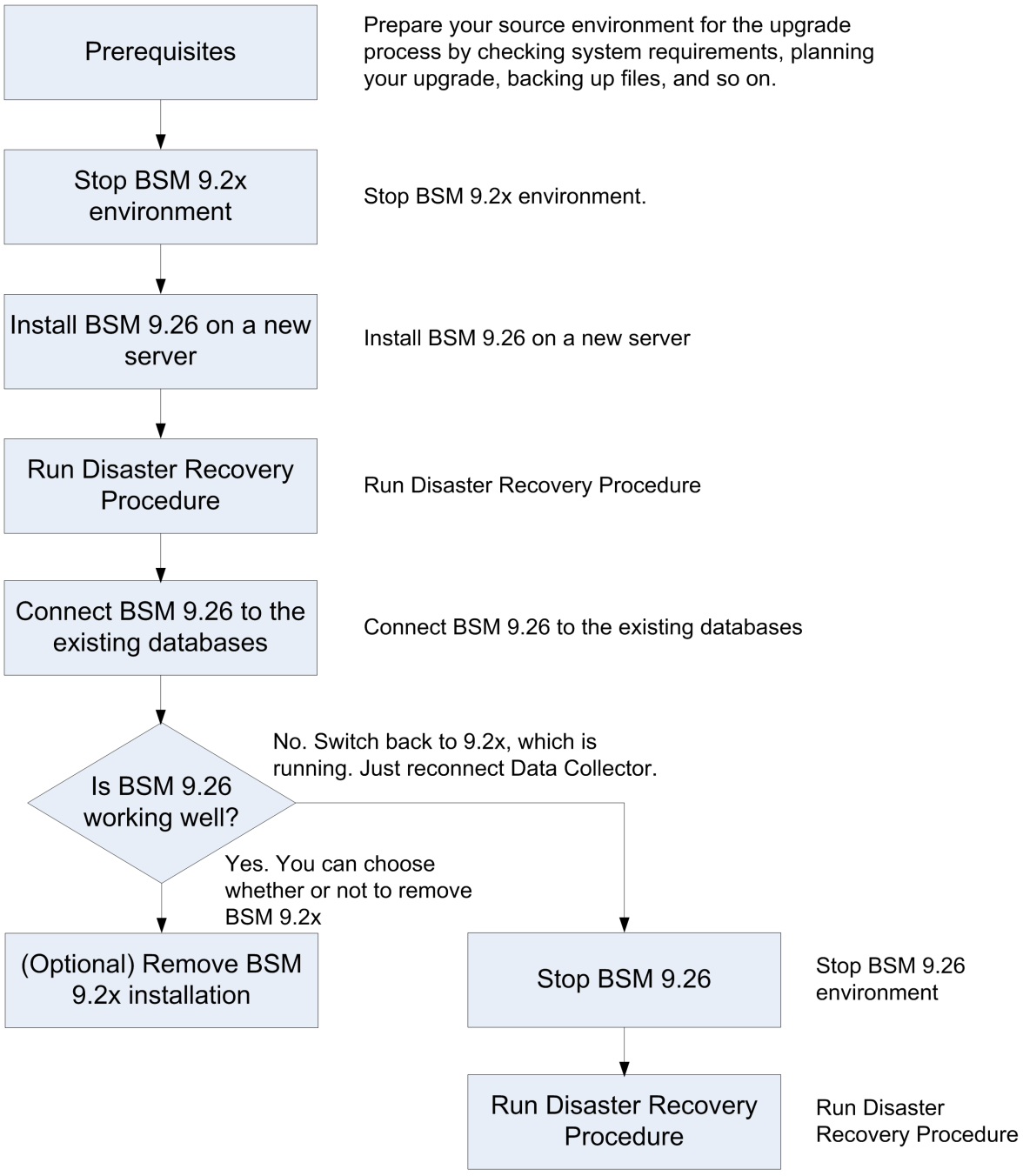
Chapter 3: Uninstall BSM 9.26 (Rolling Back)

If you installed BSM 9.26 on a machine that had the 9.2x version of BSM, and you now want to roll back to that version, revert to the 9.2x BSM environment using the backup you created before installing BSM 9.26.

Part 2: Method II Upgrade (Indirect)

Chapter 4: Overview of BSM 9.2x to BSM 9.26 Method II Upgrade (Indirect)

The upgrade from BSM 9.2x to BSM 9.26 involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Chapter 5: Method II Upgrade from BSM 9.2x to BSM 9.26

Note:

- If any custom configuration changes were made to the IIS web server on the BSM server, this upgrade may fail. For details and troubleshooting instructions, refer to "Installation and Connectivity Troubleshooting" on page 98.
- BSM versions 9.20-9.25 use SonicQ. BSM 9.26 uses HornetQ. Therefore, the internal ports used between the servers (DPSs, GWs) for the messaging cluster have changed. If you configured your firewall to allow the Sonic ports, after upgrading to 9.26, event synchronization will not work. For information on the HornetQ ports, see the Port Usage chapter in the Platform Administration Guide.

1. **Prerequisites**

   - It is recommended that you back up all BSM databases and files you made custom changes to.
   - If you create an SLA in BSM version 9.23, and then upgrade to any newer BSM version, the SLA will not work. This limitation is applicable to SLAs created in BSM version 9.23 only. Before creating SLAs in BSM version 9.23, run patch KM00706628, and then upgrade.

2. **Run the Pre-Upgrade Tool**.

   The Pre-Upgrade Tool temporarily stores some configuration and certificates in the BSM database to help migrate them to 9.26. It should be run on all BSM Gateway and the active DPS servers.

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

      On all BSM Gateway servers, run the PreUpgradeTool using the following command:

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

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

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

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

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

Additional Information

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

The Pre-Upgrade Tool executes the following steps:

- Ensures the Sonic Queue is emptied
- Gives the customer the ability to shorten the upgrade process by choosing to not upgrade closed events

3. **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 on a new set of servers.

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

   Note: On the Summary page of the Post-installation Wizard, click **Exit. Complete the upgrade or installation process at a later time**.

4. **Run the Disaster Recovery Procedure**.

   See "Introduction to Disaster Recovery for BSM" on page 28.

5. **Connect BSM 9.26 to the existing databases.**

   To connect BSM 9.26 to the existing databases, run the Configuration Wizard. To access the Configuration Wizard, click:

   Linux: Open a terminal command line and launch **/opt/HP/BSM/bin/config-serverwizard.sh**

   Windows: Start > Programs > HP Business Service Management > Administration > Configure HP Business Service Management

   Note: The User Engagement schema is mandatory. For information on creating a User Engagement schema, see the BSM 9.26 Installation Guide.

6. **Enable BSM.**

   Enable BSM 9.26 on all servers.

7. **Repeat Hardening Procedures (optional).**

   If your original environment was secured with SSL ,you need to repeat the hardening procedures in “Using TLS in BSM” in the Hardening Guide.

   If SSL/TLS termination is configured on the BSM Gateway and you are using Server Aliases with Subject Alternative Name (SAN) certificate in your environment and your deployment is using Apache as a BSM Gateway Web Server, you need to add the list of all aliases as described in “Using TLS in BSM” in the BSM Hardening Guide.

8. **Upgrade SHA metadata.**

   If you had previously installed SHA on a working version of BSM 9.20, perform this procedure:

   a. If you backed up your SHA analytics metadata (in case you made manual changes), merge any manual changes onto the new files.

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

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

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

      <BSM DPS installation directory>/conf/analytics/metadata/default

   b. Log onto the JMX console on the DPS using the following address:

      http://<BSM_DPS_FQDN>:29924/mbean?objectname=Topaz%3Aservice%3DAnalyticsMetadata

   c. In **java.lang.string.reloadmetadata**, under **Value**, click **True**, and then click Invoke.

d. Restart the analytics loader.

You can do this by restarting the analytics_loader on all BSM Gateway servers (avoiding system downtime), or restart all BSM Gateway servers.

9. **Validate BSM Service.**

After the Windows installation, validate that the BSM service is running with the same credentials as before the installation.

Note: The build patch removes and re-installs the HP BSM service. Therefore, all service configurations are reset to the default values.

a. In Microsoft's Services window, double-click **HP Business Service Management**. The HP Business Service Management Properties (Local Computer) dialog box opens.

b. Click the **Log On** tab. In the **This account** field, the credentials of the user running the BSM services is displayed.

Note: There is no need to validate the user in the Linux installation.

10. **Update Data Collectors.**

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

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

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

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

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

where

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

b. Search for InitString and copy the value.

c. Access the flat xml file located at:

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

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

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

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

where

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

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

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

g. Enter the following values and invoke the method:

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

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

12. **Add New REST URLs to LW-SSO configuration.**

a. Launch your Web browser and enter the following address:
http://<server_name>:29000
where **<server_name>** is the name of the machine on which BSM is installed.

b. Under **Foundations**, click **Foundations:service=Infrastructure Settings Manager** to open the JMX MBEAN View page.

c. Locate **addURLToConfigurationFile**.

d. Enter the following URL : **.*/topaz.*/omi.*/integration.***

e. Click **Invoke**.

f. Repeat steps a – e for the following URLs :

- **.*/topaz.*/acweb.***
- **.*/topaz.*/personalization.***
- **.*/topaz.*/bsmLight.***
- **.*/topaz.*/ldapContext.***
- **.*/topaz.*/bsmLight.*/BPM.***

13. **Enable event receiving on the production system.**
    a. Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
    b. In the applications field, select **Operations Management** and locate the **Event Pipeline Receiver Settings** table. Set **Disable receiving of Events** to **false**.
14. **(Optional) If BSM 9.26 is running well, you can remove the BSM 9.2x installation.**
15. **If BSM 9.26 is not running well, stop BSM 9.26 and run the Disaster Recovery procedure.**

    See "Introduction to Disaster Recovery for BSM" on page 28.

Chapter 6: Disaster Recovery for BSM

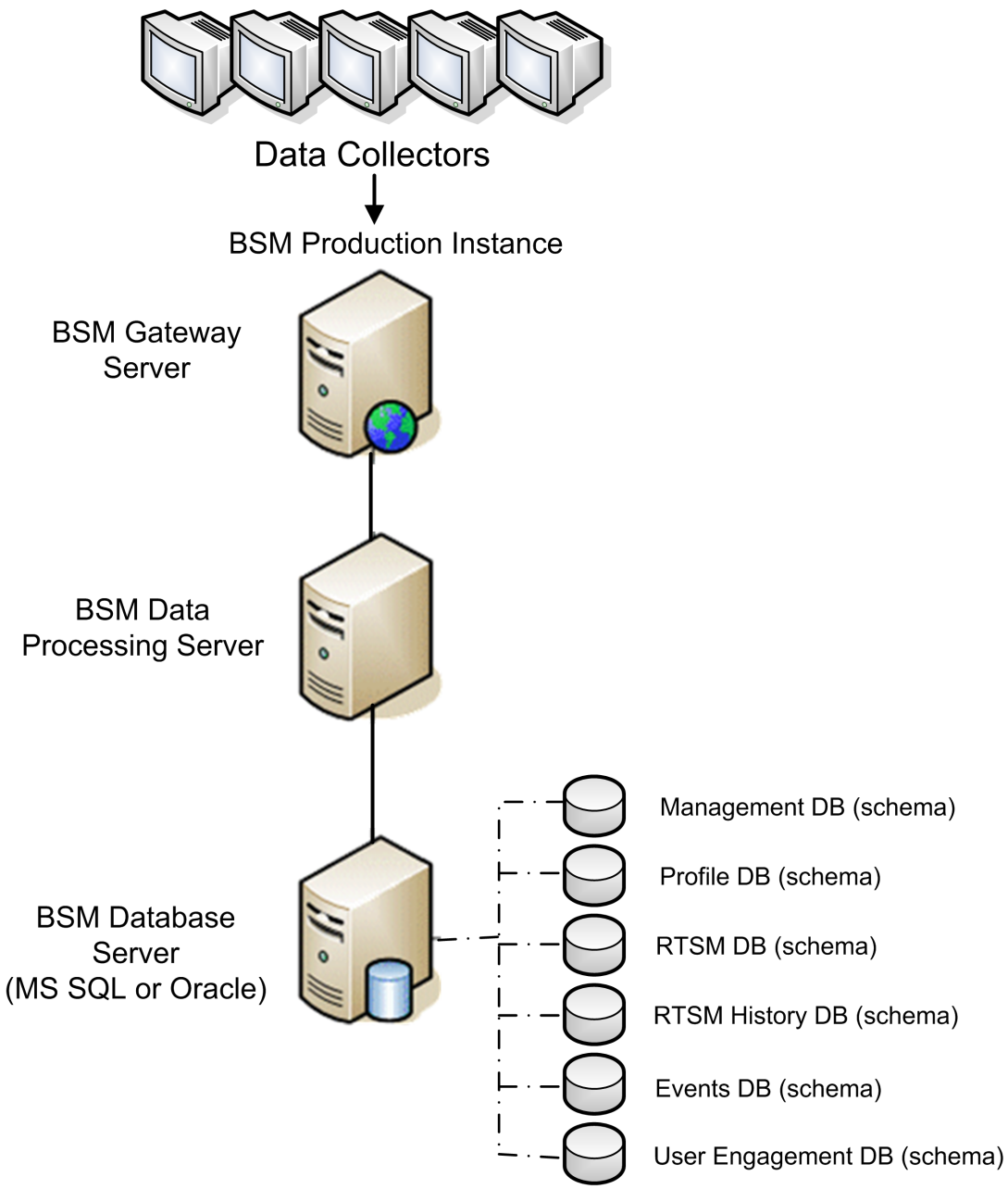
Introduction to Disaster Recovery for BSM 28
Preparing the Disaster Recovery Environment 31
Cleanup Procedure 35
Configure the New Environment 42
Configure Data Collectors 43

Introduction to Disaster Recovery for BSM

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

This chapter 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: If you are installing BSM 9.26, then the Secondary BSM system refers to BSM 9.26.
If you are uninstalling BSM 9.26 (rolling back), then the Secondary BSM system refers to BSM 9.2x.



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

Note: If you used SSL, you should create new certificates for the new environment.

Be aware that if your original environment was hardened, you need to repeat the hardening procedures on the new environment after performing the Disaster Recovery Procedure.

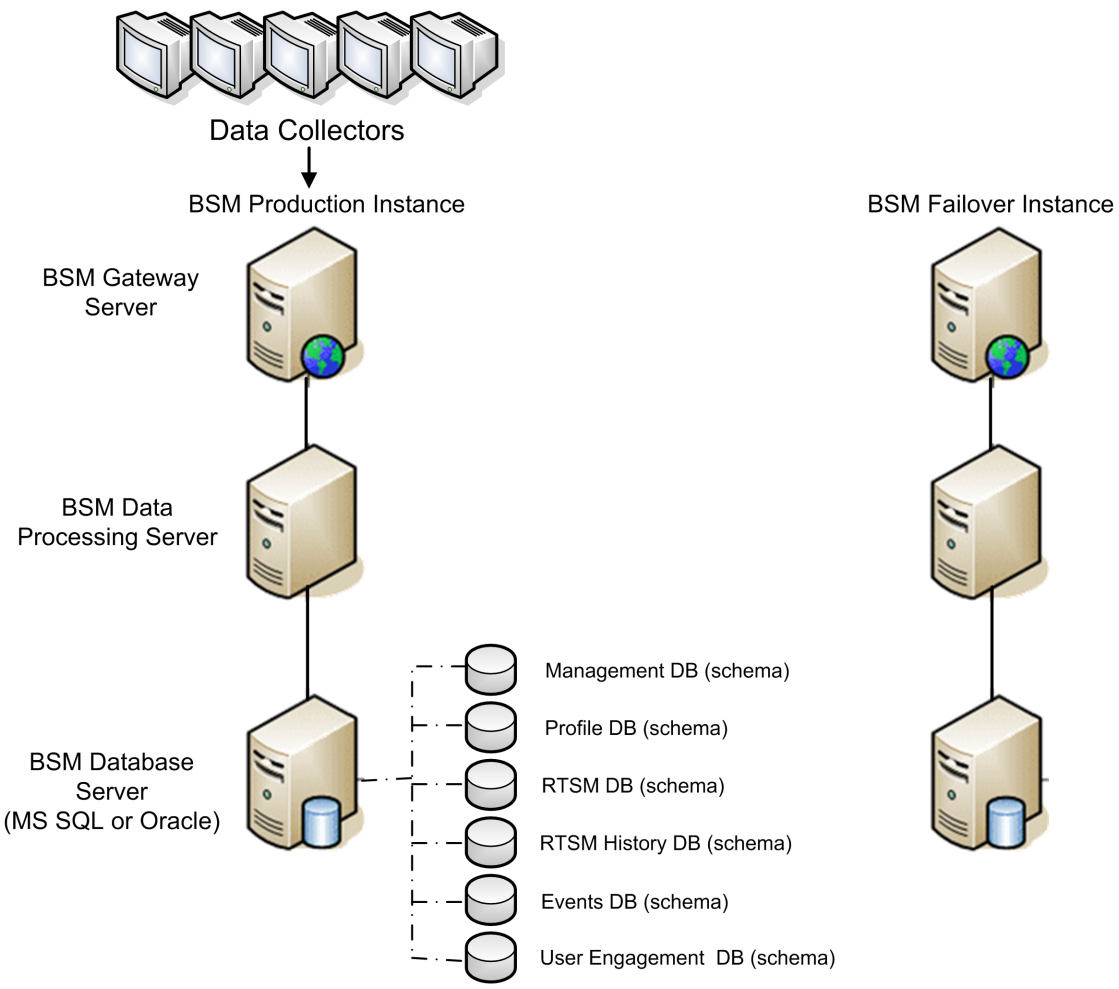
Preparing the Disaster Recovery environment by performing the following steps:

1. Install a set of BSM servers

   - Install BSM 9.26.
   - 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.

   Note: If you are installing BSM 9.26, then the BSM Failover Instance has BSM 9.26 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 Database (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.

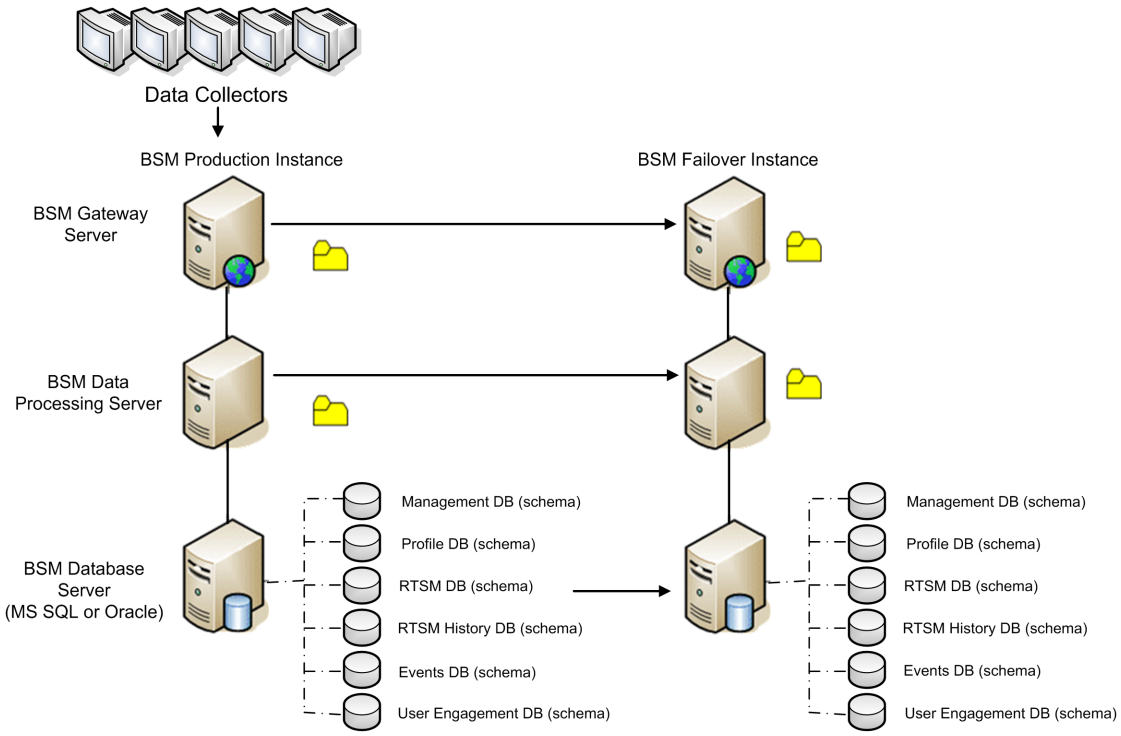
- **Oracle–configure the Standby database (Data Guard)**

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'
- update SETTING_PARAMETERS set SP_VALUE='<eventschemaname>' where SP_CONTEXT='opr' and SP_NAME='opr.db.connection.dbname'
- update SETTING_PARAMETERS set SP_VALUE='<dbhostname>' where SP_CONTEXT='opr' and SP_NAME='opr.db.connection.host'

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 on the event database.

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:

   - **Linux:** Open a terminal command line and launch **/opt/HP/BSM/bin/config-serverwizard.sh**
   - **Windows:** 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 > Setup 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.

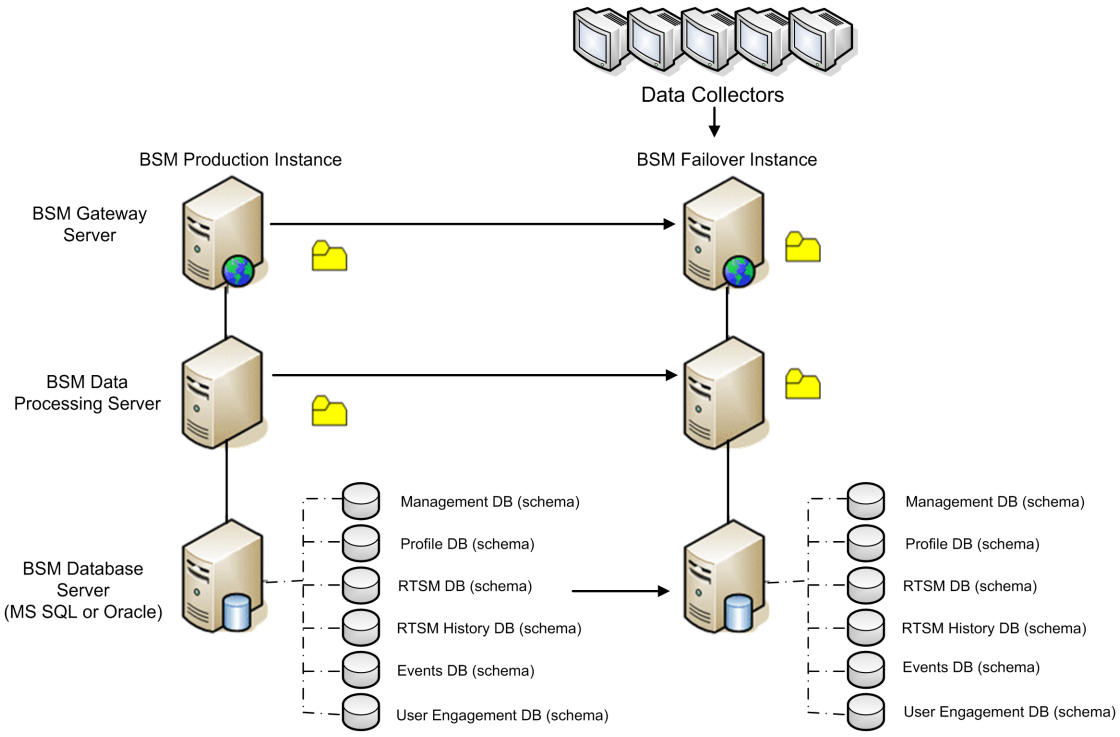
   For details, see “Using TLS in BSM” in the BSM Hardening Guide.

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:


Data Collectors
BSM Production Instance
BSM Failover Instance
BSM Gateway Server
BSM Data Processing Server
BSM Database Server (MS SQL or Oracle)
Management DB (schema)
Profile DB (schema)
RTSM DB (schema)
RTSM History DB (schema)
Events DB (schema)
User Engagement DB (schema)
Management DB (schema)
Profile DB (schema)
RTSM DB (schema)
RTSM History DB (schema)
Events DB (schema)
User Engagement DB (schema)

2. Configuring failover data collector connections.

If any of the data collectors used SSL, you should add their certificates to BSM.

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	In all cases, do the following:
	a. Go to **SiteScope** > **Preferences** > **Integration preferences**.
	b. Select your BSM integration and update the BSM IP address .
	c. Click **Re-Synchronize**.
	Note: If SiteScope just changed its hostname, perform step **e** and **f** only.
	d. From SiteScopeA, use the Sitescope ConfigTool to Export Data (including the log files) to the file **SitescopeOrig.zip**.
	e. Turn off both SiteScopeA and SiteScopeB and change the service on SitescopeA to **disabled**.
	f. Copy **SitescopeOrig.zip** to the SiteScopeB machine.
	g. Run the ConfigTool on SiteScopeB to import the data using the **SitescopeOrig.zip** file. Do not start SiteScopeB.
	h. On the BSM gateway machine, open **<HPBAC Dir>\Tools\TopazBrowser** and run the following SQL queries against the BSM management database:
	◦ In the HOST table, identify the record that contains information from SiteScopeA :
	`select * from hosts`, identify the record that pertains to SiteScopeA and record the **H_ID** and **H_LocID** values and run
	`update hosts set h_name ='<NewHostName>' where h_id=<H_ID PreviouslyFound>`
	◦ In the LOCATIONS table, change the location to match the new value
	`select * from locations where l_locid=<H_LocID PreviouslyFoundFromHOSTS>`and run
	`update locations set L_LOCNAME='<NewHostName>' where l_locid=<H_LocID PreviouslyFoundFromHOSTS>`
	◦ In the SESSIONLOCATIONS table, locate the correct SESSION_ID
	`select * from sessionlocations where sl_locid=<H_LocID PreviouslyFoundFromHOSTS>` and record the **SESSION_ID** from the record found.
	◦ In the SESSION_SITESCOPE_PROPS table, modify the

Data Collector	Procedure
	SiteScope properties to match the new host: `select * from session_sitescope_props where session_id=<Session_ID PreviouslyFound>`, verify that this is the correct record and run `update session_sitescope_props set SITESCOPE_HOST='<NewHostName>',SITESCOPE_LOCATION='<NewHostName>' where session_id=<Session_ID PreviouslyFound>` i. Start SiteScopeB.
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.

Chapter 7: Uninstall BSM 9.26 (Rolling Back)

The following provides instructions for uninstalling BSM 9.26. For example, this means rolling back from BSM 9.26 to BSM 9.2x.

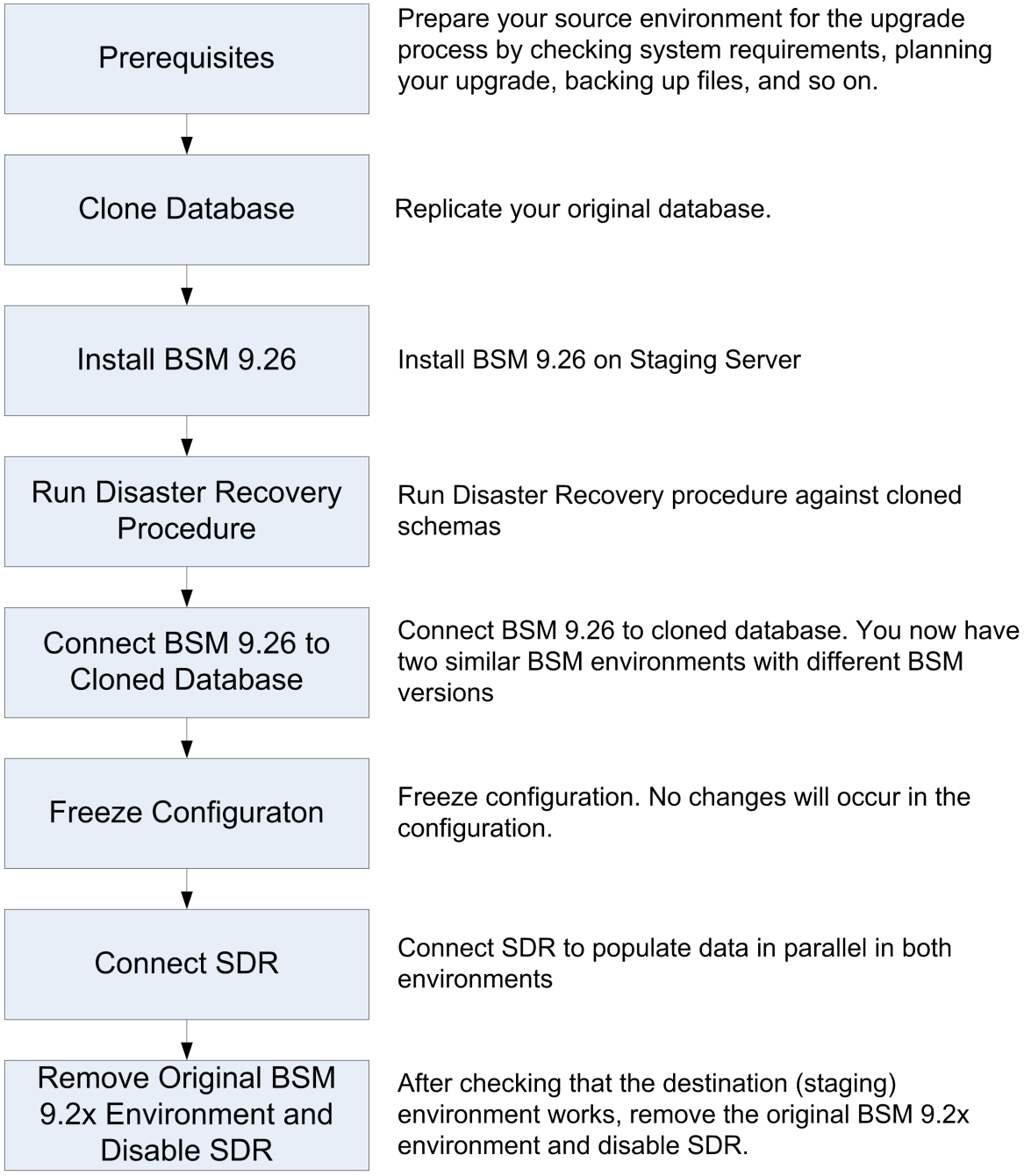
If you installed BSM 9.26 using Method II:

1. Disable BSM 9.26.
2. Perform Disaster Recovery Procedure.
3. Start BSM 9.2x.

Part 3: Method III Upgrade (Staging)

Chapter 8: Overview of BSM 9.2x to BSM 9.26 Method III Upgrade (Staging)

The upgrade from BSM 9.2x to BSM 9.26 involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Chapter 9: Method III Staging Upgrade of BSM 9.2x to BSM 9.26

Note:

- If any custom configuration changes were made to the IIS web server on the BSM server, this upgrade may fail. For details and troubleshooting instructions, refer to "Installation and Connectivity Troubleshooting" on page 98.
- BSM versions 9.20-9.25 use SonicQ. BSM 9.26 uses HornetQ. Therefore, the internal ports used between the servers (DPSs, GWs) for the messaging cluster have changed. If you configured your firewall to allow the Sonic ports, after upgrading to 9.26, event synchronization will not work. For information on the HornetQ ports, see the Port Usage chapter in the Platform Administration Guide.

1. **Prerequisites**

   - It is recommended that you back up all BSM databases and files you made custom changes to.
   - If you create an SLA in BSM version 9.23, and then upgrade to any newer BSM version, the SLA will not work. This limitation is applicable to SLAs created in BSM version 9.23 only. Before creating SLAs in BSM version 9.23, run patch KM00706628, and then upgrade.

2. **Run the Pre-Upgrade Tool**.

   The Pre-Upgrade Tool temporarily stores some configuration and certificates in the BSM database to help migrate them to 9.26. It should be run on all BSM Gateway and the active DPS servers.

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

      On all BSM Gateway servers, run the PreUpgradeTool using the following command:

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

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

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

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

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

Additional Information

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

The Pre-Upgrade Tool executes the following steps:

- Ensures the Sonic Queue is emptied
- Gives the customer the ability to shorten the upgrade process by choosing to not upgrade closed events

3. **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 on a new set of servers.

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

   Note: On the Summary page of the Post-installation Wizard, click **Exit. Complete the upgrade or installation process at a later time**.

4. **Replicate the Database**

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

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

5. **Run the Disaster Recovery Procedure**.

   See "Introduction to Disaster Recovery for BSM" on page 63.

6. **Connect BSM 9.26 to the replicated databases.**

   To connect BSM 9.26 to the replicated databases, run the Configuration Wizard. To access the Configuration Wizard, click:

   Linux: Open a terminal command line and launch **/opt/HP/BSM/bin/config-serverwizard.sh**

   Windows: Start > Programs > HP Business Service Management > Administration > Configure HP Business Service Management

7. **Enable BSM.**

   Enable BSM 9.26 on all servers.

8. **Repeat Hardening Procedures (optional).**

   If your original environment was secured with SSL ,you need to repeat the hardening procedures in “Using TLS in BSM” in the Hardening Guide.

   If SSL/TLS termination is configured on the BSM Gateway and you are using Server Aliases with Subject Alternative Name (SAN) certificate in your environment and your deployment is using Apache as a BSM Gateway Web Server, you need to add the list of all aliases as described in “Using TLS in BSM” in the BSM Hardening Guide.

9. **Upgrade SHA metadata.**

   If you had previously installed SHA on a working version of BSM 9.20, perform this procedure:

   a. If you backed up your SHA analytics metadata (in case you made manual changes), merge any manual changes onto the new files.

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

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

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

      <BSM DPS installation directory>/conf/analytics/metadata/default

   b. Log onto the JMX console on the DPS using the following address:

http://<BSM_DPS_FQDN>:29924/mbean?objectname=Topaz%3Aservice%3DAnalyticsMetadata

c. In **java.lang.string.reloadmetadata**, under **Value**, click **True**, and then click Invoke.

d. Restart the analytics loader.

You can do this by restarting the analytics_loader on all BSM Gateway servers (avoiding system downtime), or restart all BSM Gateway servers.

10. **Validate BSM Service.**

After the Windows installation, validate that the BSM service is running with the same credentials as before the installation.

Note: The build patch removes and re-installs the HP BSM service. Therefore, all service configurations are reset to the default values.

a. In Microsoft's Services window, double-click **HP Business Service Management**. The HP Business Service Management Properties (Local Computer) dialog box opens.

b. Click the **Log On** tab. In the **This account** field, the credentials of the user running the BSM services is displayed.

Note: There is no need to validate the user in the Linux installation.

11. **Update Data Collectors.**

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

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

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

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

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

where

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

b. Search for InitString and copy the value.

c. Access the flat xml file located at:

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

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

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

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

where

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

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

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

g. Enter the following values and invoke the method:

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

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

13. **Add New REST URLs to LW-SSO configuration.**

a. Launch your Web browser and enter the following address:
http://<server_name>:29000
where **<server_name>** is the name of the machine on which BSM is installed.

b. Under **Foundations**, click **Foundations:service=Infrastructure Settings Manager** to open the JMX MBEAN View page.

c. Locate **addURLToConfigurationFile**.

d. Enter the following URL: **.*/topaz.*/omi.*/integration.***

e. Click **Invoke**.

f. Repeat steps a – e for the following URLS:

- **.*/topaz.*/acweb.***
- **.*/topaz.*/personalization.***
- **.*/topaz.*/bsmLight.***
- **.*/topaz.*/ldapContext.***
- **.*/topaz.*/bsmLight.*/BPM.***

14. **Enable event receiving on the production system.**

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

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

15. **Perform the Staging Mode procedure.**

See "Staging Mode" on page 87.

Chapter 10: Disaster Recovery for BSM

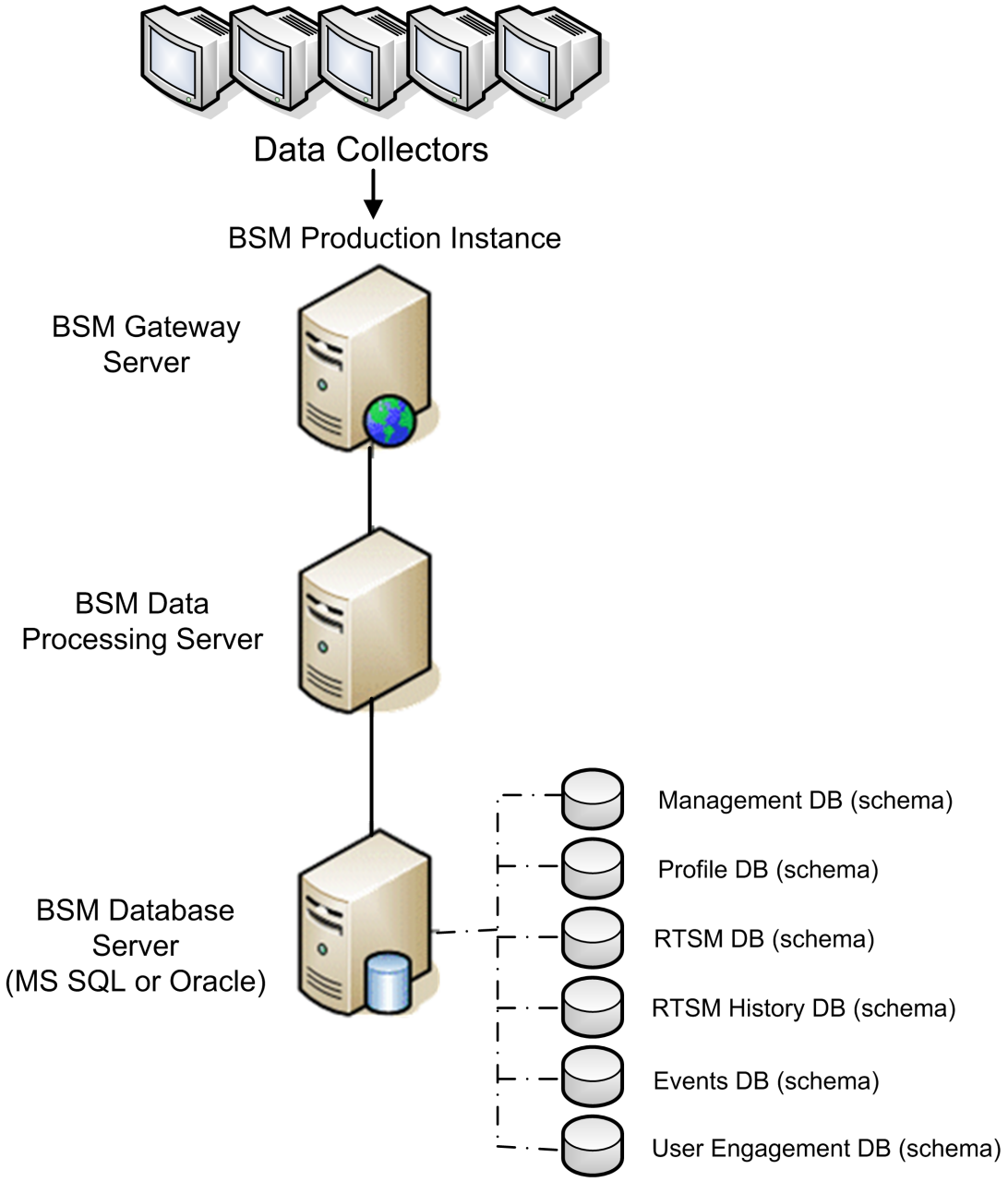
Introduction to Disaster Recovery for BSM 63
Preparing the Disaster Recovery Environment 65
Cleanup Procedure 69
Configure the New Environment 76
Configure Data Collectors 77

Introduction to Disaster Recovery for BSM

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

This chapter 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: If you are installing BSM 9.26, then the Secondary BSM system refers to BSM 9.26.



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

Note: If you used SSL, you should create new certificates for the new environment.

Be aware that if your original environment was hardened, you need to repeat the hardening procedures on the new environment after performing the Disaster Recovery Procedure.

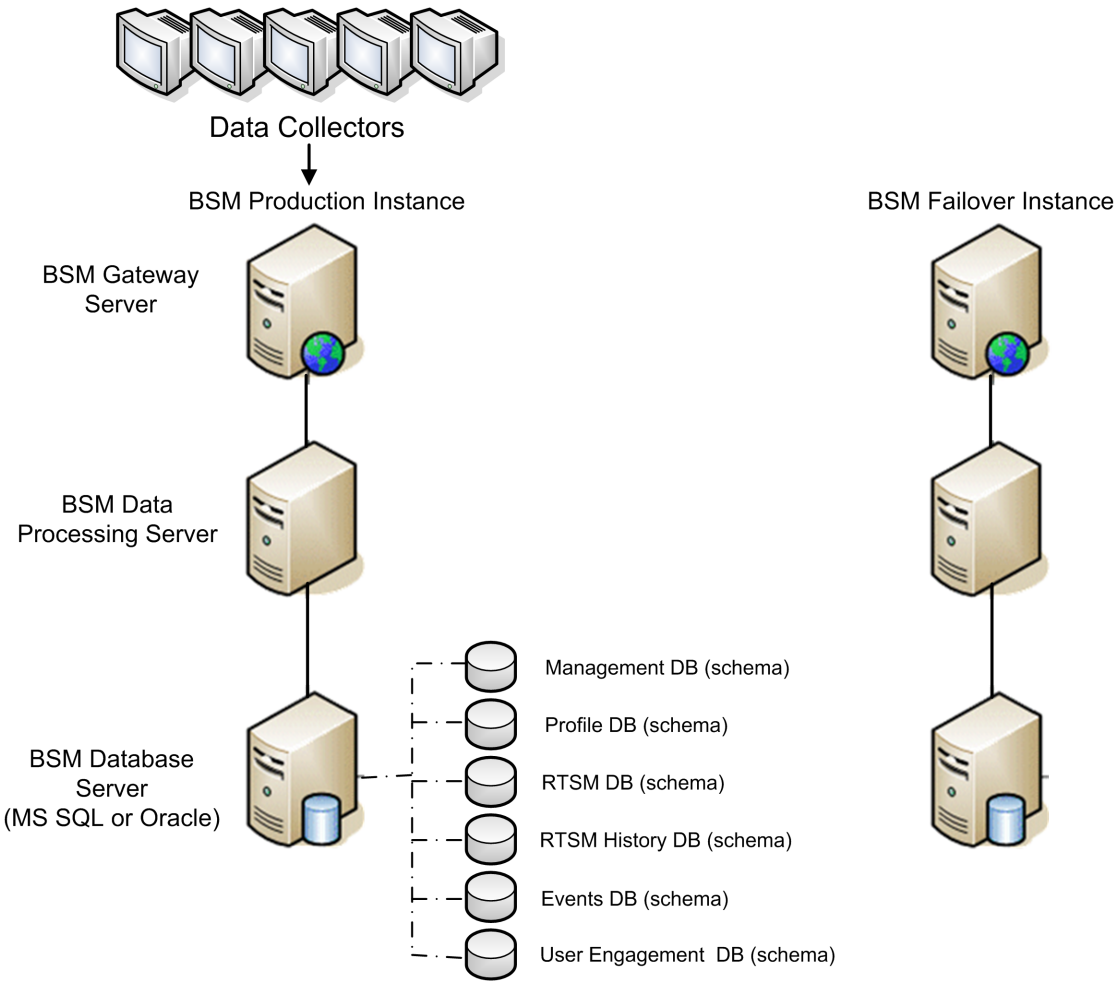
Preparing the Disaster Recovery environment by performing the following steps:

1. Install a set of BSM servers

   - Install BSM 9.26.
   - 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.

   Note: If you are installing BSM 9.26, then the BSM Failover Instance has BSM 9.26 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 Database (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.

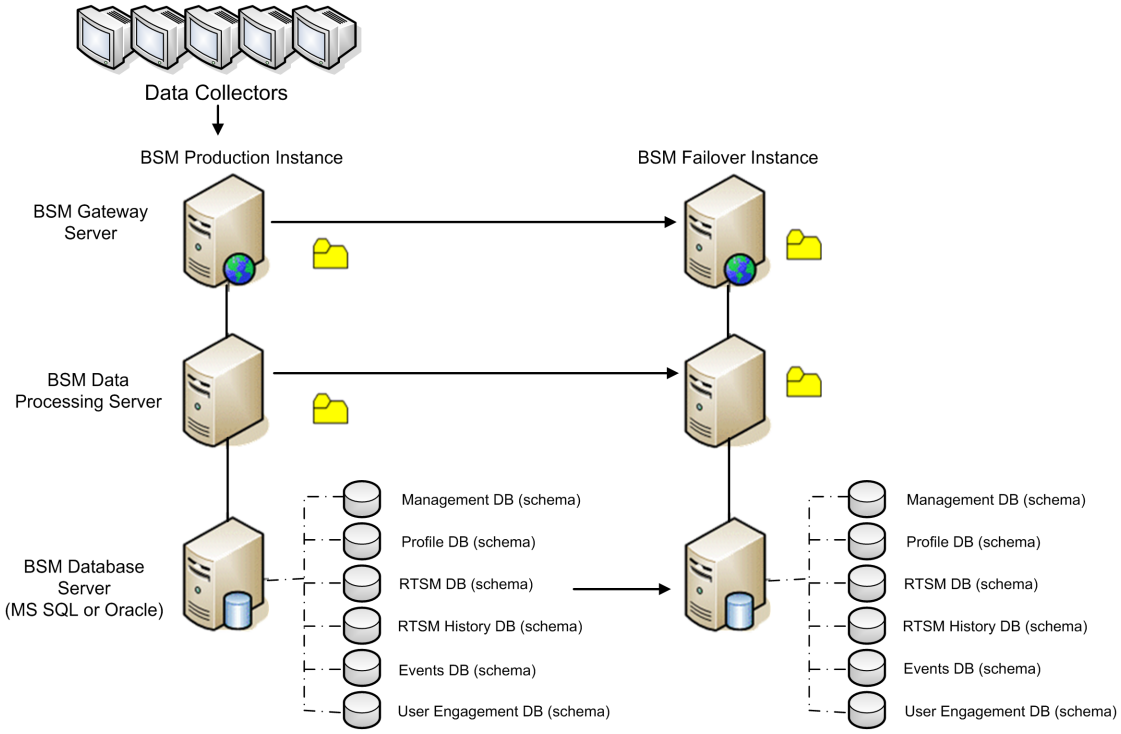
- **Oracle–configure the Standby database (Data Guard)**

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'
- update SETTING_PARAMETERS set SP_VALUE='<eventschemaname>' where SP_CONTEXT='opr' and SP_NAME='opr.db.connection.dbname'
- update SETTING_PARAMETERS set SP_VALUE='<dbhostname>' where SP_CONTEXT='opr' and SP_NAME='opr.db.connection.host'

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 on the event database.

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:

   - **Linux:** Open a terminal command line and launch **/opt/HP/BSM/bin/config-serverwizard.sh**
   - **Windows:** 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 > Setup 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.

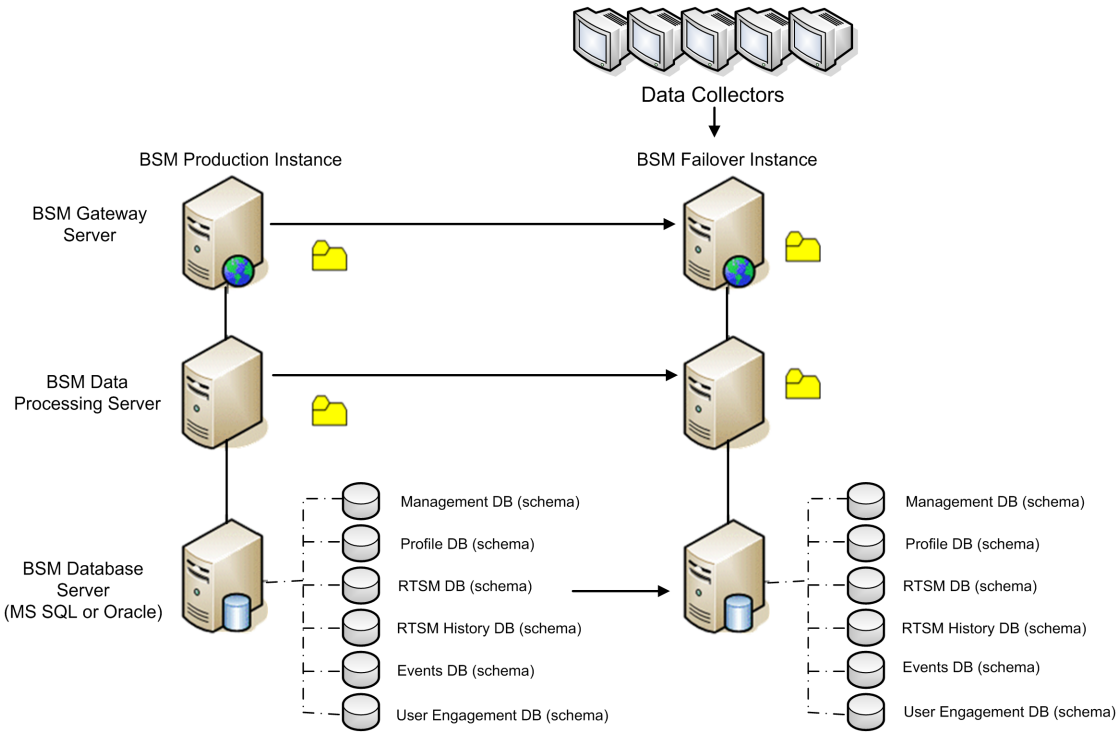
   For details, see “Using TLS in BSM” in the BSM Hardening Guide.

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:


Data Collectors
BSM Production Instance
BSM Failover Instance
BSM Gateway Server
BSM Data Processing Server
BSM Database Server (MS SQL or Oracle)
Management DB (schema)
Profile DB (schema)
RTSM DB (schema)
RTSM History DB (schema)
Events DB (schema)
User Engagement DB (schema)
Management DB (schema)
Profile DB (schema)
RTSM DB (schema)
RTSM History DB (schema)
Events DB (schema)
User Engagement DB (schema)

2. Configuring failover data collector connections.

If any of the data collectors used SSL, you should add their certificates to BSM.

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	In all cases, do the following:
	a. Go to **SiteScope** > **Preferences** > **Integration preferences**.
	b. Select your BSM integration and update the BSM IP address .
	c. Click **Re-Synchronize**.
	Note: If SiteScope just changed its hostname, perform step **e** and **f** only.
	d. From SiteScopeA, use the Sitescope ConfigTool to Export Data (including the log files) to the file **SitescopeOrig.zip**.
	e. Turn off both SiteScopeA and SiteScopeB and change the service on SitescopeA to **disabled**.
	f. Copy **SitescopeOrig.zip** to the SiteScopeB machine.
	g. Run the ConfigTool on SiteScopeB to import the data using the **SitescopeOrig.zip** file. Do not start SiteScopeB.
	h. On the BSM gateway machine, open **<HPBAC Dir>\Tools\TopazBrowser** and run the following SQL queries against the BSM management database:
	◦ In the HOST table, identify the record that contains information from SiteScopeA :
	`select * from hosts`, identify the record that pertains to SiteScopeA and record the **H_ID** and **H_LocID** values and run
	`update hosts set h_name ='<NewHostName>' where h_id=<H_ID PreviouslyFound>`
	◦ In the LOCATIONS table, change the location to match the new value
	`select * from locations where l_locid=<H_LocID PreviouslyFoundFromHOSTS>`and run
	`update locations set L_LOCNAME='<NewHostName>' where l_locid=<H_LocID PreviouslyFoundFromHOSTS>`
	◦ In the SESSIONLOCATIONS table, locate the correct SESSION_ID
	`select * from sessionlocations where sl_locid=<H_LocID PreviouslyFoundFromHOSTS>` and record the **SESSION_ID** from the record found.
	◦ In the SESSION_SITESCOPE_PROPS table, modify the

Data Collector	Procedure
	SiteScope properties to match the new host: `select * from session_sitescope_props where session_id=<Session_ID PreviouslyFound>`, verify that this is the correct record and run `update session_sitescope_props set SITESCOPE_HOST='<NewHostName>',SITESCOPE_LOCATION='<NewHostName>' where session_id=<Session_ID PreviouslyFound>` i. Start SiteScopeB.
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.

Chapter 11: Staging Mode

The Staging Data Replicator (SDR) takes the data coming into your source environment and copies it to the staging environment. The SDR does not transfer event data.

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

Chapter 12: Staging Data Replicator

Staging Data Replicator - Overview 89

Running the Staging Data Replicator (Standalone) 90

Verifying that the SDR Server Can Communicate with the Production Server 92

Unsubscribing the Staging Data Replicator from the Source Server 93

Running the SDR with Basic Authentication 94

Enable Event Receiving on the Production System 95

SSL Configuration for the Staging Data Replicator 96

Staging Data Replicator - Overview

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

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

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

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

HPBSMSDR\conf\ core\Tools\log4j\sdreplicator\sdreplicator.properties

This tool is only supported in staging mode. For more information about staging mode, see "Staging vs. Direct Upgrade Overview" on page 1.

In Linux, you can change the installer working directory (default /tmp) by running the following commands:

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

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

where `/new/temp` is the new /temp directory.

The SDR must be installed on a machine in the same network as the production environment, with the ability to access the staging environment. If the staging server cannot communicate with the production server, the SDR must be installed as a standalone utility on a different machine.

For task details, see "Running the Staging Data Replicator (Standalone)" on the next page.

Running the Staging Data Replicator (Standalone)

To use the Staging Data Replicator standalone utility:

1. To use the Staging Data Replicator as a standalone utility, you must install it on a separate machine with access to both your production and staging servers.

   - To check that the SDR server can connect to the staging server, enter the following url in an any internet browser from the standalone server:

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

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

   - Check that the SDR server can connect to the production server. For details, see "Verifying that the SDR Server Can Communicate with the Production Server" on page 92.

2. Run the appropriate replicator file.

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

   b. Click **Search**.

   c. For Windows, select **Application Performance Management (BAC) > 9.26 > Windows**).

      For Linux, select **Application Performance Management (BAC) > 9.26 > Linux**).

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

   e. Locate the Staging Data Replicator package and save it locally.

   f. Launch the relevant setup file.

3. Follow the on-screen instructions to install the Staging Data Replicator. Select the type of deployment based on the version of your source environment.

4. After you have completed the Staging Data Replicator installation, open the **<Staging Data Replicator root directory>\conf\b2G_translator.xml** file and modify the following:

   - **_SOURCE_HOST_NAME_.** Replace this with the host name of the source (production) BSM Gateway Server. If you have more than one Gateway Server, you can use the name of any of them for this value.

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

<ForwardURL url="http://__DESTINATION_HOST_NAME__/ext/mod_mdrv_wrap.dll?type=md_sample_array&acceptor_name=__DESTINATION_HOST_NAME__&message_subject=topaz_report/samples&request_timeout=30&force_keep_alive=true&send_gd=true"/>

- **clientid="".** If you do not require guaranteed delivery of data when the Staging Data Replicator stops running, delete the value for this parameter. It is generally recommended that you do not modify this parameter.

5. If the web server on the staging server uses basic authentication, the SDR cannot communicate with the staging server unless you run the **basicauth** tool. For details, see "Running the SDR with Basic Authentication" on page 94.

6. If the web server on the staging server uses SSL, you will need to perform custom configurations to allow the SDR to communicate with the staging server. For details, see "SSL Configuration for the Staging Data Replicator" on page 96.

7. Begin running the Staging Data Replicator.

   - Windows: Select **Start > HP BSM Staging Data Replicator > Administration > Enable HP BSM Staging Data Replicator**.

     Verify that the SDR is running by looking for **hpbsmsdr** in the Windows Task Manager.

   - Linux: Run the following command:
     <SDR installation directory>/scripts/run_hpbsmsdr.sh start

     Verify that the SDR is running searching for the hpbsmsdr process (for example: **ps -ef | grep hpbsmsdr**)

8. After starting the SDR, copy the **<SDR installation directory>/dat/sdr/SDRBusConnectionStartTime.properties** file from the SDR server to the staging Gateway server in the **<BSM home directory>/dat/sdr** directory.

9. After you have completed the staging process and are prepared to move your staging environment to a production environment, stop the Staging Data Replicator.

   - Windows: Select **Start > HP BSM Staging Data Replicator > Administration > Disable HP BSM Staging Data Replicator**.

   - Linux: Run the following command:
     <SDR installation directory>/scripts/run_hpbsmsdr.sh stop

10. Unsubscribe the staging data replicator from the source server. For details, see "Unsubscribing the Staging Data Replicator from the Source Server" on page 93.

Verifying that the SDR Server Can Communicate with the Production Server

1. Ping the production server.

    a. Ping the production Gateway Server from the SDR server using the Gateway Server's short name. If this works, continue to step 2. If it does not work, continue with step 1 b.

    b. Ping the production Gateway Server from the SDR server using the Gateway Server's fully qualified domain name. If this works, open the relevant **hosts** file for your operating system and add the mapping between the production Gateway Server name and its IP address.

2. Verify connection.

    a. **Production Gateway Server runs Windows:** Run **ipconfig** on the production Gateway Server.

    Production Gateway Server runs Solaris/Linux: Run **ifconfig -a** on the production Gateway Server.

    b. Verify all the listed IP addresses are open to connection to and from the server running the SDR.

    If this is not feasible, contact HP Software Support.

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

Unsubscribing the Staging Data Replicator from the Source Server

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

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

To unsubscribe the SDR:

1. Stop the SDR.
    a. Open the Nanny Manager jmx console from **http://<machine name>:11021**, where **<machine name>** for an embedded SDR is the name of the Load Balancer (if it exists) or destination BSM Gateway Server. For a Standalone SDR, **<machine name>** is **localhost**.
    b. Select **Foundations: type=NannyManager**
    c. Open **showServiceInfoAsHTML**
    d. Stop the **HPBSMSDR-x.x** process.
2. Open the **<Staging Data Replicator root directory>\conf\b2G_translator.xml** file and locate the <Message Selector> element(s).
3. Within the **<Message Selector>** element(s), replace the attribute value of enabled to 0 (the default is **enabled="1"**) in the following line:

    <MessageSelector name="customer_name" value="Default Client" enabled="0" />
4. Start the SDR.
    a. Open the Nanny Manager jmx console from **http://<machine name>:11021**, where **<machine name>** for an embedded SDR is the name of the Load Balancer (if it exists) or destination BSM Gateway Server. For a Standalone SDR, **<machine name>** is **localhost**.
    b. Select **Foundations: type=NannyManager**
    c. Open **showServiceInfoAsHTML**
    d. Start the **HPBSMSDR-x.x** process.
5. Wait several minutes, and then stop the SDR as described in step 1.

Running the SDR with Basic Authentication

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

To configure SDR to work with basic authentication:

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

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

Where:

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

-standalone is for a standalone SDR

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

disabled is to disable basic authentication.

Enable Event Receiving on the Production System

Enable event receiving on the production system as follows:

1. Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. In the applications field, select **Operations Management** and locate the **Event Pipeline Receiver Settings** table. Set **Disable receiving of Events** to **false**.

SSL Configuration for the Staging Data Replicator

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

To configure the SDR to support SSL:

1. Configure SDR to use SSL.

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

2. Configure the SDR to trust the BSM certificate.

   a. Obtain a copy of the certificate used by the web server on the BSM Gateway Server or certificate of Certificate Authority that issued BSM web server certificate. This file must be a DER encoded binary X.509 (.CER) file.

   b. Import the above-mentioned certificate into SDR's truststore. For details, see the BSM Hardening Guide.

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

      Example:

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

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

      Locate the following line:

      ```
      SET PROCESS_OPTS=%PROCESS_OPTS% -Dconf.file=%PRODUCT_HOME_PATH%\conf\b2g_
      translator.xml -Dprop.file=%PRODUCT_HOME_PATH%\conf\b2g_
      translator.properties -Dmsg.filter.file=%PRODUCT_HOME_
      PATH%\conf\includedSamples
      ```

      At the end of this line, add the following:

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

      -Dnet.ssl.trustStorePassword=passphrase
      ```

Part 4: Troubleshooting

Chapter 13: Installation and Connectivity Troubleshooting

Installation Fails Due to IIS Web Server Custom Configuration Changes

The following is a workaround if the BSM 9.26 upgrade fails. This failure may occur if any custom configuration changes were made to the IIS web server on the BSM server.

Before running this procedure, save the details of your custom IIS configuration. Remember that the Backup and Restore procedure is not applicable since after the Restore step the BSM configuration could be reset. Therefore, you need to manually restore your custom settings after running this procedure.

1. Stop BSM.
2. Open Run as Administrator PowerShell command prompt (small blue icon on taskbar, next to Server Manager).
3. In the PowerShell command prompt, run the following commands in order to save existing IIS configuration information for subsequent recovery steps:
   a. `Set-ExecutionPolicy RemoteSigned` (Click enter twice.)
   b. `Import-Module WebAdministration` (Click enter.)
   c. `Get-WebBinding -Name "Default Web Site"` Save the output, protocol, and binding Information.
   d. `etsh http show sslcert` Save the output, Certificate Hash, and Application ID.
4. To remove all bindings information from IIS run the following:

   ```
   Get-WebBinding -Name "Default Web Site" | Remove-WebBinding
   ```

5. Change the URLPort value to **80** in the **HPBSM_postinstall\userInputs.user** file.
6. Run the BSM 9.26 upgrade procedure.
7. Open a regular command prompt window with administrator privileges and run the commands below, with the values you save above.

a. `C:\Windows\system32\inetsrv\appcmd set site /site.name:"Default Web Site" /+bindings.[protocol='http',bindingInformation='*:80: [FQDN host name] ']`

b. `C:\Windows\system32\inetsrv\APPCMD set site /site.name:"Default Web Site" /+bindings.[protocol='https',bindingInformation='*:443: [FQDN host name] ']`

c. `netsh http add sslcert ipport=0.0.0.0:443 certhash= <Certificate Hash> appid={<Application ID>}`

For example:
`netsh http add sslcert ipport=0.0.0.0:443 certhash=bf5126df5bc1b511faf769e7d1be89ce9dd06d5f appid={4dc3e181-e14b-4a21-b022-59fc669b0914}`

8. Restart BSM.

After installing BSM 9.26 installation, 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.

Cannot log in to LDAP after upgrade

Description: The upgrade process could not reuse an LDAP configuration created before BSM version 9.25. Therefore, newly created users are not able to log in to LDAP. This is because support for multiple LDAPs was added in BSM version 9.25.

Workaround: After upgrading from BSM version 9.24 or earlier to version 9.25 or later, reconfigure LDAP.

JBoss does not start when there are two enabled NICs

Description: JBoss does not start when there are two enabled NICs.

Workaround: There is a known issue with JBoss 7 (used by BSM 9.26) when there are multiple NICs (LANs) on the box. To resolve this problem, install the following hotfix on top of BSM 9.26 IP1 **https://patch-central.corp.hpecorp.net/crypt-web/protected/viewContent.do?patchId=QCCR1I118920_HOTFIX**.

Server is not ready message

Desciription: 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.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on BSM Upgrade Guide - 9.2x to 9.26 (Business Service Management 9.26)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Sw-doc@hpe.com.

We appreciate your feedback!