HP Business Service Management

For the Windows, Linux operating systems

Software Version: 9.23

BSM - Operations Manager Integration Guide

Document Release Date: December 2013

Software Release Date: December 2013

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

Acknowledgements

This product includes software developed by the Apache Software Foundation (www.apache.org).

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

This product includes software developed by the MX4J project (mx4j.sourceforge.net).

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

BSM OMi - HP Operations Manager Integration Overview

Operations Manager (HPOM) can be integrated into your BSM environment to become a data source for BSM Operations Management. Both Operations Manager for Windows and Operations Manager for UNIX (HP-UX and Linux) are supported.

After you have installed both BSM and HP Operations Manager (HPOM), follow the procedures described in this chapter to connect BSM and HPOM. This connection enables bi-directional synchronization of events between the two systems, tool execution, and instruction text retrieval. The connection configuration requires you to establish a trust relationship between BSM and the HPOM systems, and configure a message forwarding policy.

Note: You must have an Event Management Foundation license to use this functionality.

The integration between BSM and Operations Manager (HPOM) provides you with the following capabilities:

- **HPOM events > Operations Management.** If you have an Event Management Foundation license, events from HPOM are displayed in the Event Browser in Operations Management.
- **HPOM events > BSM health indicators.** After you set up the previous integration, if the HPOM events have corresponding health indicators defined, these health indicators automatically affect the status of the relevant Configuration Items (CIs) in BSM applications such as Service Health and Service Level Management.

  For an introduction to health indicators, see Health Indicators and KPIs in the BSM User Guide.
- **Operations Management Actions, Tools, and Instructions.** You can specify tools, for example, to ping a system. These tools are launched from events or from the Actions panel and run on the associated CI. Tools are designed to help users solve common problems quickly and efficiently. All available tools are launched in the context of a configuration item. The selection of tools a particular user sees in context menus depends on the tools that are available for the configuration item affected by a particular event.

  Events received in the Event Browser from HPOM may contain event-related actions configured in HPOM. If event-related actions exist, you can run these actions from the BSM Operations Management console. HPOM actions can be either operator-initiated, or can run automatically when an event occurs. For a complete overview of available actions and how to run them, see the BSM Operations Management online help.

  Operators working with the HPOM message browser can see additional instructions for the selected message. It is equally helpful for Operations Management operators to be able to access this information when using HPOM servers to forward events to Operations Management. This information is displayed in the Instructions tab of the Event Browser.

  For details, see Event Perspectives and Tools in the BSM User Guide.
- **HPOM topology > RTSM topology.** If you have the Event Management Foundation license enabled, the HPOM topology can synchronize with the BSM RTSM topology. Using topology

synchronization the OM Services are synchronized with BSM, and using corresponding mapping rules they are transformed into CIs stored in the RTSM.

For details, see Topology Synchronization in the BSM Application Administration Guide.

Note: If the HPOM topology is not synchronized with the RTSM topology using the OMi (dynamic) topology synchronization mechanism, the **Monitored by** property of the BSM CIs corresponding to the HPOM services may be empty. As a consequence, these CIs are not displayed in the System Monitors only Perspective, System Hardware Monitoring, and System Software Monitoring views.

Workflow: Configuring the Connections Between BSM OMi and HPOM

1. ## Establish a Trust relationship between BSM and external servers

   For connection and communication between BSM and HPOM hosts, establish a trust relationship between all the servers.

   For task details, see "How to Establish a Trust Relationship for a Server Connection" on page 9.

   To verify the trusted relationship, see "How to Verify the Trusted Relationship" on page 12.

2. ## Set up the HPOM Management Server system as a Connected Server

   Set up the HPOM server as a connected server so that you can run actions and tools from Operations Management, and retrieve instructions from the HPOM server.

   For task details, see "How to Create a Connection to an HPOM Server" on page 13.

3. ## Configure the HPOM forwarding policy

   To enable event synchronization between HPOM and BSM, set up a message forwarding policy on the HPOM management server. The policy includes the node name of the target BSM server. Alternatively, specify the load balancers, if configured, or one Gateway Server for each BSM installation, as appropriate for your high availability arrangement.

   - **HPOM for UNIX.** For task details, see "How to Configure the HPOM for UNIX Forwarding Policy" on page 20.
   - **HPOM for Windows.** For task details, see "How to Configure the HPOM for Windows Forwarding Policy" on page 17.

4. ## Import content packs *(optional)*

   The Operations Management application in BSM uses content packs to exchange customized configuration data between BSM installations. Import the relevant content packs.

   For task details, see "How to Import Content Packs (Optional)" on page 26.

5. ## Validate event synchronization

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

   For task details, see "How to Validate Event Synchronization" on page 24.

6. ## Configure Packages in Operations Management Infrastructure Settings

   List the packages that are used for Topology Synchronization.

For task details, see "How to Configure the Packages used for Topology Synchronization" on page 28.

7. ## Synchronize the topology

   To populate the BSM database (RTSM) with configuration item (topology) and service data from HPOM, you need to perform Topology Synchronization. Topology synchronization is configured to update all specified servers with the topology and service data from the HPOM management server.

   For task details, see "How to Run Dynamic Topology Synchronization" on page 30.

8. ## Manage BSM with HPOM *(optional)*

   You can manage BSM servers with HPOM by installing and configuring an HP Operations Agent. For details, see the section appropriate for your HPOM installation:

   - **HPOM for UNIX.** For task details, see "How to Manage a BSM Host System with HPOM for UNIX or Linux (Optional)" on page 37.
   - **HPOM for Windows.** For task details, see "How to Manage a BSM Host System with HPOM for Windows (Optional)" on page 35.

How to Establish a Trust Relationship for a Server Connection

For connection and communication between BSM and external servers such as HPOM hosts, other BSM hosts where Operations Management is running, or a BSM Server with an event channel license, you must establish a trust relationship between the systems.

In HPOM Server Pooling, the virtual server must have a certificate which is trusted by all HPOM hosts in the server pool and by all BSM hosts where Operations Management is running.

> **Note:** Generally, the trust relationship must be set up on all nodes (Data Processing Servers, Gateway Servers, manager of manager configurations, load balancers, and reverse proxies). However, some load balancer technologies include a by-pass or pass-through functionality for incoming encrypted messages to its pool members. When using such technologies, trust relationship on the load balancer node is not required, if you are load balancing on the recommended OSI level 2 or 4.

To establish a trust relationship between the Data Processing Servers and external servers:

1. Copy the **opr-cli.jar** file and the **BBCTrustServer** script file to your HPOM server host system from the BSM Data Processing Server system:

   > **Note:**
   >
   > **HPOM for Windows:** Starting with patches OMW_00121 (32-bit) and OMW_00122 (64-bit), the **BBCTrustServer** tool is already installed to the folder **%OvInstallDir%\contrib\OVOW** on the HPOM for Windows management server.
   >
   > **HPOM for UNIX:** Starting with patches Patch PHSS_42736 (HP-UX), OML_00050 (Linux), and ITOSOL_00772 (Solaris), the **BBCTrustServer** tool is already installed to the directory **/opt/OV/bin** on the HPOM for UNIX or Linux management server.
   >
   > If you have the appropriate patch installed, you can skip this step.

   a. Locate the following files on the BSM Data Processing Server:

      <HPBSM root directory>/opr/lib/cli/opr-cli.jar

      <HPBSM root directory>/opr/bin/BBCTrustServer.bat

      <HPBSM root directory>/opr/bin/BBCTrustServer.sh

   b. *HPOM for Windows only:* Copy the files to the computer that is running the HPOM for Windows management server.

      Copy **opr-cli.jar** to **%OvInstallDir%\java\opr-cli.jar**.

      Copy **BBCTrustServer.bat** to **%OvBinDir%\BBCTrustServer.bat**.

   c. *HPOM for UNIX or Linux only:* Copy the files to the computer that is running the HPOM for UNIX or Linux management server.

Copy **opr-cli.jar** to **/opt/OV/java/opr-cli.jar**.

Copy **BBCTrustServer.sh** to **/opt/OV/bin/BBCTrustServer.sh**.

Change the permissions of the **BBCTrustServer** tool by entering the following command:

chmod 555 /opt/OV/bin/BBCTrustServer.sh

2. On the HPOM server, execute the following command:

   BBCTrustServer.[bat|sh] <*load_balancer_or_single_gateway_server_or_RP_or_Server_Pool_Virtual_Interface*>

3. On the BSM Data Processing Server, execute the following command:

   BBCTrustServer[.bat|sh] <*external_server*>

   Replace **<*external_server*>** with the DNS name of the external system (for example, `ommgmtsv`).

   > **Note:** The value of *<external_server>* should be the virtual name in case of HPOM server pooling.

   When asked whether to add the certificate to the trust store, enter: **y**.

   The tool informs you if a trusted certificate already exists and asks you whether to overwrite the existing certificate. To replace the existing certificate with the new one, enter: **y**.

4. If your load balancer is configured to work on **OSI levels 2 or 4**, execute the following command on the external system (for OSI level 7, see the next step):

   BBCTrustServer.[bat|sh] <*load_balancer_or_single_gateway_server_or_RP_or_Server_Pool_Virtual_Interface*>

   a. When asked whether to add the certificate to the trust store, enter: **y**.

   b. The tool informs you if a trusted certificate already exists and asks you whether to overwrite the existing certificate. To replace the existing certificate with the new one, enter: **y**.

5. If your load balancer is configured to work on **OSI level 7**, you must exchange the certificates manually follows (for OSI levels 2 or 4, skip this step):

   a. On a BSM Processing Server, execute the following command: **ovcert -exporttrusted -file omi.cer**.

   b. On the external machine, execute the following command: **ovcert -exporttrusted -file other.cer**.

   c. Copy **other.cer** from the external machine to a BSM Processing Server.

   d. Copy **omi.cer** from the BSM Processing Server to the external server.

   e. On the BSM Processing Server, execute the following commands: **ovcert -importtrusted -file other.cer** and **ovcert -importtrusted -file other.cer -ovrg server**.

   f. On the external server, execute the following commands: **ovcert -importtrusted -file omi.cer** and **ovcert -importtrusted -file omi.cer -ovrg server**.

6. If you are using a load balancer, where your data sources are not communicating directly with the BSM Gateway Servers, make sure that Port 383 is routed through the load balancer to the BSM Gateway Servers.

   If the load balancer/reverse proxy is configured to pass through traffic directly (OSI level 2 or 4), skip to the next step. If it is configured to work on level 7, perform the following. (Note that HP recommends to use levels 2 or 4.)

   - The certificate on the load balancer must be installed for port 383 (or the port that you have configured for secure communication).
   - Communication between the load balancer and the gateway systems must be secured.
   - The load balancer must possess a server certificate for authentication so that external servers such as HPOM can connect successfully. The load balancer must also validate client certificates presented by external clients (for example, HPOM management servers).
   - The load balancer must possess a client certificate for authentication with BSM.

   a. Issue a certificate for the load balancer from the BSM Data Processing server with the following command:

      ovcm -issue -file <*certificate file*> *-name* <*Fully Qualified Domain Name of Virtual Interface*> [-pass <*passphrase*>]

   b. Import this certificate as server and client certificate into your load balancer.

      For details on the required format, refer to your load balancer documentation. You can use openssl to convert the certificates into the required format.

7. Check the connection between the servers. For details, see "How to Verify the Trusted Relationship" on the facing page.

How to Verify the Trusted Relationship

After establishing a trust relationship between the BSM Data Processing Server and external systems, check the connection between the two systems.

To check the connection between the BSM server environment and an external system:

1. From the external host, verify that communication to the BSM installation is possible (the return value should be `eServiceOk`) by executing the following command on the external server system:

   bbcutil -ping https://<*load_balancer_or_single_gateway_server_or_RP_or_Server_Pool_Virtual_Interface*>

   Example of the command result:

   ```
   https://<HP BSM servername>: status=eServiceOK
   coreID=7c66bf42-d06b-752e-0e93-e82d1644cef8 bbcV=06.10.105
   appN=ovbbccb appV=11.03.031 conn=1 time=1094 ms
   ```

2. From all HP BSM Gateway Server hosts, verify that communication with the external server host is possible (the return value should be `eServiceOk`) by executing the following command on each Gateway Server host:

   bbcutil -ping https://<*external server hostname*>

   Example of the command result:

   ```
   https://<external_host_server_name>: status=eServiceOK
   coreID=0c43c032-5c94-7535-064a-f7654a86f2d3 bbcV=06.10.070
   appN=ovbbccb appV=11.03.031 conn=7 time=140 ms
   ```

Troubleshooting:

If the **bbcutil –ping** command executes but does not return **eServiceOk**, you may need to stop and start ovc as follows:

- Linux: **/opt/OV/bin/ovc –kill**, and **/opt/OV/bin/ovc –start**
- Windows: **ovc –kill** and **ovc –start**.

How to Create a Connection to an HPOM Server

This task shows you how to create a server connection to an HPOM server. Operations Management can forward events, run actions and tools on, and retrieve instructions from an HPOM server. Credentials for the HPOM web service are required for this processing.

For Server Pooling environments, configure the virtual interface as the main connected server. Specify the integration user and password for the Outgoing Connection. For all physical servers in the server pooling environment, add them as connected servers and specify the virtual interface server as the server to use for the Outgoing Connection.

> **Note:** To use Operations Management Administration areas, you must be granted permission to work with these or a subset of these. For details, see How to Set Operations Management User or Group Permissions in the BSM Application Administration Guide.

To create a server connection to an HPOM server:

1. Open the Connected Servers manager from Operations Management Administration:

   Admin > Operations Management > Setup > Connected Servers

2. In the Connected Servers pane, click the ✱ button to open the Create New Server Connection dialog box.

3. Enter a display name, a unique internal name, if you want to replace the automatically generated name, and (optional) a description of the connection being specified.

4. Select **Active**, if you want to enable the server connection immediately.

5. Click **Next** to open the Server Type page.

6. Select the HP Operations Manager server type.

7. Click **Next** to open the Server Properties page.

8. Enter the fully qualified DNS name of the host system of the HPOM management server.

   If the host system is a high-availability cluster, enter the fully qualified DNS name of the cluster package where the HPOM server is installed.

   If HPOM is installed in a server pooling environment, add the virtual interface as the first HPOM management server. Add all physical pool servers separately as connected servers.

9. Enter the Integration User name used to log on to the HPOM management server.

   > **Note:** All messages forwarded from HPOM systems are treated as allowing read and write. Any changes made to these events result in a back synchronization to the originating HPOM server.

> For HP Operations Manager for Windows, the selected user must have at least PowerUser rights and must be a member of HP-OVE-Admins group and the local administrators group.
>
> For HP Operations Manager for UNIX, the Integration User must have HPOM administrator rights (for example, opc_adm) to be able to synchronize topology and execute tools.

10. *Optional:***Advanced Delivery Options** It is possible to customize the way events and change notifications are delivered to this server. The available options are:

    - **Serial** — Events and change notifications are delivered serially in the order that they were received.
    - **Serial per Source** — *(Default)* Each originating server is provided with a dedicated outgoing request delivery path. For each individual outgoing request delivery path, events and change notifications are delivered serially in the order that they were received. This can increase the throughput for delivery of events and change notifications when many events are received from multiple originating servers, while maintaining the incoming order.
    - **Parallel** — The configured number of outgoing request delivery paths are used when forwarding events and change notifications. This can further increase the throughput for delivery of events and change notifications. However, because the source of the event is not considered, maintenance of the incoming order cannot be guaranteed.

    Open the Advanced Delivery Options and select the Event Forwarding and Change Notification method. Serial per Source is the default.

11. Specify if you want to forward dynamic topology information from the Operations Manager i instance to which you are logged on, to the HPOM instance that you are currently configuring.

    > **Note:** If you change the status of the **Forward Dynamic Topology to this Target Server** check box for a configured server, you must restart the WDE process on all gateway servers.

12. Select the HPOM product type. The options include:

    - HP Operations Manager for UNIX
    - HP Operations Manager for Windows

13. Click **Test Connection** to check that the specified connection attributes are correct. If an error link is displayed, check the error message, correct the connection information, and re-test the connection.

14. Click **Next** to open the Outgoing Connection page.

    The outgoing connection is used to receive instructions, and execute tools and actions on external nodes.

    > **Note:** If you are editing outgoing connection properties (for example, integration user,

> password, and port), you must restart the **MercuryAS** process for the changes to take effect.

15. If you are using an alternative server to provide instructions, and execute actions and tools, select **Use other Server**, and select a server from the list. For the physical servers in a server pooling environment, select the virtual interface connected server.

    Alternatively, if using this server that you are configuring for receiving instructions, and executing tools and actions on external nodes, enter the password for the integration user and the port required to access the server for receiving instructions, and executing tools and actions. The default port value is automatically inserted and can be restored using **Set default port**.

    > **Note:** For HP Operations Manager for Windows, the selected user must have at least PowerUser rights and must be a member of HP-OVE-Admins group and the local administrators group.
    >
    > For HP Operations Manager for UNIX, the Integration User must have HPOM administrator rights (for example, opc_adm) to be able to synchronize topology and execute tools.

16. *Optional:* If you are using secure communication (default), make sure that the **Use Secure HTTP** option is selected, and apply a certificate using one of the following methods.

    > **Note:** Secure communication is necessary for Server Pooling Environments. However, do not use the `Import from file` or `Retrieve from server` options.
    >
    > Set up a trusted relationship between all HPOM and BSM servers as described in "How to Establish a Trust Relationship for a Server Connection" on page 9.

    - **Import from file** — Opens the file browser and enables you to navigate to and specify a Base64 Encoded X.509 certificate file for the server connection.
    - **Retrieve from server** — Retrieve a certificate from the host system specified in this server connection.

    Alternatively, if you want actions to be run from an alternative server, select **Use Other Server** and select an HPOM server from the list of configured servers.

    > **Note:** Avoid selecting an alternative action execution server which creates a loop and results in specifying the connected server as the action execution server. Select an alternative action execution server or use the **Use this Server** option.

17. Click **Test Connection** to check that the specified connection attributes are correct. If an error link is displayed, check the error message, correct the connection information, and re-test the connection.

18. Select **Finish**.

> **Note:** In a clustered HP Operations Manager for Windows environment, IIS on all cluster nodes must have the same certificate. If different, valid certificates are used, problems such as tools execution may be experienced after switching to a node with a different certificate.
>
> If you are editing outgoing connection properties, for example, integration user (located in Server Properties), password, and port, you must restart the **MercuryAS** process for the changes to take effect.

19. If the HPOM server is connected to BSM using a load balancer, the URL of the load balancer (`http://<load balancer>:80`) must be specified in the infrastructure setting:

    Foundation > Platform Administration > Host Configuration > Default Virtual Gateway Server for Data Collectors URL

    > **Note:** If you omit this setting, event synchronization might get confused as it is using the wrong sender hostname (the physical gateway server in place of the virtual system name.

How to Configure the HPOM for Windows Forwarding Policy

To enable event synchronization between HPOM and BSM, set up a message forwarding policy on the HPOM management server. The policy includes the node name of the target BSM server. Alternatively, specify the load balancers, if configured, or one Gateway Server for each BSM installation, as appropriate for your high availability arrangement.

Before setting up a policy and to avoid overwriting the current settings, verify whether a policy of the type **Server-based Flexible Management** is already active on the HPOM for Windows server. If a policy does not exist, create a new policy as described in the section "Create a New Policy" below. If a policy already exists and is active, adapt the policy as described in the section "Adapt an Active Policy" on the facing page.

> **Note:** The following sections relate to HPOM for Windows; for details on HPOM for UNIX see "How to Configure the HPOM for UNIX Forwarding Policy" on page 20.

Create a New Policy

To set up a new policy on HPOM for Windows, complete the following steps:

1. Start the HPOM for Windows console as follows:
   Start > Programs > HP > HP Operations Manager

2. In the left pane of the HPOM for Windows console, select the following:
   Policy management > Policies grouped by type > Server Policies > Server-based Flexible Management

3. Verify that no Server-based Flexible Management policy exists. If such a policy does exist, go to "Adapt an Active Policy" on the facing page.

4. Right-click **Server-based Flexible Management** (or a blank space in the right pane) and select **New > Policy**.

   The Server-based Flexible ManagementEditor dialog opens.

5. In the **General** tab text pane, insert the following policy text:

```
TIMETEMPLATES
# none
RESPMGRCONFIGS
   RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
   SECONDARYMANAGERS
   ACTIONALLOWMANAGERS
   MSGTARGETRULES
      MSGTARGETRULE DESCRIPTION "Forward all messages rule"
         MSGTARGETRULECONDS
         MSGTARGETRULECOND DESCRIPTION "Forward all messages"
         MSGTARGETMANAGERS
            MSGTARGETMANAGER
            TIMETEMPLATE "$OPC_ALWAYS"
            OPCMGR IP 0.0.0.0 "<HP BSM fully qualified host name>"
```

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

6. Replace `<HP BSM fully qualified host name>` in the policy text with the fully-qualified hostname of the Gateway server to receive HPOM messages (for example, `HPGwSrv.example.com`).

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

7. Click **Check Syntax** to check for syntax errors in the new policy text.

8. After correcting any syntax errors, click **Save and Close**.

9. In the Save As dialog box that opens, enter a name and description for the new policy.

10. Click **OK** to close the Save As dialog.

11. From the Policy Management folder, right-click the policy and select:

    All Tasks > Deploy on

    The Deploy server policy on dialog box opens.

12. In the Deploy server policy on dialog box, select the name of your HPOM management server.

13. Click **OK** to deploy the server-based flexible management policy on the HPOM for Windows management server.

Adapt an Active Policy

If a message-forwarding policy already exists on the HPOM for Windows system, perform the following instructions to edit this policy and add another message target manager to it.

1. Start the HPOM for Windows console as follows:
   Start > Programs > HP > HP Operations Manager

2. In the left pane of the HPOM for Windows console, select the following:
   Policy management > Server policies grouped by type > Server-based Flexible Management

3. In the right pane of the HPOM for Windows console, double-click the existing policy that you want to edit. The Server-based Flexible Management Editor dialog opens.

   If such a policy does not exist, go to "Create a New Policy" on the previous page.

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

   ```
   TIMETEMPLATES
   # none
   RESPMGRCONFIGS
   ```

```
RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
SECONDARYMANAGERS
ACTIONALLOWMANAGERS
MSGTARGETRULES
   MSGTARGETRULE DESCRIPTION "Forward all messages rule"
      MSGTARGETRULECONDS
      MSGTARGETRULECOND DESCRIPTION "Forward all messages"
      MSGTARGETMANAGERS
         MSGTARGETMANAGER
         TIMETEMPLATE "$OPC_ALWAYS"
         OPCMGR IP 0.0.0.0 "<First Target Manager>"

         MSGTARGETMANAGER
         TIMETEMPLATE "$OPC_ALWAYS"
         OPCMGR IP 0.0.0.0 "<HP BSM fully qualified host name>"
```

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

5. Replace `<HP BSM fully qualified host name>` in the text with the fully qualified hostname of the Gateway server that should receive HPOM messages (for example, `HPGwSrv.example.com`).

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

6. Click **Check Syntax** to check for syntax errors in the new policy text.

7. After correcting any syntax errors, click **Save and Close**.

Redeploy the server-based flexible management policy on the HPOM for Windows management server.

How to Configure the HPOM for UNIX Forwarding Policy

To enable event synchronization between HPOM and the Operations Management application in BSM, you must set up a message forwarding policy on each HPOM management server with the node name of the load balancer, if configured, or one Gateway Server, as appropriate for your high-availability arrangement.

Before setting up a policy, make sure that the forwarding target is set up as node (see "How to Set Up a Forwarding Target in the HPOM for UNIX Node Bank" on page 23). In addition, verify whether the **msgforw** message forwarding policy is already active on the HPOM server. If the **msgforw** message forwarding policy does not exist, create a new policy as described in the section "Create a New Policy" below. If the **msgforw** message forwarding policy already exists and is active, adapt the policy as described in the section "Adapt an Active Policy" on the next page.

> **Note:** The following sections relate to HPOM for UNIX; for details on HPOM for Windows see "How to Configure the HPOM for Windows Forwarding Policy" on page 17.

Create a New Policy

To set up a new message forwarding policy on HPOM, complete the following steps:

1. Change to the `work_respmgrs` directory as follows:
   cd /etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs/

   > **Note:** Policy template files can be found in:
   > **/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs**

2. Create a new policy file using the following command:
   vi <policy file name>

3. Insert the following text in new policy file:

```
TIMETEMPLATES
# none
RESPMGRCONFIGS
   RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
   SECONDARYMANAGERS
   ACTIONALLOWMANAGERS
   MSGTARGETRULES
      MSGTARGETRULE DESCRIPTION "Forward all messages rule"
         MSGTARGETRULECONDS
         MSGTARGETRULECOND DESCRIPTION "Forward all messages"
         MSGTARGETMANAGERS
            MSGTARGETMANAGER
            TIMETEMPLATE "$OPC_ALWAYS"
            OPCMGR IP 0.0.0.0 "<HP BSM fully qualified host name>
```

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

4. Replace `<HP BSM fully qualified host name>` in the text with the fully qualified hostname of the Gateway server that should receive HPOM messages (for example, `HPGwSrv.example.com`).

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

5. Enter the following command to check for syntax errors in the new policy text:
   /opt/OV/bin/OpC/opcmomchk -msgforw <policy file name>

6. After correcting any syntax errors, copy the policy to the **msgforw** policy file in the **respmgrs** directory as follows:

   cp <policy file name> /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/msgforw

7. Inform the server processes to re-read the configuration as follows:

   /opt/OV/bin/ovconfchg

   Message forwarding from HPOM to BSM is now configured and enabled.

Adapt an Active Policy

If the message forwarding policy already exists on the HPOM system, perform the following instructions to edit this policy and add another message target manager to it:

1. Change to the `work_respmgrs` directory as follows:
   cd /etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs/

   > **Note:** Policy template files can be found in:
   > **/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs/**

2. Edit the existing policy to which you want to add the BSM server as a target as follows:

   vi <policy file name>

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

```
# none
RESPMGRCONFIGS
   RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
   SECONDARYMANAGERS
   ACTIONALLOWMANAGERS
   MSGTARGETRULES
      MSGTARGETRULE DESCRIPTION "Forward all messages rule"
         MSGTARGETRULECONDS
         MSGTARGETRULECOND DESCRIPTION "Forward all messages"
```

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

   MSGTARGETMANAGER
   TIMETEMPLATE "$OPC_ALWAYS"
   OPCMGR IP 0.0.0.0 "<HP BSM fully qualified host name>"
```

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

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

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

5. Enter the following command to check for syntax errors in the new policy text:
   /opt/OV/bin/OpC/opcmomchk -msgforw <policy file name>

6. After correcting any syntax errors, copy the policy to the **msgforw** policy file in the **respmgrs** directory as follows:
   cp <policy file name> /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/msgforw

7. Inform the server processes to re-read the configuration as follows:

   /opt/OV/bin/ovconfchg

   Message forwarding from HPOM to Operations Management is now configured and enabled.

How to Set Up a Forwarding Target in the HPOM for UNIX Node Bank

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

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

```
/opt/OV/bin/OpC/utils/opcnode -add_node node_name=<node_name> net_type
=NETWORK_IP mach_type=<machine_type> group_name=<group_name> node_labe
l=<node_name>
```

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

- Linux: `MACH_BBC_LX26RPM_X64`
- Windows: `MACH_BBC_WIN2K3_X64`

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

- linux
- hp_ux
- solaris

How to Validate Event Synchronization

This section provides you with instructions about how to validate event synchronization and test the connection between HPOM and BSM.

> **Note:** Ensure that you have configured HPOM to enable BSM users to use tools, actions, and instruction text. You configure this in the Connected Servers manager in BSM. For details, see "How to Create a Connection to an HPOM Server" on page 13.

Verify Message Forwarding from HPOM to Operations Management

In this section, you check whether the message forwarding policy for sending messages from HPOM to Operations Management in BSM is correctly configured.

To check whether the message forwarding policy is correctly configured, complete the following steps:

1. Make sure the BSM servers are running.
2. Make sure at least one open message interface policy is deployed on your HPOM system. For instructions and details, see the *HP Operations Manager* documentation.
3. On the HPOM system, open a command or a shell prompt and create a new message by executing the following command:

   Windows:

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

   UNIX:

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

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

   > **Note:** If the message is sent multiple times, no new message is generated by HPOM. These messages are regarded as duplicates and only the message duplicate count is increased.
   >
   > To generate a new message, modify the message text for example as follows:
   >
   > UNIX:
   >
   > **/opt/OV/bin/OpC/opcmsg a=App o=Obj msg_text="Hello_002"**
   >
   > Windows:
   >
   > **opcmsg a=App o=Obj msg_text="Hello_002"**

Synchronize Operations Management Events with HPOM Messages

In this section, you check whether a change to an event in Operations Management which is already synchronized between the Operations Management application and HPOM is re-synchronized in HPOM.

To change the severity of an event, complete the following steps:

1. Make sure the BSM platform is running.
2. Log on to the BSM platform management console.
3. Select **Applications** > **Operations Management**.
4. In the Event Browser, select the event for which you want to change the severity. Choose an event that has been synchronized in HPOM and in BSM earlier and change its severity, for example, from minor to major.
5. Access the General tab of the Event Details pane.
6. From the Severity drop-down list, choose another severity (for example, major) and click **Save** to change it to the selected severity.
7. In HPOM event browser, verify the severity of this event and make sure it has been set to the new severity value.

How to Import Content Packs *(Optional)*

This section provides you with instructions about how to import content packs. These are stored on the Gateway Server servers. As a minimum, you need the content packs that match the HPOM Smart Plug-ins that you are using.

> **Note:** Content packs delivered with BSM are usually automatically imported from the default directory during installation and on every BSM startup.
>
> Any package that has not already been loaded, and which does not have unresolved package dependencies (references to packages, which are neither already loaded nor in the same folder), is loaded during this startup.
>
> For details, see the BSM Installation Guide.

The Operations Management application in BSM uses content packs to exchange customized configuration data between instances of the BSM installations. A content pack can contain a complete snapshot of all (or any part of) rules, tools, mappings, and assignments that you define and configure.

For more details about content packs and the Content Manager, see Content Packs in the BSM Platform Administration Guide.

To import content packs, complete the following steps:

> **Note:** To load all content packs delivered with BSM, you can use the following command line tool on the Data Processing Server:
> **<HPBSM>/bin/ContentManager**
>
> If you want to load the content packs individually, use the steps described in this section.

1. Open the Content Packs Manager: **Admin > Platform > Content Packs**

   Select the button in the **Content Pack Definitions** pane to open the Import Content Pack dialog box.

2. In the Import Content Pack dialog box, use the **Browse (...)** button to locate the content pack you want to import. Content packs are usually in ZIP format. However, XML format content packs can also be imported. Content Packs to be imported with the Content manager UI must reside on the system that the BSM browser is running on.

   The default location for content packs is:

   <HPBSM root directory>/conf/opr/content/<locale>

   In a distributed deployment, this directory is located on the Data Processing server.

   > **Note:** By default, BSM looks for content packs in the file system on the system where you start the browser session. If the browser is running on a remote system, you must navigate to the file system of the BSM host.

3. *Optional:* You can select **Test** to run the import in test mode. In test mode, changes are not committed, so you can see if any problems exist before running an actual import.

   Note: Existing items with the same ID are generally overwritten.

   If you are importing a predefined content pack, only predefined content is overwritten with new data. Customized content is left untouched. Importing a custom content pack always overwrites existing data.

   Unresolved references in the imported definition (for example, to unknown CI types) are not allowed.

4. Select **Import** to start the import or test operation.

   Note: It is not possible to start an import if an import is already running.

You can load other content packs you want to work with by following the same steps.

How to Configure the Packages used for Topology Synchronization

This task shows you how to specify the packages to be used by Topology Synchronization.

To specify the packages to be used by Topology Synchronization, configure the Packages for Topology Sync setting as follows:

1. Open Infrastructure Settings from the Platform Administration:

   Admin > Platform > Setup and Maintenance > Infrastructure Settings

2. Select **Applications** and use the list to set the administration context to **Operations Management**.

3. Go to the **HPOM Topology Synchronization Settings** section.

4. Open the **Packages for Topology Sync** (click the associated ✎ button to open the Edit Setting dialog box).

   The Edit Setting dialog box displays the values of the Topology Synchronization packages.

5. Specify all required Topology Synchronization packages in a semicolon-separated list in the **Value** field.

   For example, the packages specified by default are: `default;nodegroups;operations-agent`

   The topology synchronization packages are located in:

   `<HPBSM root directory>/conf/opr/topology-sync/sync-packages`

   The standatrd topology synchronization packages are:

   - `default`
   - `HPOprAds`
   - `HPOprBes`
   - `HPOprClu`
   - `HPOprExc`
   - `HPOprIis`
   - `HPOprJee`
   - `HPOprLys`
   - `HPOprMss`
   - `HPOprOra`
   - `HPOprSap`
   - `HPOprSys`

- `HPOprVir`
- `nodegroups`
- `operations-agent`

For example, if you are using the HP Operations Smart Plug-in for Oracle, include the `HPOprOra` topology synchronization package in the semicolon-separated list.

6. Select **Save**.

How to Run Dynamic Topology Synchronization

Before configuring forwarding of topology (node and service) data to Operations Management from Operations Manager management servers, complete the following configuration steps in Operations Management:

- Add the Operations Manager management server as a connected server in Operations Management. For details, see "How to Create a Connection to an HPOM Server" on page 13.
- Establish a trust relationship between the Data Processing Server and the Operations Manager management server. For details, see "How to Establish a Trust Relationship for a Server Connection" on page 9.
- *Optional:* Use the `opr-sdtool.bat` command-line tool to upload new or changed synchronization packages from the file system to the database. For details, see the Operations Manager i section of the *Extensibility Guide*.

After ensuring that the Operations Manager management server is added in Operations Management as a connected server, configure the forwarding of topology (node and service) data on the Operations Manager management server as described in the following section.

The following sections describe how to configure topology synchronization:

- "How to Configure Dynamic Topology Synchronization on HPOM for Windows Systems" below
- "How to Migrate from Scheduled Synchronization on HPOM for Windows Systems" on the next page
- "How to Configure Dynamic Topology Synchronization on HPOM for UNIX or Linux Systems" on page 32
- "How to Migrate from Scheduled Synchronization on HPOM for UNIX or Linux Systems" on page 33

How to Configure Dynamic Topology Synchronization on HPOM for Windows Systems

This section describes how to configure dynamic topology synchronization on HPOM for Windows management servers. For further details, see the HPOM for Windows documentation.

To forward topology data to Operations Management, complete the following steps on the Operations Manager for Windows management server from which you want to receive topology information:

1. *Prerequisite:* Make sure that the minimum patch level for the HPOM for Windows management server is installed:
   - Version 8.16: Patch OMW_00121 or superseding patch.
   - Version 9.00: Patch OMW_00122 or superseding patch.
2. *Prerequisite:* Configure trusted certificates for multiple servers.

In an environment with multiple servers, you must configure each server to trust certificates that the other servers issued.

3. In the console tree, right-click **Operations Manager**, and then click **Configure > Server...**. The Server Configuration dialog box opens.
4. Click **Namespaces**, and then click **Discovery Server**. A list of values appears.
5. Add the hostname of the server to **List of target servers to forward discovery data**. If there is more than one target server, separate the hostnames with semicolons, for example:

   ```
   server1.example.com;server2.example.com
   ```

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

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

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

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

How to Migrate from Scheduled Synchronization on HPOM for Windows Systems

This section describes how to migrate from scheduled synchronization on HPOM for Windows management servers. For further details, see the HPOM for Windows documentation.

To migrate from scheduled synchronization, complete the following steps on the Operations Manager for Windows management server from which you want to receive topology information:

1. *Prerequisite:* Make sure that the minimum patch level for the HPOM for Windows management server is installed:
   - Version 8.16: Patch OMW_00121 or superseding patch.
   - Version 9.00: Patch OMW_00122 or superseding patch.
2. Clear the agent repository cache on the HPOM management server using the following command:

   ```
   %OvBinDir%\ovagtrep -clearall
   ```

3. Remove the service auto-discovery policies from the HPOM management server node, type:

   ```
   %OvBinDir%\ovpolicy -remove DiscoverOM
   ```

   ```
   %OvBinDir%\ovpolicy -remove DiscoverOMTypes
   ```

4. Synchronize the policy inventory on the HPOM management server:

   a. In the console tree, right-click the management server.

   b. Select **All Tasks > Synchronize inventory > Policies**.

   The management server creates a deployment job to retrieve the inventory from the local agent.

5. Make sure the listener process is running:

   a. In the console tree, right-click **Operations Manager**, and select **Configure Server.**

   The Server Configuration dialog box opens.

   b. Click **Namespaces**, and select **Discovery Server**.

   A list of values appears.

   c. Set the value of **Enable discovery WMI listener** to true. This is the default value.

   d. Click **OK** to save your changes and close the Server Configuration dialog box.

   e. Restart the OvAutoDiscovery Server process for your changes to take effect using the following commands:

   ```
   net stop "OvAutoDiscovery Server"
   ```

   ```
   net start "OvAutoDiscovery Server"
   ```

6. Start the initial synchronization of topology data:

   a. In the console tree, select **Tools > HP Operations Manager Tools**.

   b. Right-click **Synchronize Topology** and select **All Tasks > Launch Tool...**.

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

How to Configure Dynamic Topology Synchronization on HPOM for UNIX or Linux Systems

This section describes how to configure dynamic topology synchronization on HPOM for UNIX or Linux management servers. For further details, see the HPOM for UNIX or Linux documentation.

To forward topology data to Operations Management, complete the following steps on the Operations Manager for UNIX or Linux management server from which you want to receive topology information:

1. *Prerequisite:* Make sure that the minimum patch level for the HPOM 9.10 for UNIX or Linux management server is installed:

   - HP-UX: Patch PHSS_42736 or superseding patch.
   - Linux: Patch OML_00050 or superseding patch.
   - Solaris: Patch ITOSOL_00772 or superseding patch.

2. *Prerequisite:* Make sure that the HP Operations Agent version on the HPOM for UNIX or Linux management server is 8.60.500 or higher. (Older agents require the agent hotfix

QCCR1A100254 and agtrep must be configured to send complete instance data.)

3. *Prerequisite:* Configure trusted certificates for multiple servers.

   In an environment with multiple servers, you must configure each server to trust certificates that the other servers issued.

4. *Prerequisite:* Set up the forwarding target (BSM Gateway Server, Reverse Proxy, or Load Balancer) in the node bank as a managed node. For details, see "How to Set Up a Forwarding Target in the HPOM for UNIX Node Bank" on page 23.

5. Type the following command to enable topology synchronization:

   ```
   /opt/OV/contrib/OpC/enableToposync.sh -online -target <comma_
   separated_server_list>
   ```

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

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

6. Type the following command to start the initial synchronization of topology data:

   ```
   /opt/OV/bin/OpC/startInitialSync.sh
   ```

How to Migrate from Scheduled Synchronization on HPOM for UNIX or Linux Systems

This section describes how to migrate from scheduled synchronization on HPOM for UNIX or Linux management servers. For further details, see the HPOM for UNIX or Linux documentation.

To migrate from scheduled synchronization, complete the following steps on the Operations Manager for UNIX or Linux management server from which you want to receive topology information:

1. *Prerequisite:* Make sure that the minimum patch level for the HPOM for Windows management server is installed:

   - HP-UX: Patch PHSS_42736 or superseding patch.
   - Linux: Patch OML_00050 or superseding patch.
   - Solaris: Patch ITOSOL_00772 or superseding patch.

2. Clear the agent repository cache on the management server using the following command:

   ```
   /opt/OV/bin/ovagtrep -clearall
   ```

3. Remove the service auto-discovery policies from the management server node using the following command:

   ```
   /opt/OV/bin/ovpolicy -remove DiscoverOM
   ```

   ```
   /opt/OV/bin/ovpolicy -remove DiscoverOMTypes
   ```

4. Deassign the service auto-discovery policies from the management server node using the following command:

```
/opt/OV/bin/OpC/utils/opcnode -deassign_pol node_name=<management_
server> net_type=NETWORK_IP pol_name=DiscoverOMTypes
pol_type=svcdisc
```

```
/opt/OV/bin/OpC/utils/opcnode -deassign_pol node_name=<management_
server> net_type=NETWORK_IP pol_name=DiscoverOM
pol_type=svcdisc
```

```
/opt/OV/bin/OpC/opcragt -dist <management_server>
```

Replace `<management_server>` with the name of the management server.

5. Type the following command to enable topology synchronization:

   ```
   /opt/OV/contrib/OpC/enableToposync.sh -online
   ```

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

6. Type the following command to start the initial synchronization of topology data:

   ```
   /opt/OV/bin/OpC/startInitialSync.sh
   ```

How to Manage a BSM Host System with HPOM for Windows *(Optional)*

> **Note:** The following agents are supported:
>
> - 11.12 and higher (HP recommends using the latest available agent version).
> - 11.11 (Not in conjunction with Monitoring Automation).
> - 11.10 (Not in conjunction with Monitoring Automation).
>
>   If the BSM system is on Windows contact HP Support and ask for Hotfix **QCCR1A147794**.
>
>   If you are installing HPOA 11.10 after installing BSM, install the **QCCR1A149034** hotfix before installing HPOA 11.10.

To install an HP Operations Agent on a system where BSM is installed, execute the following steps on all Data Processing Servers and all Gateway Servers:

1. Exchange certificate trusts between the HPOM and BSM host systems. For details, see "How to Establish a Trust Relationship for a Server Connection" on page 9.

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

   > **Note:** When configuring the HP Operations Agent using the **`oainstall -i -a`** command, use the HPOM management server as the value for the **`-srv`** option, and the BSM Data Processing Server as value for the **`-cert_srv`** option.

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

3. On the HPOM management server, use the Configure Managed Nodes dialog box to add the BSM server system as a managed node. In the node's properties, manually add the core ID and set the certificate state to `Installed`.

   > **Note:** The core ID can be obtained from the local BSM server with the command: **`ovcoreid`**. The output of the command is the core ID.

4. On the HPOM management server, check that you can manage the BSM server system with the command:

   opcragt -status <BSM_Server>

   The output should indicate that the agent is running.

5. Synchronize packages on the BSM node.

In the HPOM console, right-click the BSM node that you want to synchronize and select the following menu items:

All Tasks > Synchronize inventory > Packages

For more information about HPOM for Windows, see the HPOM for Windows online help.

How to Manage a BSM Host System with HPOM for UNIX or Linux *(Optional)*

> **Note:** The following agents are supported:
>
> - 11.12 and higher (HP recommends using the latest available agent version).
> - 11.11 (Not in conjunction with Monitoring Automation).
> - 11.10 (Not in conjunction with Monitoring Automation).
>
>   If the BSM system is on Windows contact HP Support and ask for Hotfix **QCCR1A147794**.
>
>   If you are installing HPOA 11.10 after installing BSM, install the **QCCR1A149034** hotfix before installing HPOA 11.10.

To install an HP Operations Agent on a system where BSM is installed, execute the following steps on all Data Processing Servers and all Gateway Servers:

1. Exchange certificate trusts between the HPOM and BSM host systems. For details, see "How to Establish a Trust Relationship for a Server Connection" on page 9.
2. Install a supported HP Operations Agent on the BSM host system. For details, see the HPOM and HP Operations Agent documentation.

   > **Note:** When configuring the HP Operations Agent using the `oainstall -i -a` command, use the HPOM management server as the value for the `-srv` option, and the BSM Data Processing Server as value for the `-cert_srv` option.

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

3. On the HPOM management server, specify the core ID of the BSM server:

   /opt/OV/bin/OpC/utils/opcnode -chg_id node_name=<BSM Server> id=<core ID of BSM Server>

   > **Note:** The core ID can be obtained from the local BSM server with the command: `ovcoreid`. The output of the command is the core ID.

4. On the HPOM management server, add the BSM server as a managed node in HPOM:

   /opt/OV/bin/OpC/utils/opcnode -add_node <BSM Server>

5. On the BSM Server, specify the core ID of the HPOM host system:

   ovconfchg -ns sec.core.auth -set MANAGER_ID <core ID of HPOM Server>

6. Validate the agent installation with the command:

opcragt -status <BSM Server hostname>

The output should indicate that the agent is running.

7. Add the forwarding target into an existing node group.

For further details, see HP Operations Manager documentation and the HP Operations Agent documentation.

How to Install BSM on a System Managed by HPOM

> **Note:** The following agents are supported:
>
> - 11.12 and higher (HP recommends using the latest available agent version).
> - 11.11 (Not in conjunction with Monitoring Automation).
> - 11.10 (Not in conjunction with Monitoring Automation).
>
>   If the BSM system is on Windows contact HP Support and ask for Hotfix **QCCR1A147794**.
>
>   If you are installing HPOA 11.10 after installing BSM, install the **QCCR1A149034** hotfix before installing HPOA 11.10.

1. Before installing BSM, on all Data Processing Servers and all Gateway Servers, run the following command:

   ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <*FQDN of primary DPS*>

2. Install BSM 9.20.

3. Install BSM 9.23.

4. ***Linux installations only:*** Move the contents of the following folder, including all sub-folders and their contents:

   `/tmp/OV_backup_<yyyymmdd>_<hhmm>/client_ks`

   to:

   `/var/opt/OV/datafiles/sec/ks`

5. Configure BSM according to the BSM Installation Guide.

6. Integrate HPOM as described from the beginning of this guide, with the configuration of the environment.

   If no event synchronization between HPOM and BSM/OMi is required, configure in accordance with the *Certificate Handling for OMi in Service Provider Environments* white paper.

Limitations: Uninstalling BSM or HP Operations Agent

When uninstalling BSM on a system managed by HPOM:

Uninstall BSM using the instructions found in the BSM Installation Guide. Note the following:

- If the BSM System was installed on Windows. and HP Operations Agent 11.04 is also uninstalled, a package called **HPSharedComp** will remain on the system. This can be removed by calling **MsiExec.exe /I{64386EA2-1E28-40EB-96BC-9FA83CF72AFE}** in a command shell.