HP Business Service Management

For the Windows, Linux operating systems

Software Version: 9.22

BSM - Service Manager Integration Guide

Document Release Date: April 2013

Software Release Date: April 2013

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® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

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

UNIX® is a registered trademark of The Open Group.

Acknowledgements

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

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

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

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

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

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

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

This document was last updated: Thursday, April 11, 2013

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

BSM - Service Manager Integration Overview

You can integrate HP Service Manager with one or more of the BSM components, as described below. Each integration can be performed separately.

Note: In general, the following document is for integrating BSM 9.2x with Service Manager 9.31.

For instructions on integrating BSM with earlier versions of Service Manager, see http://support.openview.hp.com/selfsolve/document/KM1303768/binary/BSM9.12_SM_Integration_Interactive_Docs.html. Download and extract the zip file contents; open the file **sm_interactive_document.htm** and follow the guidelines.

The options are as follows:

- **Downtime exchange between BSM and Service Manager.** BSM enables you to forward downtimes (also known as outages) from BSM to Service Manager, and from Service Manager to BSM. The downtime defined in BSM is converted to a request for change in Service Manager, and vice versa. For details, see "Downtime Exchange Between BSM and HP Service Manager" on page 10.
- **Incident exchange between Service Manager and Operations Manager i.** BSM enables you to forward events from Operations Management to Service Manager. Forwarded events and subsequent event changes are synchronized back from Service Manager to Operations Management. You can also drill down from Operations Manager events to Service Manager incidents. For details, see "Incident Exchange between HP Service Manager and HP Operations Manager i" on page 15.
- **View planned changes and incident details in Service Health.** This integration enables you to view planned changes and incident details in the Changes & Incidents tab in the 360° View page in Service Health. For details, see "View Changes and Incidents in Service Health Using Standalone HP Universal CMDB" on page 27 and "View Changes and Incidents in Service Health Using RTSM" on page 40.
- **Submit an incident through BSM alerts.** Incidents are automatically opened incidents in Service Manager when a CI Status alert is triggered in BSM. For details, see "Generate Incidents in Service Manager When a BSM Alert is Triggered" on page 51.
- **View the Number of Open Incidents in Service Health and create SLAs (EMS).** This integration enables you to view the Number of Open Incidents in Service Health views and reports and to manage, in Service Level Management, SLAs over Serviceability KPIs based on Service Manager incidents (EMS option). For details, see "View Incident Data in BSM, and Manage SLAs Based on Service Manager" on page 53.
- The **Business Impact Report** integration is described in the *Closed Loop Incident Process (CLIP)* Guide. When deployed as part of the BSM solution, Incident Management users can launch an impact report from an incident in context with the incident's affected CI. Service Desk Agents can validate the updated status of the Business Impact to categorize and prioritize the incident accordingly. For details, refer to the CLIP page in the Solutions Portal: http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab1.

Note:

- **Service Manager Query Security.** If you have set up an integration from BSM to Service Manager, there is a CI context menu that enables you to access Service Manager from BSM Service Health. This drill-down option is not available if you have enabled Service Manager query security.
- **Troubleshooting Multiple Domains.** If BSM and SM are in different domains, and you are using Internet Explorer as your browser, you may need to add the domains to the list of allowed domains in the Privacy tab (**Internet Options > Privacy > Sites**).

Chapter 1

Downtime Exchange Between BSM and HP Service Manager

BSM enables you to forward downtimes (also known as outages) from BSM to Service Manager, and from Service Manager to BSM. The downtime defined in BSM is converted to an incident in Service Manager, and vice versa.

This section includes the following:

Integration Overview

The downtime integration between BSM and Service Manager includes information exchanges in both of the following directions:

- **Service Manager > BSM.** When you create a downtime RfC (request for change) in Service Manager, the RfC includes the CI that is under change and a start and end date/time of the downtime. If you do not want to waste effort with false alarms in your operations center, and do not want to have these times included in service availability reports, you can set up the integration so that these RfCs are translated to downtimes in BSM.

  In this scenario, you install and set up a downtime adapter on your CMDB (whether you are working with a uCMDB central CMS, or with RTSM). The RfC creates a planned downtime CI in the CMDB, and the adapter sends the planned downtime CI to BSM to create a downtime.

- **BSM > Service Manager.** When you define downtimes using BSM (for example, every Monday and Saturday from 8:30 PM-9:30 PM), in order to proactively support end users the help desk should be aware of such operational downtimes. After you set up the integration, downtimes in BSM trigger events, which create corresponding incidents in Service Manager.

  In this scenario, when a downtime starts, BSM generates an event. Using the event forwarding mechanism, the event generates an incident in Service Manager. When the downtime ends, an event is sent to close the downtime incident.

A single downtime can be defined on more than one CI. In the case of BSM > Service Manager, a separate event is sent for each CI in the downtime.

Prerequisites

Supported Platforms

To set up the downtime integration, you must meet the following prerequisites:

- Service Manager 9.31 and higher.
- uCMDB (RTSM/CMS) 9.05 CUP 5 and higher with content pack 11 update 2, or uCMDB 10.01 with content pack 12.
- Before deploying the adapter verify that CP11 is installed. If it is not, install the content pack. (This should be done whether you have upgraded to BSM 9.22, or if you installed BSM 9.22 directly.)
- If the adapter is installed on the RTSM, and the adapter is working behind a reverse proxy, the DPS must have the correct certificates installed to send requests to the reverse proxy.

Installing the Content Pack for CMS 9.05 or RTSM 9.05

The following section is only relevant if you are using CMS 9.05, or upgrading from BSM 9.20 (which requires the CP to be installed). If you have not yet installed the content pack, perform the following on your BSM/CMS machine:

1. From the CP installation zip file, copy the content pack zip file to the following location (depending on your environment):

   For RTSM: <BSM data processing installation folder>\odb\content\content_packs

   For CMS: <Installation drive or folder>\HP\UCMDB\content\content_packs

   The main BSM folder in Linux is located in: /opt/HP/BSM.
2. Access the following location with your browser: http://<BSM DPS or CMS hostname>:21212 /jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=Content Pack Services.
3. In the method **installContentPack()**, enter the parameters:
   a. Fill the parameter **customerID** with the value of **1.**
   b. Enter the version number found in **version.dat**, located in the content pack zip file.
   c. Invoke the method.

Global ID Generator

To enable the downtime integration, you must have a global ID generator configured in your environment.

If you are working with RTSM, perform the following to configure the global ID generator:

1. Access the following location with your browser: http://<BSM hostname>:21212/jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=Multiple CMDB Instances Services
2. In the method **setAsGlobalIdGenerator()**, fill the parameter **customerID** with the value of **1**, and click **Invoke**.

Step 1: Send BSM Downtime Events to Service Manager

To enable BSM to send downtime definitions to Service Manager, you must edit an infrastructure setting as described below. This procedure generates events in OMi; you can then use the event forwarding mechanism to generate incidents in Service Manager when a downtime in BSM begins and ends.

1. Access the following location in BSM: **Infrastructure Settings > Foundations > Downtime**.
2. Change the value of the parameter **Downtime Send Event** to **true**.

A corresponding forwarding rule that configures forwarding downtime start and end events from BSM to Service Manager should be configured in the Event Forwarding Rule dialog box. The forwarding rule should be based on the ETI Hint, as follows:

- ETI Hint equals ignore case “downtime: start”
- ETI Hint equals ignore case “downtime: end”

For details on how to use the event forwarding mechanism to generate incidents in Service Manager, refer to the section "Event Forwarding" in the *BSM Application Administration Guide*.

Downtime events use the following formats:

- **Downtime Start**

Event field	BSM Downtime
Severity	Normal
Category	Downtime Notification
Title	Downtime for <CI Type><Affected CI Name>started at <Downtime Start Time>
Key	<BSM Downtime ID>:<Affected CI ID>:downtime-start
SubmitCloseKey	False
OutageStartTime	<Downtime Start Time>
OutageEndTime	<Downtime End Time>
CiName	<Affected CI Name>
CiId	<Affected CI Global ID>
CiHint	GUCMDB:<Affected CI Global ID>|UCMDB:<Affected CI ID>
HostHint	GUCMDB:<Related Host Global ID>|UCMDB:<Related Host ID>
EtiHint	downtime:start

- **Downtime End**

Event field	BSM Downtime
Severity	Normal
Category	Downtime Notification
Title	Downtime for <CI Type><Affected CI Name> ended at < Downtime End Time>
Key	<BSM Downtime ID>:<Affected CI ID>:downtime-stop
SubmitCloseKey	true
CloseKeyPattern	<BSM Downtime ID>:<Affected CI ID>:downtime-start
EtiHint	downtime:end
LogOnly	true

Step 2: Integrate Service Manager Downtimes With BSM

To enable downtimes defined in Service Manager to be sent to BSM, you must add an integration adapter to the uCMDB where downtimes are defined.

Important:

- Following the initial integration, a large amount of data may be communicated from Service Manager to BSM. **We recommend that you perform this procedure during off-hours, to prevent negative impact on system performance.**
- The integration consists of two parts: Service Manager > CMS/RTSM, and CMS/RTSM > BSM adapter. You should configure both parts of the integration as one flow, without a significant time lag between setting up the two parts. If you set up the Service Manager > CMS/RTSM part, and then wait a long time before setting up the CMS/RTSM > BSM adapter part, the number of downtimes communicated to BSM initially may be extremely high.

Note:

- The following procedure does not describe the Service Manager > CMS/RTSM connection setup. Service Manager should be configured to create its CIs in the CMS; this procedure connects the adapter between the CMS/RTSM and BSM.
- The default job synch frequency is one minute.

Create a new integration point as follows:

1. If you are using CMS, or if you have upgraded to BSM 9.22, deploy the adapter using the steps below. (If you are not using a standalone CMS, and you have a fresh BSM 9.22 installation,

skip to "Create the integration point credentials:" below)

a. Within BSM/CMS, access **Administration > Package Management**. (In BSM, this is located within **Admin > RTSM Administration**.)

b. Click **Deploy package to server**, and import the adapter's zip file from <BSM DPS installation path>\odb\conf\factory_packages\BSMDowntimeAdapter.zip.

2. Create the integration point credentials:

a. Within BSM/CMS, access **Data Flow Management > Data Flow Probe Setup**. (In BSM, this is located within **Admin > RTSM Administration**.)

Note: You do not need a Probe to perform this integration; nevertheless you create credentials using the Data Flow Probe Setup tab.

b. Click **Add domain or probe**, and enter a name and description of your choice.

c. Expand the submenus and select **HTTP protocol**.

d. Click the **+** sign (**Add new connection details**) and enter the BSM Gateway host name, Port 80, and the BSM username and password. Leave the **Trust** fields blank. When you are done, click **OK** to save the credentials.

3. Create a new integration point:

a. Within BSM/CMS, access **Data Flow Management > Integration Studio.** (In BSM, this is located within **Admin > RTSM Administration**.)

b. Click **New integration point**, enter a name and description of your choice, and select **BSMDowntimeAdapter/SM scheduled Downtime Integration into BSM**.

c. Enter the following information for the adapter: BSM Gateway hostname and port, the integration point credentials you just created, communication protocol, and the context root (if you have a non-default context root).

d. Click **OK**, then click the **Save** button above the list of the integration points.

4. You can use the **Statistics** tab in the lower pane to track the number of downtimes that are created or updated. By default, the integration job runs every minute. If a job has failed, you can open the **Query Status** tab and double-click the failed job to see more details on the error.

If there is an authentication error, verify the BSM credentials entered for the integration point.

If you receive an unclear error message with error code, this generally indicates a communication problem. Check the communication with BSM. If no communication problem is found, restart the **MercuryAS** process.

A failed job will be repeated until the problem is fixed.

Chapter 2

Incident Exchange between HP Service Manager and HP Operations Manager i

BSM enables you to forward events from Operations Management to HP Service Manager 9.30, 9.21, or 9.20. Forwarded events and subsequent event changes are synchronized back from HP Service Manager to Operations Management. You can also drill down from Operations Manager events to HP Service Manager incidents.

Note: HP recommends this integration option for new integrations with HP Service Manager 9.30, 9.21, or 9.20. However, existing integrations that use other integration options are still supported.

This section includes the following:

Step 1: Configure the HP Service Manager Server as a Connected Server

Synchronizing events and event changes between Operations Management events and HP Service Manager incidents requires configuring a Connected Server within OMi to correctly identify the target HP Service Manager instance. The first step to achieve this is to configure HP Service Manager as a target connected server in the Connected Servers manager.

For full details about how to configure a connected server, see the Connecting Servers section of the Operations Management online help.

To configure the HP Service Manager server as a target connected server, perform the following steps:

1. Navigate to the Connected Servers manager in the Operations Management user interface:

   Admin > Operations Management > Setup > Connected Servers

2. Click the New ( ) button to open the Create New Server Connection dialog box.

3. In the **Display Name** field, enter a name for the target HP Service Manager server. By default, the Name field is filled automatically. For example, if you enter `Service Manager 1` as the Display Name for the target HP Service Manager server, `Service_Manager_1` is automatically inserted in the Name field. Of course, you can specify your own name in the Name field, if you want to change it from the one suggested automatically.

   Note: Make a note of the name of the new target server (in this example, `Service_Manager_1`). You need to provide it later on as the `username` when configuring the Service Manager server to communicate with the server hosting Operations Management.

   Optional: Enter a description for the new target server.

   Make sure that you check the **Active** checkbox.

   Click **Next**.

4. Select `External Event Processing` to choose the server type suitable for an external incident manager like HP Service Manager.

   Click **Next**.

5. Enter the Fully Qualified DNS Name of the HP Service Manager target server.

   Click **Next**.

6. Next, you need to establish the type of integration. In the Integration Type dialog box, you can choose between using a Groovy script adapter, or the Event Synchronization Web Service.

   a. As an HP Service Manager Groovy script adapter is provided for integrating with HP Service Manager, select **Call Script Adapter**.

   b. In the Script Name field, select **sm:ServiceManagerAdapter**.

   c. Click **Next**.

7. In HP Service Manager, set up an Integration User with user name and password. This is the user name and password needed to access the HP Service Manager target server.

8. In the Operations Management user interface, the next step is to provide the credentials (user name, password, and port number) to connect to the HP Service Manager target server and to forward events to that server. In the Outgoing Connection dialog box, enter the following values:

   a. In the **User Name** field, enter the user name for the Integration User you set up in HP Service Manager.

   b. In the **Password** field, enter the password for the user you just specified. Repeat the password entry in the **Password (Repeat)** field.

   c. In the **Port** field, specify the port configured on the HP Service Manager side for the integration with Operations Management. To find the port number to enter:

- If you are using default ports on Service Manager, select/deselect **Use Secure HTTP**, then click **Set default port**. The port will be automatically set.
- If you need to find the port number, access the following file on your HP Service Manager Server: `<HP Service Manager root directory>/HP/Service Manager <version>/Server/RUN/sm.ini`. In the `sm.ini` file, you will find two port entries, depending on whether you want to use a secure HTTP connection: the `httpPort`, with default port number `13080`, and `httpsPort`, with default port number `13443`. The actual values for the ports can differ from these default values depending on how they are configured. Enter the appropriate value in the Port field.

d. If you do not want to use secure HTTP, make sure that the Use secure HTTP checkbox is *not* checked.

   If Use Secure HTTP is selected, download and install a copy of the target server's SSL certificate by clicking the link "Retrieve from Server", or "Import from File" if the certificate is available in a local file.

e. Make sure that the **Enable Synchronize and Transfer Control** checkbox is checked. When the Enable Synchronize and Transfer Control flag is set, an Operations Management operator is then able to transfer ownership of the event to the target connected server. If the flag is not set, then the option Synchronize and Transfer Control does not appear in the list of forwarding types when configuring forwarding rules.

   Also, note that if the Enable Synchronize and Transfer Control flag is not set for any target connected server, the Transfer Control to option does not appear at all in the Event Browser context menu.

   If a specific server is configured without the Enable Synchronize and Transfer Control flag set, then that server is not available in the Event Browser context menu as a server to which you can transfer ownership.

f. Test the connection. A **Success** or **ERROR** hyperlink will appear; click the link to get a more detailed message.

g. Click **Next**.

9. If, in addition to automatically generating HP Service Manager incidents from OMi events, you want to also be able to drill-down into HP Service Manager, you need to specify the fully qualified DNS name and port of the HP Service Manager system where you want to perform incident drill-down.

   Note: To enable incident drill-down to HP Service Manager, you must install a web tier client for your HP Service Manager server according to your HP Service Manager server install/configuration instructions.

   In the Event Drilldown dialog box of the Connected Servers manager, configure the server where you installed the web tier client along with the configured port used.

   If you do not specify a server in the Event Drilldown dialog box of the Connected Servers manager, it is assumed that the web tier client is installed on the server used for forwarding events and event changes to HP Service Manager, and receiving event changes back from HP Service Manager.

> If nothing is configured in the Event Drilldown dialog box, and the web tier client is not installed on the HP Service Manager server machine, the web browser will not be able to find the requested URL.

Click **Next**.

10. The next thing to do is to enable event changes to be synchronized back from HP Service Manager to Operations Management. For this you need to provide credentials for the HP Service Manager server to access the server hosting Operations Management.

    a. In the Incoming Connection dialog box, select the **Accept event changes from external processing server** checkbox, and then enter a password that the HP Service Manager server requires to connect to the server hosting Operations Management.

    > **Note:** Make a note of this password. You need to provide it later on when configuring the HP Service Manager server to communicate with the server hosting Operations Management. This password goes with the server name (`Service_Manager_1`) you configured in step 3.

    (If **Supports Synchronize & Transfer Control** was previously selected, the **Accept event changes from external processing server** option is assumed, and cannot be disabled.)

    b. Click **Finish**. The target HP Service Manager server appears in the list of Connected Servers.

Step 2: Configure an Event Forwarding Rule

The next step is to configure an event forwarding rule that determines which events are forwarded automatically to HP Service Manager.

Refer to the Operations Management online help for full details about configuring filters.

To configure a forwarding rule, carry out the following steps:

1. Navigate to the Forwarding Rules manager in the Operations Management user interface:

   Admin > Operations Management > Event Automation > Event Forwarding

2. Click the **New** button to open the Create New Forwarding Rule dialog box.
3. In the **Display Name** field, enter a name for the forwarding rule, in this example `Forward Critical (Sync and Transfer Control).`

   Optional. Enter a description for the forwarding rule you are creating.

   Make sure the **Activate Rule after creation** checkbox is checked. A rule must be active in order for its status to be available in HP Service Manager.

4. Click the browse button next to the Event Filter field. The Select an Event Filter dialog box opens.

   In the Select an Event Filter dialog box, do one of the following:

- Select an existing filter
- Create a new filter as follows:

  i. Click the **New** button to open the Filter Configuration dialog box.

  ii. In the **Filter Display Name** field, enter a name for the new filter, in this example, **FilterCritical**.

  Uncheck the checkboxes for all severity levels except for the severity Critical.

  Click **OK**.

  iii. You should see your new filter in the Select an Event Filter dialog box (select it, if it is not already highlighted).

  Click **OK**.

5. Under **Target Servers**, select the target connected server you configured in the section "Step 1: Configure the HP Service Manager Server as a Connected Server" on page 15. In this example, this is `Service Manager 1`.

   Click the **Add** button next to the target servers selection field. You can now see the connected server's details. In the **Forwarding Type** field, select the forwarding type.

   Click **OK**.

Step 3: Configure URL Launch of Event Browser from HP Service Manager

Before operators are able to perform event drill-down from HP Service Manager into the Operations Management user interface using a URL launch of the Event Browser, the operators must be set up as valid users in BSM with appropriate permissions in Operations Manager i:

User account requirements

- If Single Sign-On (SSO) authentication is configured, set up each user in BSM with the *same* user name that is used by the HP Service Manager operator to log onto HP Service Manager and to perform the URL call. (The password of each BSM user can be any string, but not empty.) After successfully logging into HP Service Manager, the BSM users can launch the Operations Management Event Browser without further authentication.

  For details on setting up SSO, see *Configuring HP Service Manager to Use the SSL-based Trusted Sign-On and LW-SSO* in the Service Manager documentation library.

- If HP Service Manager is not configured to use SSO authentication, set up each user with the *same* user name that is used by the HP Service Manager operator and specify a valid password. The users are required to enter their user name and password when launching the Operations Management Event Browser.

Required user permissions

You must grant the permission `Events assigned to user` including the required actions to each BSM user. You can optionally grant the permission to view events not assigned to each user.

Note: Without valid user names, or if a user does not have the required viewing permissions, any attempt to perform a URL launch of the Operations Management Event Browser from HP Service Manager results in an empty browser window.

Step 4: Configure URL Launch of HP Service Manager from the Event Browser

To be able to perform a URL launch of HP Service Manager from the Operations Management Event Browser using the web tier client, perform the following:

1. Navigate to the **Connected Server Admin** screen, and click the **Manage Scripts** icon on the right.
2. Select the **sm:ServiceManagerAdapter** script, and click the Edit button.
3. Locate the following text in the Groovy script:

   ```
   private static final String SM_WEB_TIER_NAME = 'webtier-9.30'
   ```

4. Change the value of `webtier-9.30` to the value required to access the HP Service Manager web tier client.

   The full drill-down URL is made up like this:

   `http://<FQDNS of HP Service Manager web tier server>/<web path to HP Service Manager>/<URL query parameters>`

   where *<FQDNS of HP Service Manager web tier server>* is the fully qualified DNS name of the HP Service Manager server where the web tier client is installed. This part of the URL is added automatically (together with `http://`) according to the values that you provided when you configured the HP Service Manager as a target connected server in the Connected Servers manager (refer to "Configure the HP Service Manager Server as a Connected Server").

   Here is an example of how the drill-down URL looks:

   ```
   http://smserver.example.com/SM930/index.do?ctx=docEngine&file=probsummary&query=number%3D
   ```

   So in this example, the you must replace `webtier-9.30` with `SM930`. All the other parts of the URL are configured automatically.

5. When finished editing, save the new version of the script. (Note that the script can always be reverted to its original version.)
6. In the HP Service Manager web tier configuration file `web.xml`, set the value of the `querySecurity` parameter from the default value (`true`) to **`false`**.

   For more details, see the section Web parameter: querySecurity in the HP Service Manager online help.

Step 5: Configure HP Service Manager Server

The next step is to configure HP Service Manager server to integrate with Operations Management.

To configure the HP Service Manager server, complete the following steps in the HP Service Manager:

1. From the left hand pane of the HP Service Manager user interface, navigate to:

   Tailoring > Integration Manager

2. Click **Add** to add a new configuration.
3. Select the **SMOMi** integration template from the Integration Template field. Click **Next**.
4. *Optional*. Change the log level to the desired value.

   Optional. Change the description, for example, to `This is for SMOMi integration`.

   Click **Next**.
5. In the General Parameters tab, replace the existing entries with the following values:

Name	Value	Category
`omi.server.url`	`http://<BSM_gateway_FQDN>/opr-gateway/rest/9.10/synchronization/event/`	General
`username`	`Service_Manager_1` (This is the name of the HP Service Manager target server you configured previously in the section "Step 1: Configure the HP Service Manager Server as a Connected Server" on page 15).	Header
`omi.eventdetail.baseurl`	`http://<BSM_gateway_FQDN>/opr-console/opr-evt-details.jsp?eventId=`	General

6. In the Secure Parameters tab, set the password to the one you specified in the Incoming Connection dialog box when configuring the target connected server in the section "Step 1: Configure the HP Service Manager Server as a Connected Server" on page 15. In our example, this is `HPqwer1_`.

   Click **Next**.
7. In the Integration Instance Fields dialog box, click **Next**.
8. In the Integration Instance Mapping dialog box, click **Finish**.

Note: Ensure that the rule is active. To make the rule active, select the rule and click **Enable**.

Step 6: Mapping and Customization

You can add your own custom attributes in a Groovy script and then map these custom attributes to HP Service Manager to the appropriate field in HP Service Manager. You can also change how attributes are mapped from Operations Management to HP Service Manager. The mapping is done in the BDM Mapping Manager in HP Service Manager:

System Administration > Ongoing Maintenance > BDM Mapping Management

For full details about mapping attributes, see the HP Service Manager online help.

Step 7: Test the Connection

To test the connection, send an event to the server hosting Operations Management that matches the filter you defined (in our example filter, the severity value is `Critical`), and then verify that the event is forwarded to HP Service Manager as expected.

To test the connection, do the following:

1. On the Gateway Server system running Operations Management, open an Event Browser.
2. On the system running Operations Management, open a command prompt and change to the following directory:

   `<HPBSM root directory>\opr\support`
3. Send an event using the following command:

   `sendevent -s critical -t test111-1`
4. Verify that the event appears in the Operations Management Event Browser.
5. Select the **Forwarding** tab.
6. In the External Id field, you should see a valid HP Service Manager incident ID.
7. Next, verify that the incident appears in the Incident Details in HP Service Manager:

   If the event drill-down connection is configured correctly, click the hyperlink created with the Incident ID. A browser window opens, which takes you directly to the incident in the Incident Details in HP Service Manager.

   If the event drill-down connection is not configured, do the following:

   a. In the Forwarding tab in the Operations Management Event Browser, copy or note the incident ID from the External Id field.

   b. In the HP Service Manager user interface, navigate to:

      Incident Management→Search Incidents

   c. Paste or enter the incident ID in the Incident Id field.

   d. Click the **Search** button. This takes you to the incident in the Incident Details.
8. Close the incident in HP Service Manager.
9. Verify that the change in the state of the incident (it is now `closed`) is synchronized back to

Operations Management. You should not be able to see the event that was closed in HP Service Manager in the active Event Browser, but it should now be in the History Browser.

Step 8: Synchronize Attributes

Not all attributes are synchronized back from Service Manager to Operations Management by default. When the Service Manager incident is initially created from an Operations Management event, all possible event attributes are mapped to the corresponding Service Manager incident attribute. Out of the box, after the initial incident creation, whenever the incident or event subsequently changes, only a subset of the changed event and incident attributes are synchronized. The following describes how to customize the list of attributes to synchronize upon change.

Uni-directional Synchronization: Operations Management to HP Service Manager

The following attributes are transferred to HP Service Manager from Operations Management one a one-time basis, that is, when the event was initially created, and the transfer of control of the event was configured in the Connected Servers manager.

These attributes support bi-directional synchronization, but are disabled out-of-the-box:

- Title
- Severity
- Priority
- Operator: the operator assigned to the event who forwarded the event
- Category
- Subcategory
- Related CI

For the above attributes, there is no back synchronization from HP Service Manager to Operations Management.

Bi-directional Synchronization

Attributes that support bi-directional synchronization between Operations Management and HP Service Manager are:

- Description
- Lifecycle state (the state is only updated when the state changes to closed)
- Solution
- Operations Management event annotations are synchronized to HP Service Manager activity log
- Contents under the Forwarding tab in the Event Details

Attribute Synchronization using Groovy Scripts

If you want to change the out-of-the-box behavior regarding which attributes are updated, you can specify this in a Groovy script. In the Groovy script, you would specify which fields are updated in

HP Service Manager, and which fields are updated in Operations Management. You can also specify custom attributes in the Groovy script.

In the Groovy script, you would specify which fields are updated in HP Service Manager, and which fields are updated in Operations Management. You can also specify custom attributes in the Groovy script.

Tips for Customizing Groovy Scripts

This section provides some tips about customizing Groovy scripts. Below we show just a few selected examples of what you can customize. You can look at the configuration section of a Groovy script to see further items that can be modified.

In the configuration section of a Groovy script, you can define and modify the attributes that are to be synchronized between Operations Management and HP Service Manager. The configuration section of a Groovy script also contains the default value mappings for lifecycle state, severity, and priority. You can also modify these, and it is possible to define the mappings for in-going and out-going requests differently.

More advanced configuration can be done in other parts of the Groovy script if required.

The beginning and the end of the configuration section of a Groovy script is marked as follows:

```
//
// configuration section to customize the Groovy script
// BEGIN
...
...
//
// configuration section to customize the Groovy script
// END
```

Note: As of BSM 9.20, modifications to Groovy scripts are not overwritten by patches and hotfixes; your customized version of a script will remain after an update/patch. If you want to use the newer version of a script, make a copy of your version, revert back to the predefined version, and then re-apply your changes.

The mapping from Operations Management to HP Service Manager is compliant to BDM 1.1 incident web service specifications. The mapping of the BDM 1.1 incident web service to HP Service Manager is specified in HP Service Manager in the BDM Mapping Manager. For more information about the BDM Mapping Manager, see the BDM Mapping Manager section of the HP Service Manager online help.

Controlling Attribute Synchronization

You can control how updates to certain attributes are synchronized between Operations Management and HP Service Manager by setting some Boolean variables to true or false.

Here are two examples:

- As of BSM 9.21 there is a new variable called `SyncAllProperties`. By default it is `false`; if you set it to `true`, all properties will be synchronized in both directions. The other variables will be ignored.

Here are two additional examples:

- `private static final SyncTitleToSMOnUpdate = false;`

  This line of the Groovy script disables the synchronization of changes to the title made in Operations Management to HP Service Manager.

- `private static final Boolean SyncTitleToOPROnUpdate = false;`

  This line of the Groovy script disables the synchronization changes to the title made in HP Service Manager to Operations Management.

The title is a required attribute in HP Service Manager, and is set, independently of the flags above, using the title given in Operations Management during the creation of the incident.

Mapping OPR Lifecycle States to BDM Lifecycle States

Individual OPR event state and Service Manager incident status changes may be selected for synchronization. Out of the box, only the "closed" state is synchronized in both directions. To change this behavior add the desired states to the appropriate list, SyncOPRStatesToSM or SyncSMStatusToOPR .

Here are two examples:

- `private static final Set SyncOPRStatesToSM = ["closed", "in_ progress", "resolved"]`
- `private static final Set SyncSMStatusToOPR = ["closed", "resolved"]`

In the example the OPR event lifecycle states closed, in_progress and resolved are synchronized to the Service Manager incident status, and Service Manager incident status closed and resolved are synchronized to the OPR event state.

Note: The special state "*" denotes all states, so to synchronize all OPR event states to the SM incident status property specify the following:

```
private static final Set SyncOPRStatesToSM = ["*"]
```

Additionally two maps are used to specify the mapping of OPR event lifecycle state to BDM incident status. The maps are named MapOPR2SMStatus and MapSM2OPRState. Out of the box, all possible states have a mapping.

Here is an example:

- `private static final Map MapOPR2SMStatus = ["open": "open", "in_ progress": "work-in-progress", "resolved": "resolved", "closed": "closed"]`
- `private static final Map MapSM2OPRState = ["accepted": "open", "assigned": "open", "open": "open", "reopened": "open",`

  `"pending-change": "in_progress", "pending-customer": "in_progress", "pending-other": "in_progress",`

```
"pending-vendor": "in_progress", "referred": "in_progress",
"suspended": "in_progress",

"work-in-progress": "in_progress", "rejected": "resolved",
"replaced-problem": "resolved",

"resolved": "resolved", "cancelled": "resolved", "closed": "closed"]
```

Syntax Errors

If you get a syntax error when customizing your Groovy scripts, you will get an event in the event browser with a detailed description of the error. In addition you may view the log file `opr-event-sync-adapter.log` for information about how to resolve the error. You can find the log file here:

`<`*`Gateway Server root directory`*`>/log/opr-event-sync-adapter.log`

Chapter 3

View Changes and Incidents in Service Health Using Standalone HP Universal CMDB

This integration enables you to view planned changes and incident details in the Changes & Incidents tab in the 360° View page in Service Health, when you are using a standalone HP Universal CMDB.

This task describes how to configure the HP Service Manager - BSM federated integration in order to allow both products to share information and data.

Note: Beginning with UCMDB version 9.05, a new SM adapter (ServiceManagerAdapter9-x) is supplied with UCMDB out of the box, in addition to the legacy adapter (ServiceManagerAdapter7-1).

- For SM versions 9.30 and 9.31, use ServiceManagerAdapter9.xx.
- For SM versions 9.20 and earlier, use ServiceManagerAdapter7-1.

This section includes the following:

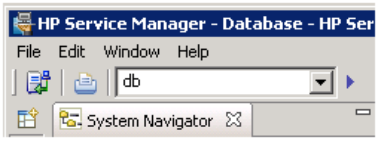
Prerequisites

- **Data-Flow Probes (for SM 9.3x).** If you are using SM 9.30 or 9.31, before you begin you must install *two* data-flow probes - one with UCMDB as its target, and another with the BSM Gateway Server as its target. When you configure the integration points, you will select these probes.
- **Trusted Sign-on and LW-SSO.** If you want HP Service Manager to use the SSL-based Trusted Sign-on protocol and LW-SSO, configure it according to the instructions in the HP Service Manager online help if you have not already done so. In addition, see *Configuring HP Service Manager to Use the SSL-based Trusted Sign-On and LW-SSO* in the Service Manager documentation library.

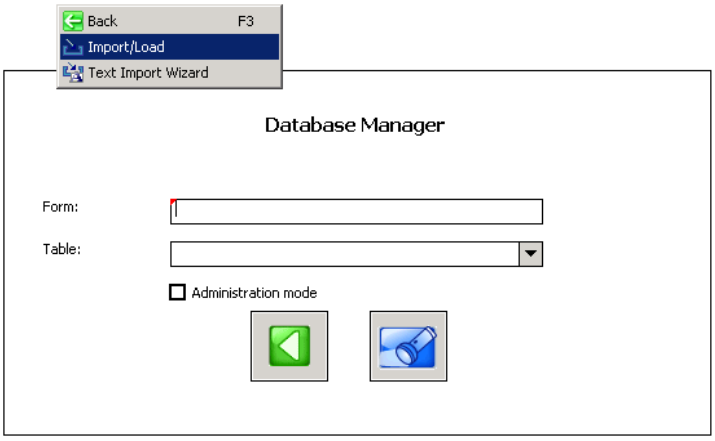
Step 1: Load .unl Files to Provide External Access to Service Manager

This procedure enables BSM to query incidents and changes:

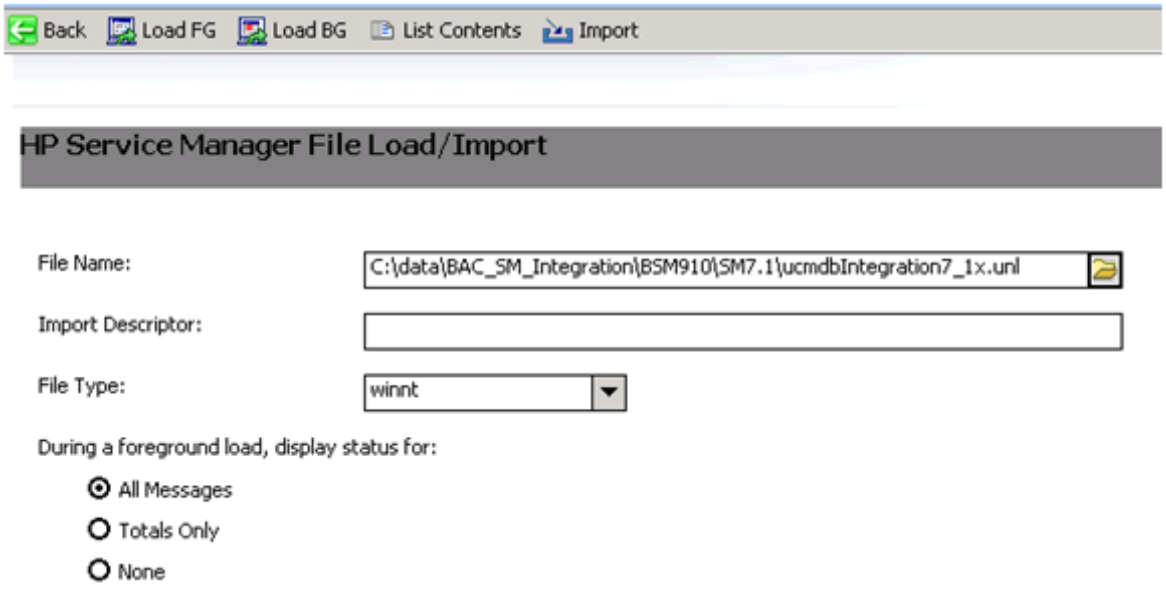
1. Copy the following files from the BSM 9.x DVD to a local directory:
   - SM_Integration/SM_Unloads/SM7.1/ucmdbIntegration7_1x.unl
   - SM_Integration/SM_Unloads/SM7.1/BACExtAccess_71_v1.unl
2. Before loading these .unl files, apply the fix described in http://support.openview.hp.com/selfsolve/document/KM1015767. This is required because the .unl file expects the name attribute in the EXTACCESSM1 table to be length 50 in the database, but its default out-of-the-box length is 100. You therefore need to reduce the size of the attribute, load the unl file, then increase the size again. These steps are for the SQL Server, but you can refer to the KM document for the equivalent Oracle syntax.
   a. Database field truncation may result in data loss if data in the field exceeds the default length, so first check the size of data in the field: `Select NAME, LEN(NAME) from EXTACCESSM1 order by 2 desc`
   b. Reduce the size of the field: `alter table EXTACCESSM1 alter column NAME VARCHAR(50)`
   c. Load the ucmdbIntegration7_1x.unl file as described in the following steps. When you are done, you will increase the size of the field back to what it was originally.
3. In Service Manager, type **db** in the command line text widget in the menu bar at the top of the client display.



4. Right-click the white background and select **Import/Load** from the context menu that appears.



5. Click the folder icon at the end of the File Name box. and navigate to the .unl file you copied from BSM. Select the file, and click **Open**.



6. Click **Load FG** on the toolbar to load the file. If you receive a message saying "The file you are loading will change the keys...", click **Yes**.
7. Increase the size of the field back to what it was originally: `alter table EXTACCESSM1 alter column NAME VARCHAR(100)`
8. Repeat the above steps for the BACExtAccess_71_v1.unl file.

Step 2: Configure the Service Desk Adapter Time Zone

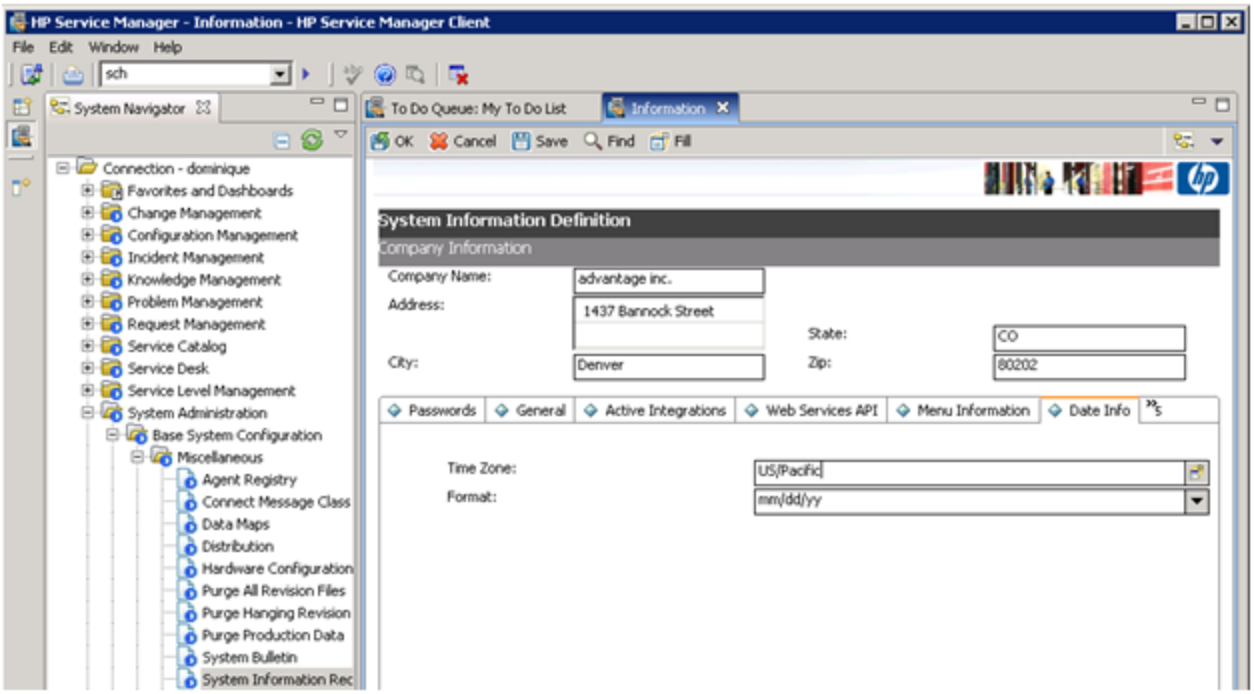
Configure the time zone so Incidents and Planned Changes have the correct time definitions:

1. In Service Manager, select **Navigation pane > Menu navigation > System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Within the **Date Info** tab, open the <BSM DPS root directory>/odb/runtime/fcmdb/CodeBase/<ServiceManagerAdapter9-x or ServiceDeskAdapter7-1>/serviceDeskConfiguration.xml file.
3. Find the row that includes the following string:

   <globalConnectorConfig><![CDATA[<global_configuration><date_pattern>MM/dd/yy HH:mm:ss</date_pattern><time_zone>US/Pacific</time_zone>

   and check the date and time format, and time zone. Note that the date is case-sensitive. Change either Service Manager or the xml file so that they both match each other's settings.

   Note: Specify a time zone from the Java time zone list that matches the time zone used in Service Manager; for example, America/New York.



4. Restart the corresponding server to make the change take effect. (If you changed the time zone on SM, restart the Service Manager server; if you changed the time zone on BSM, restart the BSM server.)

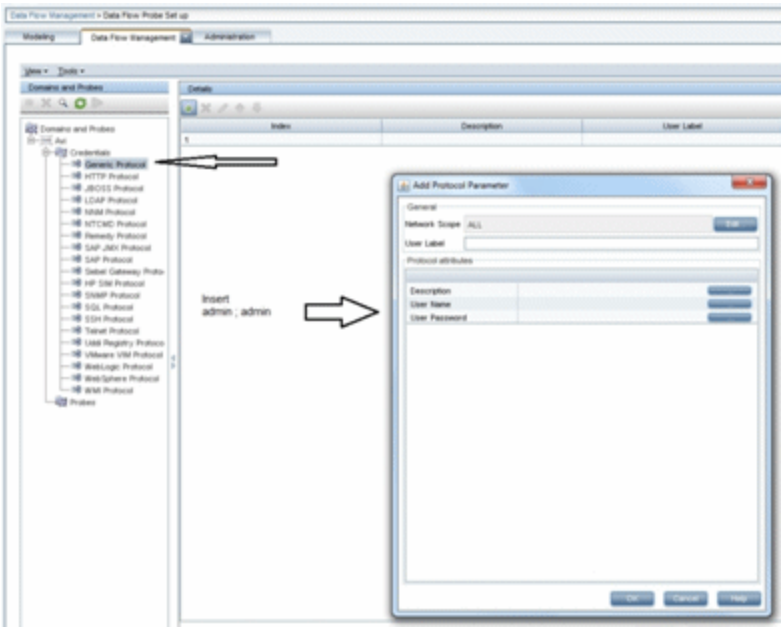
Step 3: Configure BSM to Generate Global IDs

1. Navigate to the BSM JMX console: http://<Data Processing server name>:21212/jmx-console
2. Enter the Username and Password.
3. In the UCMDB section, select **UCMDB:service=Multiple CMDB Instances Services**.
4. For **setAsGlobalIdGenerator**, click Invoke.
5. On the DPS, open the file <BSM Install folder>/odb/runtime/fcmdb/CodeBase/<ServiceManagerAdapter9-x or ServiceManagerAdapter7-1>/sm.properties, and set the **use.global.id parameter** to **true**.

For SM versions 9.20 and earlier, proceed with the next step. For SM versions 9.30 and 9.31, skip to "Step 5: Configure SM Adapter in UCMDB" on next page.

Step 4 (for SM 9.20 and earlier only): Add a Domain

1. In BSM, select **Admin > RTSM Administration**, click the **Data Flow Management** tab, and select **Data Flow Probe Setup**.
2. In the **Domains and Probes** pane, click  .
3. In the **Add New Domain** dialog box, enter a new domain name and click **OK**. This creates a new domain and its protocols.
4. Within the domain you added, select **Credentials > Generic Protocol**, and click the **Add new connection details** button in the right pane. In the **Add Protocol Parameter** dialog box that opens, insert the SM administrator credentials.



Step 5: Configure SM Adapter in UCMDB

1. Within the UCMDB user interface, access **Data Flow Management** > **Adapter Management**.
2. In the resources window, select **ServiceManagerAdapter9-x** or **ServiceManagerAdapter7-1** > **Configuration files**.
3. Select **ServiceManagerAdapter9-x/sm.properties** or **ServiceManagerAdapter7-1/sm.properties**.
4. In the window on the right side of the screen, modify the **use.global.id** parameter, set it to **false**, and click **OK**.

Step 6: Configure the SM-UCMDB Integration: Create an Integration Point

1. Within the UCMDB user interface, select **Data Flow Management > Integration Studio**.
2. In the Integration Point pane, select **Create New Integration Point**. The Create New Integration Point dialog box opens. Enter the following:

Name	Recommended Value	Description
Integration Name	**SM Integration**	The name you give to the integration point.
Adapter	**<user defined>**	Select the appropriate adapter for the version of SM that you are using.
Is Integration Activated	**selected**	Select this check box to create an active integration point.
Hostname/IP	**<user defined>**	The name of the SM server.
Port	**<user defined>**	The port through which you access SM.
Credentials	**<user defined>**	▪ For SM 9.20 and earlier, select the user credentials created in "Step 4 (for SM 9.20 and earlier only): Add a Domain" on previous page. ▪ For SM 9.30 and 9.31, in the default domain select Generic Protocol, and enter the credentials of the SM administrator.
Probe Name (for ServiceManagerAdapter9-x only)	**<user defined>**	If you are using ServiceManagerAdapter9-x, select the probe which reports to *CMS* (see "Prerequisites" on page 28).

Note: It is recommended to click the **Test Connection** button to verify that the details

entered are working before continuing.

3. In the **Integration Point** pane, click the Integration Point you just created, and click the **Federation** tab in the right pane.
4. In the **Supported and Selected CI Types** area, verify the **Incident**, **Problem**, and **Request for Change** CITs are selected.

Step 7: Configure the SM-UCMDB Integration: Set Up Data Push Jobs

Depending on your adapter version, perform the following:

For ServiceManagerAdapter9-x:

1. Edit the **SM Push** job, and select **Scheduler Definition**.
2. For the **Repeat** field, you can select **Changes Sync/All Data Sync**.
3. Set the **Repeat Every** field to **1 Day**, and click **OK**.

For ServiceManagerAdapter7-1:

1. Edit the **SM Topology Comparison Push** job, and select **Scheduler Definition**.
2. For the **Repeat** field, select **interval**.
3. Set the **Repeat Every** field to **1 Day**, and click **OK**.
4. Edit the **SM History-based Push** job, and select **Scheduler Definition**.
5. For the **Repeat** field, select **interval**.
6. Set the **Repeat Every** field to **1 Day**, and click **OK**.

Step 8: Configure the SM-UCMDB Integration: Run Data Push Jobs

1. In the Integration Point pane, select the correct integration.
2. Select the **Data Push** tab. The Job Definition pane is displayed.
3. Select your job and click **Synchronize All** to run the push job.

> **Note:** For ServiceManagerAdapter7-1, run this first for the **SM History-based Push** job, then repeat for the **SM Topology Comparison Push** job.

4. When the Confirm synchronizing window is displayed, click **Yes**.
5. Click the **Statistics** tab to view the progress of the synchronization.
6. Click **Refresh** to view the updated synchronization status.

Step 9: Configure the SM-UCMDB Integration: Add UCMDB Connection Information to SM

1. Log on to your UCMDB system as an administrator. Verify that all UCMDB services are running.
2. Log on to your SM system as an administrator.
3. Select **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
4. Select the **Active Integrations** tab.
5. Select the **HP Universal CMDB** option. The form displays the UCMDB Web service URL field.
6. In the UCMDB Web service URL field, enter the URL to the UCMDB Web service API. The URL has the following format:

   http://<UCMDB server name>:<port>/axis2/services/ucmdbSMService.
7. In the UserId dialog box, enter your UCMDB user name and password and click **Save**.

Step 10: Configure the BSM-UCMDB Integration: Deploy CMS_to_RTSM_Sync.zip on UCMDB

1. Copy the file CMS_to_RTSM_Sync.zip located on the BSM-DPS machine file system under **HPBSM\odb\conf\factory_packages** to the file system on the UCMDB machine.
2. Within the UCMDB user interface, select the **Administration** tab.
3. Select **Package Manager > Deploy Packages to server (from local disk).**
4. Click the **Add** button and select the file **CMS_to_RTSM_Sync.zip** through the file system browser.
5. Select **Deploy**.

Step 11: Configure the BSM-UCMDB Integration: Create an Integration Point on BSM

1. Within the BSM user interface, select **RTSM Administration > Data Flow Management > Integration Studio.**
2. In the Integration Point pane, select **Create New Integration Point**. The Create New Integration Point dialog box opens. Enter the following:

Name	Recommended Value	Description
Integration Name	**<user defined>**	The name you give to the integration point.
Adapter	**UCMDB 9.x**	Select the adapter type from the drop-down list.
Is Integration Activated	**selected**	Select this check box to create an active integration point.
Hostname/IP	**<user defined>**	The name of the UCMDB server, load balancer, or reverse proxy.
Port	**<user defined>**	The port through which you access UCMDB, load balancer, or reverse proxy.
Credentials	**<user defined>**	If credentials appear in the Credentials column, select them. If no credentials appear, select **Generic Protocol** and click the **Add new connection details for selected protocol type** button. Enter the following information: ▪ **Description.** Enter **UCMDB**. ▪ **User Name.** Enter the UCMDB user name. The default value is **admin**. ▪ **User Password.** Enter and confirm a password.
Probe Name (for ServiceManagerAdapter9-x only)	**<user defined>**	If you are using ServiceManagerAdapter9-x, select the probe which reports to *BSM* (see "Prerequisites" on page 28).

3. Click the **Add** icon on the right side of the window and add Job definitions as follows:
   a. Name the **Job definition**.
   b. Select the **Allow Delete** check box.
   c. Click the **Add** icon in the Job definition window.
   d. From the pop up window, browse to **root - CMS sync** and select the **ActiveDirectory_ sync** job and click **OK**.
   e. Select the **Scheduler definition** check box.
   f. In the Repeat window, select **Cron**.
   g. For the Cron expression, enter the following string: *** 0/10 * * * ? *** .
   h. Adjust other settings as needed.
   i. When finished, click **OK** and save the integration.
   j. Repeat steps **a** to **i** and configure the following jobs:
      - **FailoverCluster_Sync**
      - **IIS_Sync**
      - **SOA_Sync**
      - **BusinessAndFacilities_Sync**
      - **ExchangeServer_Sync**
      - **Virtualization_Sync**
      - **Siebel_Sync**
      - **Credentials_Sync**
      - **Basicinfrastructure_Sync**
      - **J2EE_Sync**
      - **SAP_Sync**
4. Browse to UCMDB on port 21212 (for example, http://<DPS_host>.<domain>:21212), and select the **JMX Console**.
5. Log on to the JMX console.
6. From the UCMDB section, select **UCMDB:service=Multiple CMDB Instances Services**.
7. Invoke:
   a. **setAsGlobalIdGenerator** and verify it succeeded.
   b. **getGlobalIdGeneratorScopes** and verify it succeeded.
8. Within BSM, access **RTSM Administration > Data Flow Management > Integration Studio.**
9. Select the Integration Point that you have configured.
10. In the Job definition section, click **Synchronize All** to run the synchronization.

    The Integration Point should be active and the jobs are displayed properly.

Step 12: Configure the BSM-UCMDB Integration: Create an Integration Point on the CMS

1. Log into UCMDB and select **Data Flow Management > Integration Studio.**
2. In the Integration Point pane, select **Create New Integration Point**. The Create New Integration Point dialog box opens. Enter the following:

Name	Recommended Value	Description
Integration Name	**<user defined>**	The name you give to the integration point.
Adapter	**UCMDB 9.x**	Select the adapter type from the drop-down list.
Is Integration Activated	**selected**	Select this check box to create an active integration point.
Hostname/IP	**<user defined>**	The name of the BSM server, load balancer, or reverse proxy.
Port	**<user defined>**	The port through which you access BSM, load balancer, or reverse proxy.
Credentials	**<user defined>**	If credentials appear in the Credentials column, select them. If no credentials appear, select **Generic Protocol** and click the **Add new connection details for selected protocol type** button. Enter the following information: ▪ **Description.** Enter **UCMDB**. ▪ **User Name.** Enter the UCMDB user name. The default value is **admin**. ▪ **User Password.** Enter and confirm a password.
Probe Name (for ServiceManagerAdapter9-x only)	**<user defined>**	If you are using ServiceManagerAdapter9-x, select the probe which reports to the *CMS* (see "Prerequisites" on page 28).

3. Click the **Add** icon on the right side of the window and add Job definitions as follows:
   a. Name the **Job definition**.
   b. Select the **Allow Delete** check box.
   c. Click the **Add** icon in the Job definition window.
   d. From the pop up window, browse to **root - CMS sync** and select the **ActiveDirectory_ sync** job and click **OK**.
   e. Select the **Scheduler definition** check box.
   f. In the Repeat window, select **Cron**.
   g. For the Cron expression, enter the following string: *** 0/10 * * * ? *** .
   h. Adjust other settings as needed.
   i. When finished, click **OK** and save the integration.
   j. Repeat steps **a** to **i** and configure the following jobs:
      - **FailoverCluster_Sync**
      - **IIS_Sync**
      - **SOA_Sync**
      - **BusinessAndFacilities_Sync**
      - **ExchangeServer_Sync**
      - **Virtualization_Sync**
      - **Siebel_Sync**
      - **Credentials_Sync**
      - **Basicinfrastructure_Sync**
      - **J2EE_Sync**
      - **SAP_Sync**
4. Browse to UCMDB on port 8080 (for example, http://yourUCMDBhost.domain:8080), and select the **JMX Console**.
5. Log on to the JMX console.
6. From the UCMDB section, select **UCMDB:service=Multiple CMDB Instances Services**.
7. Invoke:
   a. **setAsGlobalIdGenerator** and verify it succeeded.
   b. **getGlobalIdGeneratorScopes** and verify it succeeded.
8. Within UCMDB, access **Data Flow Management > Integration Studio.**
9. Select the Integration Point that you have configured.
10. In the Job definition section, click **Synchronize All** to run the synchronization.

    The Integration Point should be active and the jobs are displayed properly.

Step 13 (Optional): Add CI Types to the Service Health Changes and Incidents Component

By default, BSM Service Health displays information on incidents and requests for change for the following CI types: Business Service, Siebel Application, Business Application, and Node.

If you want to view change and incident information for other CITs, perform the procedure described in "How to Customize the Changes and Incidents Component" on page 48.

Step 14 (Optional): Map Siebel Application CITs

To create a mapping between the **Hand Held Devices** or **Display Device** CIT in Service Manager with **Siebel Application** CITs in BSM, perform one of the following procedures:

- In Service Manager, select **Main page > To Do > Queue: Configuration Item > New > New** and click **Device**. In the Configuration Item field enter the exact name (case sensitive) of the BSM CI that corresponds to the **Siebel Application** CIT in BSM.
- Create a new population job that includes the **Hand Held Devices** or **Display Device** CIT. Those CITs correspond to the Siebel application CITs. For details about how to create a population job, see "Data Push Tab" in the *Modeling Guide*.

Result

You can now view planned changes and incident details in the Changes & Incidents tab in the 360° View page in Service Health.

Both products can now share information and data.

Chapter 4

View Changes and Incidents in Service Health Using RTSM

This integration enables you to view planned changes and incident details in the Changes & Incidents tab in the 360° View page in Service Health, when you are working with RTSM. For details, see "Changes and Incidents" in the Service Health part of the *BSM User Guide*.

This section includes the following:

Prerequisite

If you are using SM versions 9.30 or 9.31, before you begin you must install a data-flow probe with the BSM Gateway Server as its target. When you configure the integration point, you will select this probe for the integration.

Step 1: Configure the Service Desk Adapter Time Zone

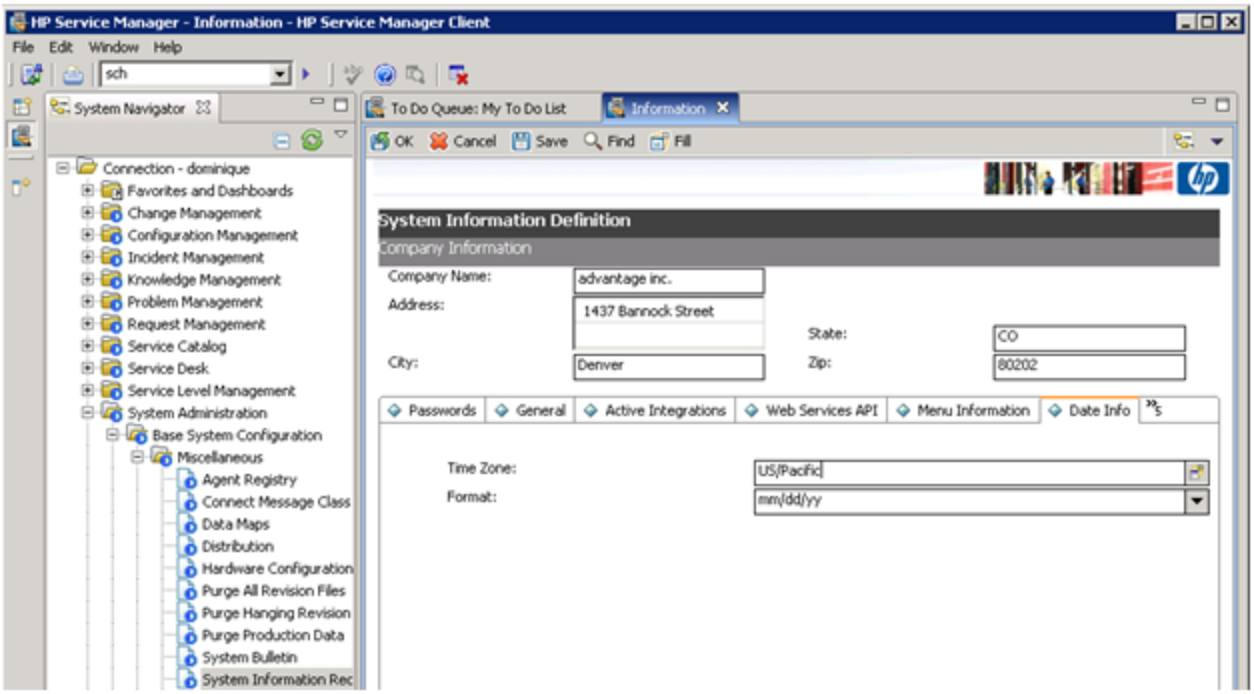
Configure the time zone so Incidents and Planned Changes have the correct time definitions:

1. In Service Manager, select **Navigation pane > Menu navigation > System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Within the **Date Info** tab, open the <BSM DPS root directory>/odb/runtime/fcmdb/CodeBase/ServiceManagerAdapter9-x or ServiceDeskAdapter7-1/serviceDeskConfiguration.xml file.
3. Find the row that includes the following string:

<globalConnectorConfig><![CDATA[<global_configuration><date_pattern>MM/dd/yy HH:mm:ss</date_pattern><time_zone>US/Pacific</time_zone>

and check the date and time format, and time zone. Note that the date is case-sensitive. Change either Service Manager or the xml file so that they both match each other's settings.

Note: Specify a time zone from the Java time zone list that matches the time zone used in Service Manager; for example, America/New York.



4. Restart the corresponding server to make the change take effect. (If you changed the time zone on SM, restart the Service Manager server; if you changed the time zone on BSM, restart the BSM server.)

Step 2: Create an Integration User Account in Service Manager

This integration requires an administrator user account for BSM to connect to Service Manager. This user account must already exist in both BSM and Service Manager.

To create a dedicated integration user account in Service Manager:

1. Log in to Service Manager as a system administrator.
2. Type **contacts** in the Service Manager command line, and press ENTER.
3. Create a new contact record for the integration user account.
   a. In the **Full Name** field, type a full name. For example, RTSM.
   b. In the **Contact Name** field, type a name. For example, RTSM.

c. Click **Add**, and then OK.

4. Type **operator** in the Service Manager command line, and press ENTER.
5. In the **Login Name** field, type the username of an existing system administrator account, and click **Search**.

   The system administrator account displays.
6. Create a new user account based on the existing one:
   a. Change the **Login Name** to the integration account name you want (for example, rtsm).
   b. Type a **Full Name**. For example, RTSM.
   c. In the **Contact ID** field, click the **Fill** button and select the contact record you have just created.
   d. Click **Add**.
   e. Select the **Security** tab, and change the password.
   f. Click **OK**.

The integration user account is created. Later you will need to add this user account (username/password) in RTSM, and then specify this user account in the **Credentials ID** field when creating an integration point in RTSM administration.

Step 3: Add the BSM Connection Information in Service Manager

The integration requires the BSM connection information to obtain CI attribute information from the BSM system, and display it in the Actual State section in the Service Manager configuration item form.

1. Log in to Service Manager as a system administrator.
2. Click System Administration > Base System Configuration > Miscellaneous > System Information Record.
3. Click the Active Integrations tab.
4. Select the HP Universal CMDB option.

   The form displays the UCMDB web service URL field.
5. In the UCMDB webservice URL field, type the URL to the HP Universal CMDB web service API. The URL has the following format: http://<UCMDB server name>:<port>/axis2/services/ucmdbSMService

   Replace <UCMDB server name> with the host name of your BSM server, and replace <port> with the communications port your BSM server uses.
6. In UserId and Password, type the user credentials required to manage CIs on the BSM system. For example, the out-of-the-box administrator credentials are admin/ admin.
7. Click Save. Service Manager displays the message: Information record updated.

8. Log out of the Service Manager system.
9. Log back into the Service Manager system with an administrator account. The Actual State section will be available in CI records pushed from BSM.

Step 4: Create an Integration Point in BSM

A default RTSM 9.05 installation already includes the ServiceManagerAdapter9-x package. To use the integration package, you must create an integration point listing the connection properties for the integration.

To create an integration point:

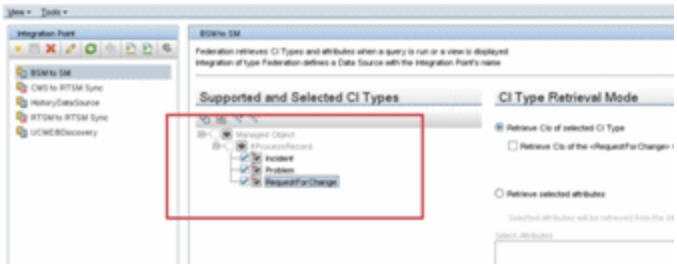
1. Access the JMX console (in case of distributed deployment) on the DPS server.
2. Navigate to **UCMDB:service=Security Services**.
3. Create a new user with the name and password that you created in SM, using the JMX **createUser**:
   - **CustomerId** = 1
   - **userName** = <userName>
   - **password** = <password>
4. Assign the user Administrator Role using the JMX **setRolesForUser** from the same section:
   - **CustomerId** = 1
   - **userName** = <userName>
   - **roles** = Admin
5. In BSM, select **Admin > RTSM Administration**, click the **Data Flow Management** tab, and select **Integration Studio**.
6. In the Integration Point pane, select **Create New Integration Point**. The Create New Integration Point dialog box opens. Enter the following:

Name	Recommended Value	Description
Integration Name	**SM Integration**	The name you give to the integration point.
Adapter	**<user defined>**	Select HP BTO Products > Service Manager > **Service Manager 9.xx**. This adapter, which supports CI/ relationship Data Push from RTSM to Service Manager, and Population and Federation from Service Manager to RTSM.
Is Integration Activated	**selected**	Select this check box to create an active integration point.

Name	Recommended Value	Description
Hostname/IP	**<user defined>**	The name of the SM server.
Port	**<user defined>**	The port through which you access SM.
Credentials	**<user defined>**	Click **Generic Protocol**, click the **Add** button to add the integration user account you created in "Step 2: Create an Integration User Account in Service Manager" on page 41, and then select it. This account must exist in both Service Manager and BSM.
Probe Name (for ServiceManagerAdapter9-x only)	**<user defined>**	Select the probe that you installed for this integration.

Note: It is recommended to click the **Test Connection** button to verify that the details entered are working before continuing.

7. In the **Integration Point** pane, click the Integration Point you just created, and click the **Federation** tab in the right pane.
8. In the **Supported and Selected CI Types** area, verify the **Incident**, **Problem**, and **Request for Change** CITs are selected.

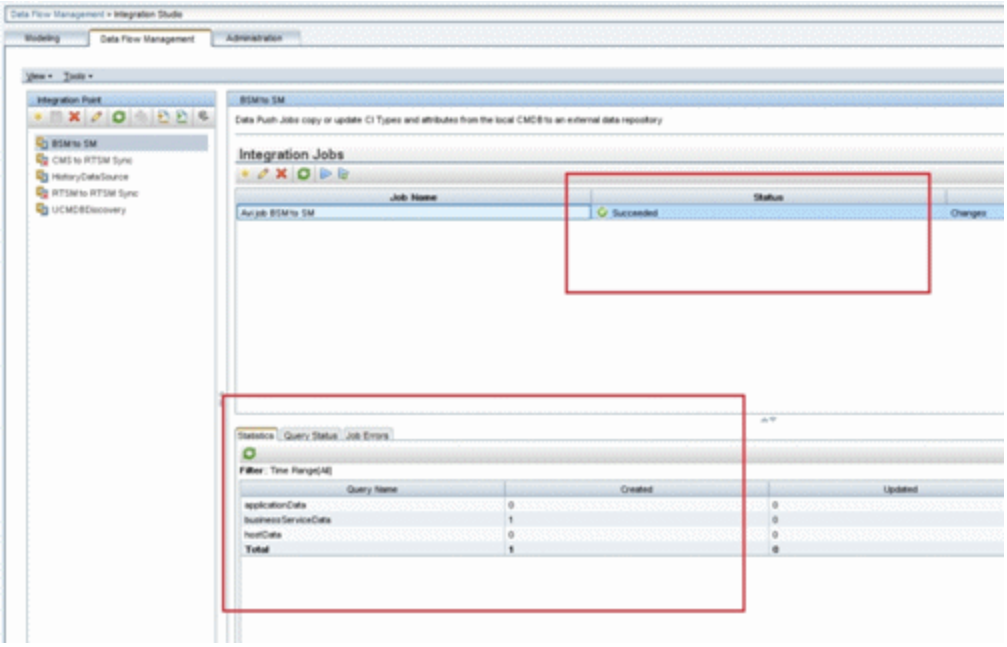


Step 5: Create New Jobs to Synchronize Between BSM and Service Manager

1. In the same location as step 5 above, click the **Data Push** tab.
2. In the New Integration Job dialog box, click the + icon on the left.
3. In the Available Queries dialog box, select the relevant queries for the job.

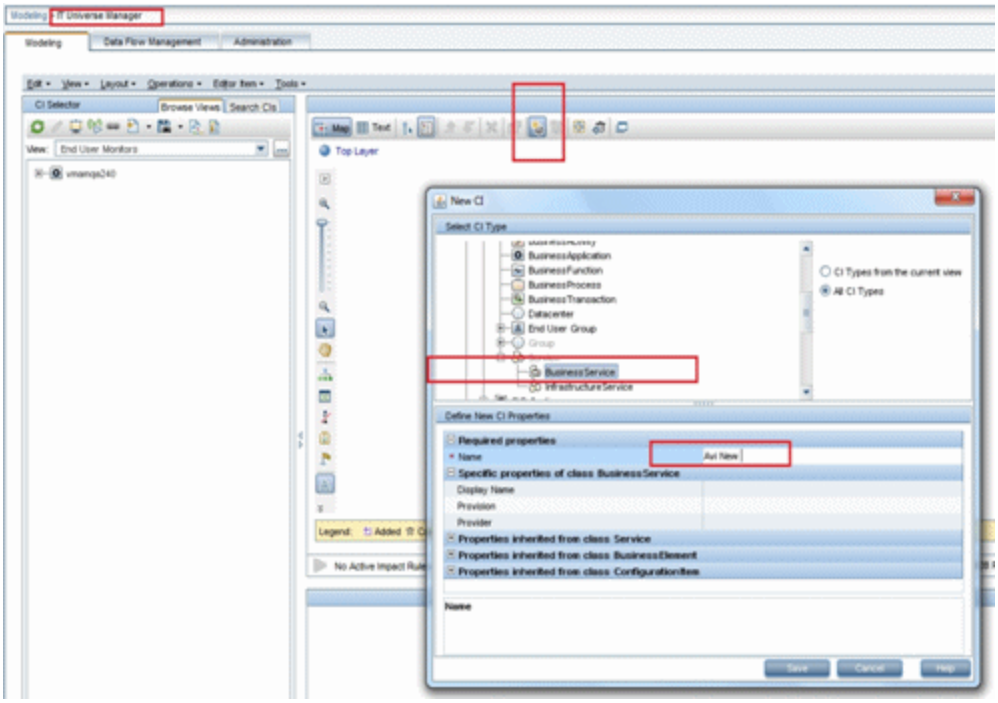
Step 6: Run the Job

When you run the job, the CIs are synchronized between BSM and Service Manager.

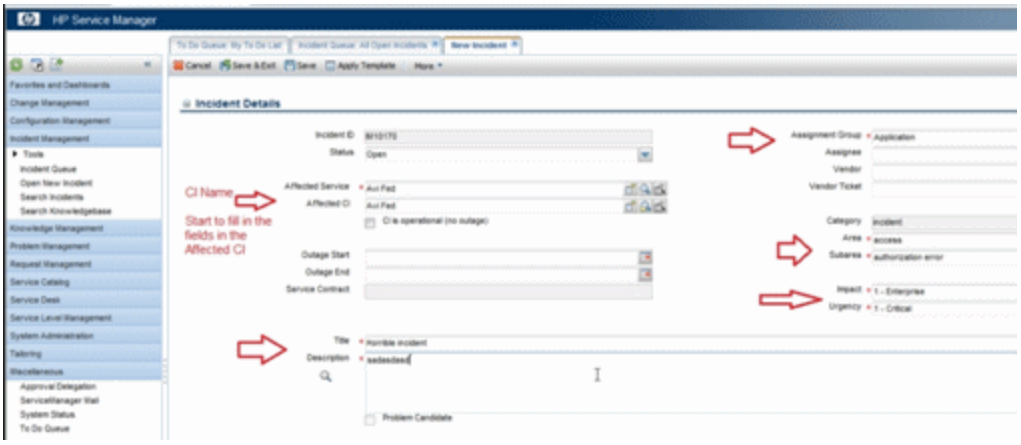


Step 7: Test the Configuration

1. In BSM, select **Admin > RTSM Administration**, click the **Modeling** tab, and select **IT Universe Manager**.
2. In the **CI Selector** pane, select the relevant view, and click  in the right pane.
3. In the **New CI** dialog box that opens, create a new CI with the **BusinessService** type.

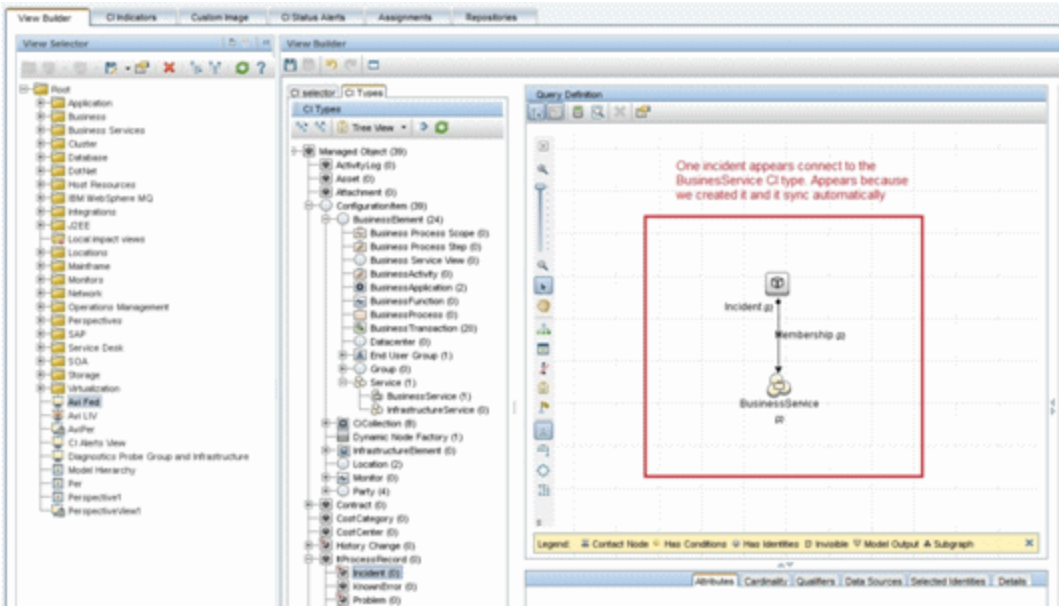


4. Create a TQL in **Admin > Service Health > View Builder** that includes only BusinessService CI Types (CITs).
5. Click the **Calculate** button. The relevant CI appears in view.
6. Click the **Data Push** tab, and run the job in order to synchronize with Service Manager. A message that the job was successful should be issued.
7. In Service Manager, create a new incident for the new CI that you created above:
   a. Select **Incident Management > Open New Incident**.
   b. **Important:** Start by entering the name of the CI you want to attach to the incident in the **Affected CI** field. This creates the Incident Id.
   c. Enter the CI name in the **Affected Service** field and click to search.
   d. Enter any incident detail.

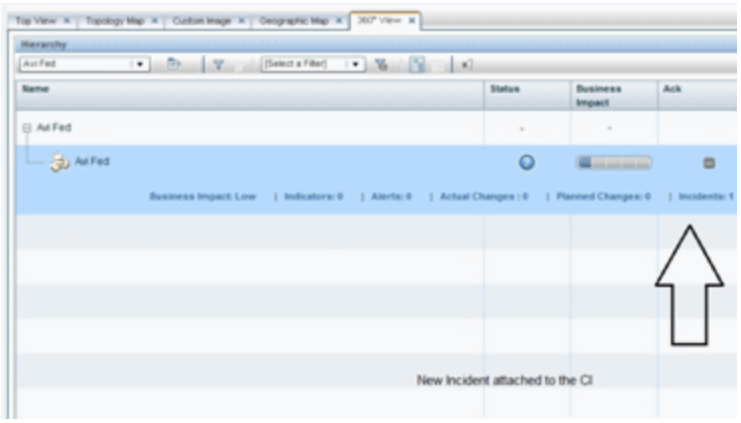


The incident is automatically attached to the CI.

8. In BSM, create a TQL with the CI Type you created connected to the Incident CI Type in a membership relationship link.
9. Click the **Calculate** button. One incident appears connected to the BusinessService CI Type because this test created it and it is synchronized automatically.



10. Delete the incident from the TQL and save the TQL to be a view. The TQL is only used for the test.
11. Select **Application > Service Health**, and click the **360 View** tab. Check that the new incident is attached to the CI.



Step 8 (Optional): Add CI Types to the Service Health Changes and Incidents Component

By default, BSM Service Health displays information on incidents and requests for change for the following CI types: Business Service, Siebel Application, Business Application, and Node.

If you want to view change and incident information for other CITs, perform the procedure described in "How to Customize the Changes and Incidents Component" on page 48.

Chapter 5

How to Customize the Changes and Incidents Component

By default, incidents and requests for change are displayed for the following CI types: Business Service, Siebel Application, Business Application, and Node. If you want to view change and incident information for other CITs, perform the following procedure:

1. Within **Admin > RTSM Administration > Modeling Studio**, copy one of the TQLs within the **Console** folder, and save your copy with a new name. These default TQLs perform the following:

TQL name	Description
CollectTicketsWithImpacts	Retrieves Service Manager incidents for the selected CI, and for its child CIs which have an Impact relationship.
CollectTicketsWithoutImpacts	Retrieves Service Manager incidents for the selected CI.
CollectRequestForChangeWithImpacts	Retrieves Service Manager requests for change, for the selected CI, and for its child CIs which have an Impact relationship.
CollectRequestForChangeWithoutImpacts	Retrieves Service Manager requests for change, for the selected CI.

2. Edit the new TQL as needed. You can add CITs as described in "Naming Constraints for New Request for Change TQLs" on next page.
3. Access **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:
   - Select **Applications**.
   - Select **Service Health Application**.
   - In the **Service Health Application - Hierarchy (360)** area, enter the name of the new TQL you have create in the corresponding infrastructure setting.

   Note that by default these infrastructure settings contain the default TQL names. If you enter a TQL name that does not exist, the default value will be used instead.

After you modify the infrastructure setting, the new TQL will be used, and the Changes and Incidents component will show this information for the CITs you have defined.

Naming Constraints for New Request for Change TQLs

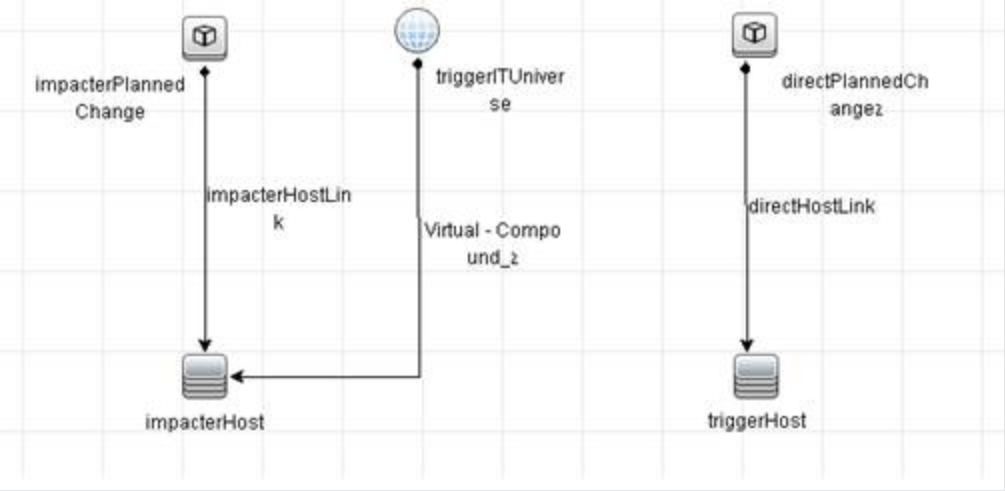
The following naming constraints should be followed in the request for change *without* impact TQL (see the TQL example below, on the right side of the image):

- The request for change CI type should start with **directPlannedChange**.
- The CI type related to the request for change should start with **trigger**.

The following naming constraints should be followed in the request for change *with* impact TQL (see the TQL example below, on the left side of the image):

- **impacterPlannedChange** represents the request for change CI type.
- The CI type related to the request for change should start with **impacter**.
- **triggerITUniverse** represents the "impacted" child CIs.

Examples of request for change TQLs:



Naming Constraints for New Incident TQLs

The following naming constraints should be followed in the incidents *without* impact TQL (see the TQL example below, on the right side of the image):

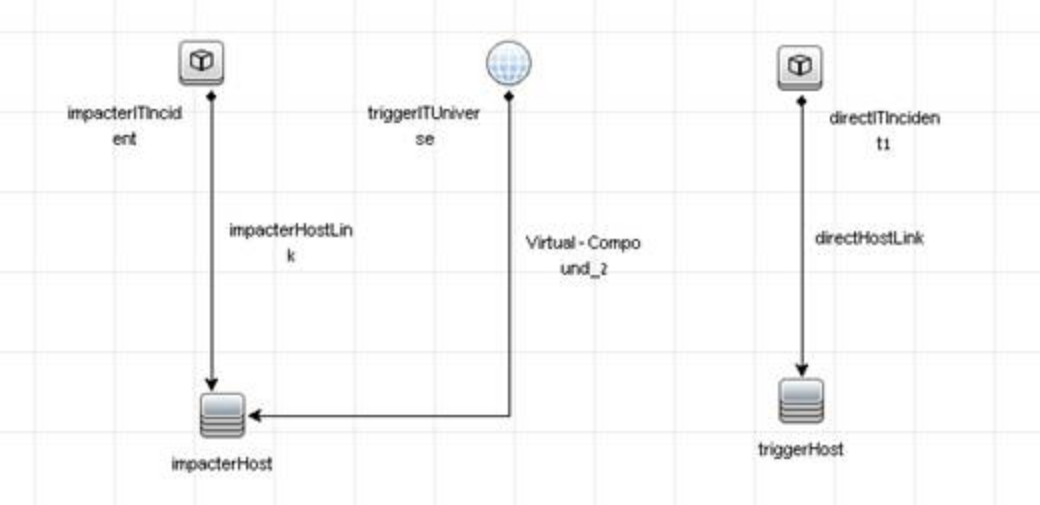
- The incident CI type should start with **directITIncident**.
- The CI type related to the incident should start with **trigger**.

The following naming constraints should be followed in the incidents *with* impact TQL (see the TQL example below, on the left side of the image):

- **impacterITIncident** represents the incident CI type.
- The CI type related to the incident should start with **impacter**.

- **triggerITUniverse** represents the "impacted" child CIs.

Examples of incident TQLs:



Chapter 6

Generate Incidents in Service Manager When a BSM Alert is Triggered

This integration enables you to configure specific CI Status alerts, SLA alerts, or EUM alerts to automatically open a corresponding incident in HP Service Manager. The alerts are mapped to the events using the Event Template.

The triggered alert forwards a corresponding event to OMi, where (using the Incident exchange between Service Manager and Operations Manager I integration) the event is changed into an incident and sent, using the Event Forwarding Service, to HP Service Manager to proactively alert the operator about a problem in the system..

To automatically forward an event when an alert is triggered, follow the steps described in this section. This section includes the following:

CI Status Alerts

By default, a CI Status alert is mapped to an event using a default Event Template. You can modify the default Event Template or select a different Event Template as follows:

1. Select **Admin > Service Health > View Management > CI Status Alerts**, select a view and a CI and click **New Alert** or select an existing alert and click **Edit**.
2. In the Actions page, click the **New Event Generation** link in the **Generate Events** section.
3. In the **CI Alert Template Repository** dialog box that opens, select the template you want to use to map the alert to an event and click **Select**. The template you selected is now listed in the Generate Events section. For user interface details, see "CI Status Template Repository Dialog Box" in the Service Health part of the *BSM Application Administration Guide*.

SLA Alerts

By default, an SLA alert is mapped to an event using a default Event Template. You can modify the default Event Template or select a different Event Template as follows:

1. Select **Admin > Service Level Management > SLA Alerts**, click **New Alert** or select an existing alert and click **Edit**.
2. In the Actions page, click the **New Event Generation** link in the **Generate Events** section.
3. In the **SLA Template Repository** dialog box that opens, select the template you want to use to map the alert to an event and click **Select**. The template you selected is now listed in the

Generate Events section. For details, see "SLA Template Repository Dialog Box" in the Service Level Management part of the *BSM Application Administration Guide*.

EUM Alerts

By default, an EUM alert is mapped to an event using a default Event Template. You can modify the default Event Template or select a different Event Template as follows:

1. Select **Admin > End User Management > Monitoring**, select the view and the CI in the left pane, click the **Alerts** tab, and click the **Press to create new alert** button, or select one of the alerts, and click the **Press to edit alert button**.
2. In the Actions page, select the **Generate Event** option.
3. In the Definition Details area, in the Actions section, click the first link in the **Generate events with <template name> template and <value> values Event Type Indicator**, to select or modify the default template that maps the alert to the event in the **Template Repository** dialog box. For user interface details, see "Notification Templates Dialog Box" in the End User Management part of the *BSM Application Administration Guide*.
4. Click the second link to open the Event Type Indicator dialog box, where you specify the ETI that corresponds to the alert. For user interface details, see "Event Type Indicator Dialog Box" in the End User Management part of the *BSM Application Administration Guide*.

Chapter 7

View Incident Data in BSM, and Manage SLAs Based on Service Manager

This integration enables you to view the Number of Open Incidents in Service Health, and manage SLAs over Serviceability KPIs based on SM incidents, using EMS configuration.

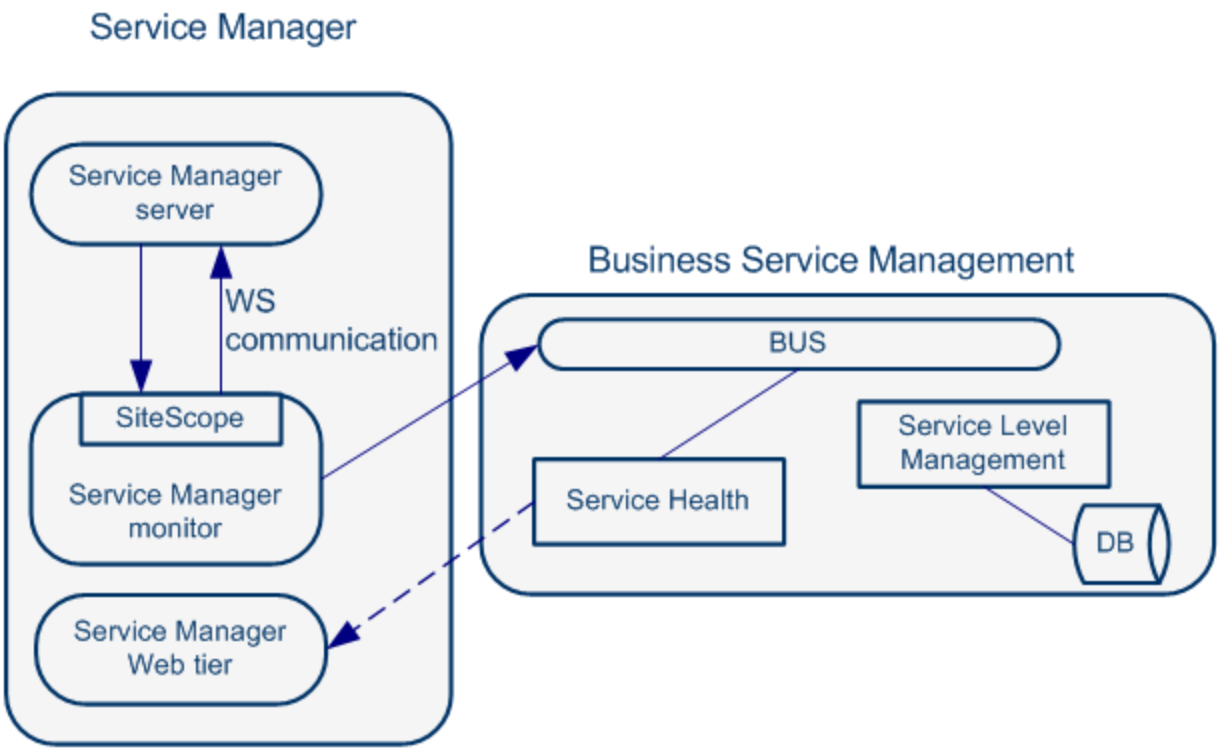
This section includes the following:

Overview: Understanding the Integration with EMS

The following sections describe the capabilities provided by the integration of Business Service Management and HP Service Manager with the EMS option.

Architecture

The architecture of the integration of Service Health and Service Level Management with HP Service Manager is as follows:



You can work with one or more of the following options:

- **Number of Open Incidents KPI.** You can view the Number of Open Incidents KPI (based on data from HP Service Manager) at the business service level in the BSM Service Health views and reports. For details about the views, see "View Topology" in the Service Health part of the *BSM User Guide*. For example: the Operator/Application support can get visibility and alerts based on the Number of Open Incidents in BSM Service Health alongside operational KPIs.
- **Drill down to HP Service Manager from EMS monitor level CIs.** You can drill down from Service Health views at the EMS monitor level business service level to HP Service Manager to view the details of the related incidents. For details about the available drill downs, see "Service Health Menu Options" in the Service Health part of the *BSM User Guide*. For example: the support person can drill down to HP Service Manager to view the details on the open incidents of the selected service. Based on the number of incidents and their details, the support person can prioritize the issues that are the most important.

The assignment of the Service Manager EMS integration enriches the relevant CIs with the appropriate KPIs, rules, and context menus that are to be assigned automatically to the CIs when the condition occurs, and the assignment is running. For details, see "EMS Integrations Application Overview" in the Integrations Administration part of the *BSM Application Administration Guide*.

Defining SLAs

You can define SLAs based on the serviceability KPIs (MTTR, MTBF, or MTBSI KPIs) that are calculated based on incidents that come from HP Service Manager. For details, see "Agreements" in the Service Level Management part of the *BSM Application Administration Guide*.

For example: the HP Service Manager manages SLAs with operational KPIs (Availability, Performance, or other KPIs) and serviceability KPIs (MTTR, MTBF, or MTBSI KPIs) using BSM

Service Level Management. The HP Service Manager can review the SLAs statuses according to the service Availability, Performance, MTTR, and MTBF side-by-side.

Elements Created in the View by the Integration with HP Service Manager

The HP Service Manager integration creates the following elements:

Element	Service Health	Service Level Management
CIs	EMS Monitor CIs for the monitored HP Service Manager system, based on the samples sent by the SiteScope HP Service Manager Monitor. Status for these CIs can be viewed in Service Health in the Business Services, Service Manager, and the Service Measurements views, and the CIs are available to add to SLAs in Service Level Management. Note: All HP Service Manager elements are currently mapped to Business Service CIs through EMS.	
Health Indicators	Ticketing EMS Monitor HI. For more information, see "Indicator Repository" in the Service Health part of the *BSM Application Administration Guide*.	MTBF EMS Monitor HI, MTBSI EMS Monitor HI, and MTTR EMS Monitor HI. For more information, see Indicator Repository" in the Service Level Management part of the *BSM Application Administration Guide*.
KPIs	Number of Open Incidents KPI. For details, see "List of Service Health KPIs" in the Service Health part of the *BSM Application Administration Guide*.	MTTR (Mean Time to Repair, MTBF (Mean Time Between Failures, and MTBSI (Mean Time Between System Incidents KPIs. For details, see "List of Service Level Management KPIs" in the Service Level Management part of the *BSM Application Administration Guide*.

Rules and Toolips	The Number of Open Incidents KPI (attached to an EMS Monitor CI) uses the Number of Open Incidents monitor rule in Service Health and the Number of Open Incidents Sentence tooltip. The rule handles the samples sent to BSM by the EMS system. For details on the rule, see List of Calculation Rules in Service Health" in the Service Health part of the *BSM Application Administration Guide*. For details on the rules, see "List of Service Level Management Business Rule Parameters" in the Service Level Management part of the *BSM Application Administration Guide*.	Each HP Service Manager KPI (attached to an EMS Monitor CI) uses its own monitor rule.
Context Menu	The HP SC Menu. For details on the context menu, see "List of Context Menus" in the Service Health part of the *BSM Application Administration Guide*.	N/A
Context Menu Item	The Service Manager context menu item. For details on the context menu, see "List of Context Menu Actions" in the Service Health part of the *BSM Application Administration Guide*.	N/A

Note: Only incidents for which you select a CI in the **Affected CI** field are retrieved by EMS. The CI listed in the **Affected CI** field represents an incident-related item. The default EMS settings only support the monitoring of Business Service CITs.

EMS does not count the incidents that were open through incident exchange (OMi events to SM incidents - part of CLIPv9 solution).

Prerequisites

The HP Service Manager server, Web tier, and Windows client components must be installed. For details, see HP Service Manager Installation guide.

Optional. If you want HP Service Manager to use the SSL-based Trusted Sign-on protocol, configure it according to the instructions in the HP Service Manager online help.

Optional. If you want HP Service Manager to use the LW-SSO, configure it according to the instructions in the HP Service Manager online help. BSM must also be configured with LW-SSO.

Note: Plan to put both the HP Service Manager Web tier and the webapp in the same container, so you can use the same certificate for both.

Step 1: Enable Access to HP Service Manager From Within Service Health

Disable the query security of the HP Service Manager application to enable accessing the application, through the right-click HP Service Manager menu option in Service Health. You still have the necessary capabilities to properly secure your system without the query hash.

To enable accessing HP Service Manager from within Service Health:

1. After installing and configuring LW-SSO, edit the web.xml file. The location of the file depends on the type of Web application server the Web tier is deployed on. It is usually located in the HP Service Manager home directory under the Apache home directory. The web.xml file can be located at: **\Apache Software Foundation\Tomcat 5.5\webapps\sm7\WEB-INF**
2. In the file, locate the **<!-- Specify the Service Manager server host and port location -->** section. This section should appear after the **sc.honorUrlPort** section.
3. Verify that the following strings exists in the section:
   <init-param>
   <param-name>querysecurity</param-name>
   <param-value>false</param-value>
   </init-param>
4. Restart the Tomcat container using the Net stop tomcat and Net start tomcat commands.

Step 2: Define HP Service Manager Tables for External Access to the Clocks

To enable the integration, load the appropriate .unl to provide external access to the clocks table in HP Service Manager. This step enables the display of the Number of Incidents KPI in Service Health. This can be done as follows (note that the probsummary table is accessed by default without .unl):

- In HP Service Manager, manually within HP Service Manager if the tables are used for other external internal integrations. For details, refer to the HP Service Manager documentation.
- Using the configuration file supplied with HP Business Service Management to enable external access to the clocks table:
  a. Locate the **Clocks_extaccess_sm702_10Nov08.unl** available in the **Setup\SM_Unloads** directory on the BSM DVD or in the electronic download package, and copy it to a local directory.
  b. Open the HP Service Manager client and connect to the server.

c. Select **Toolkit > Database Manager**.

d. In the menu on the upper right side of the Database Manager, select **Import/Load**.

e. Select the configuration file you copied to the local directory in the first step.

f. Click the **Load FG** button in the left top corner of the page.

g. Verify that the clocks table has the values described below. If the values do not match, edit the clocks table in HP Service Manager so that the values are the same as in the below table (for details on how to do that, see HP Service Manager documentation).

Field	Caption	Type
events[start]	start	DateTimeType
events[stop]	stop	DateTimeType
name	name	StringType
key.char	clockId	StringType
sysmodtime	sysmodtime	DateTimeType
type	type	StringType
Key.numeric	clockKey	DecimalType

Step 3: Correct the Clocks WSDL

Correct the clocks WSDL to enable the display of the Number of Incidents KPI in Service Health.

1. In the HP Service Manager client, select **Menu Navigation > Tailoring > Web Services > WSDL Configuration**, enter **Clocks** in the **Service Name** field, and click **Search**.
2. Click the **Field** tab.
3. Add the following entry:

Field	Caption	Type
Total	temp	StringType

Note: The values in the table have no meaning.

4. Click **Save** and **OK**.
5. Click **Search** again, click the **Fields** tab and clear the new entry.
6. Click **Save** and **OK**.

Step 4: Add the Type Field to the logical.name Link Line

This step enables EMS to count incidents that were manually opened in HP Service Manager and to display of the Number of Incidents KPI in Service Health.

Note:

- For new customers, EMS calculates ONLY incidents that were manually opened after the tailoring process was applied. For existing customers, the previous HP Service Manager version is populating these fields and the integration works even after you upgrade to HP Service Manager to 7.10. Skip this step if you use other versions. Incidents opened by incident submission are always calculated.
- Perform this step before you configure the SiteScope HP Service Manager Monitor accessed in BSM by clicking **Admin > Integrations > EMS Integration Admin**. Only incidents that were opened after this step are displayed in BSM Service Health.

You add the Type field to the logical.name link line in the probsummary link record as follows:

In HP Service Manager, login with a System Administrator user (for example, **falcon**).

1. Select **Menu Navigation > Tailoring > Tailoring Tools > Links**.
2. Enter **probsummary** in the **Name** field and click **Search**.
3. Set the cursor on the first line that includes **logical.name** in the **Source Field Name** field (line 14).
4. Select **Select Line** in the **Options** menu.
5. Make sure the following entries are present in the table:

Source Field	Target Field
logical.name	logical.name
company	company
type	type
initial.impact	default.impact
severity	problem.priority

6. Click **Save**, **Back**, and then **OK**.

Step 5: Create a Corresponding HP Service Manager User

This step enables the display of the Number of Incidents KPI in Service Health.

1. Create a dedicated user in HP Service Manager. The user should be used solely for the purposes of the HP Business Service Management/SiteScope integration.
2. Make sure that the HP Service Manager machine and the SiteScope machine share the same time zone.
3. Make sure that the HP Service Manager machine and the SiteScope machine use the same date format (SiteScope date format): **dd/mm/yy**.
4. When configuring the monitor, use the value for the **Username** and **Password** fields that you created in HP Service Manager.

Step 6: Configure the HP Service Manager Monitor in SiteScope

Configure the HP Service Manager monitor in SiteScope as follows:

1. Synchronize HP Service Manager and SiteScope so their time zones are the same. Match their System Time in the Windows or Unix operating system.
2. Make sure that the user you are using in SiteScope is the user you defined in “Create a Corresponding HP Service Manager User.”
3. Make sure you have installed the SiteScope EMS license. Note that you do not require this license if SiteScope 11.0 or later is used.
4. Configure the HP Service Manager monitors in SiteScope as follows:
   a. Stop SiteScope.
   b. On the SiteScope operating system go to **<SiteScope root directory>\conf\ems\peregrine\lib\<SM version>** and copy **incidentAttributesMapping.conf** to **<SiteScope root directory>\conf\ems\peregrine**.
   c. On the SiteScope operating system go to **<SiteScope root directory>\conf\ems\peregrine\lib\<SM version>** and copy **peregrine.jar** to **<SiteScope root directory>\WEB-INF\lib**.
   d. Start SiteScope
   e. Create a new monitor using the following fields:
      - **Web Service**: <protocol>://<SMhost>:<SMport>/sc62server/PWS/
      - **user name**: <user name defined in "Step 5: Create a Corresponding HP Service Manager User" on previous page >
      - **user pass**: <password of user created in "Step 5: Create a Corresponding HP Service Manager User" on previous page >
      - **incident management query**: <type of CI> should be the same as the **Type** field of the CI in Service Manager. For example, for the Business Service CI Type in SM, use **bizservice**.

Step 7: Specify the HP Service Manager Web Tier URL in the Infrastructure Settings

The HP Service Manager URL is used when drilling down from BSM to HP Service Manager using the **HP SC Menu** context menu item.

1. To specify the HP Service Manager URL, in BSM, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, select **Foundations**, and select **Integrations with other applications**.
2. In the Integrations with other applications - HP ServiceCenter - Ticketing Integration table, enter the appropriate URL in the **ServiceCenter/Service Manager web tier URL** entry, using the following format: **<protocol>://<host_name>:<port>/<web_app_name>/** where **host_name** is the name of the HP Service Manager server, **port** is the port number of the HP Service Manager server, and **web_app_name** is the name of the application.

The URL of HP Service Manager is, for example, **http://fando:8080/sm7/**.

Step 8: Customize the HP Service Manager EMS Integration Adapter and Check the Assignment – Optional

The HP Service Manager integration adapter is predefined. You can customize the configuration. Make sure that the assignment rule is running (it is running by default).

In BSM, select **Admin > Integrations > EMS Integration Admin, select ServiceCenter** and click **Edit**. In the Edit Integration dialog box:

1. **Configure the HP Service Manager Monitor – Optional.** The monitor is used to retrieve data from the EMS system using System Availability Management Administration. The HP Service Manager Monitor is added to a SiteScope monitor group created for this monitor and other Integration Monitor types. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and HP Business Service Management is established. For details, go to "How to Work with the HP Service Manager Integration" in *Monitor Reference* in the SiteScope documentation library.

   Note: SiteScope cannot be deployed behind a firewall. SiteScope and the monitored system must be on the same LAN or special firewall configuration might be required.

2. **Activate the data assignment rule.** Make sure that the assignment rule is running.

   When the EMS monitor sample includes open incidents in its data source, the **Number of Open Incidents** KPI (2600), the **Number of Open Incidents** rule (2600), the **HP SC Menu** context menu (hpsc), the **HP Service Manager** context menu item, and the **Number of Open Incidents** tooltip (2600) are assigned to the EMS Monitor CI.

   You can use the EMS Integrations application to customize an HP Service Manager integration. The integration forwards the retrieved data captured from the HP Service Manager system by the SiteScope HP Service Manager monitor to BSM, and creates the appropriate topology that is used to display the data in Service Health. For details on the possible customizations, see

"Edit Integration Dialog Box" in the Integrations Administration part of the *BSM Application Administration Guide*.

Step 9: Specify the State and Severity of Open Incidents to Be Displayed – Optional

To modify the state and severity of the open incidents to be displayed, you can edit the parameters of the Number of Open Incidents rule parameters:

- **For the Number of Open Incidents KPIs attached to a specific EMS Monitor CI.** In BSM, select **Admin > Service Health > Assignments > KPI Assignments**, select the **ServiceCenter** view and the EMS Monitor CI, edit the **Number of Open Incidents** rule, and edit the **Initial State, Final State,** and **Severity** parameters.
- **Globally, for all KPIs defined with the Number of Open Incidents rule**. In BSM, select **Admin > Service Health > Repositories > Business Rules**, clone or override the **Number of Open Incidents** rule, and edit the **Initial State, Final State**, and **Severity** parameters.

For details on the parameters, see "List of Calculation Rules in Service Health" in the Service Health part of the *BSM Application Administration Guide*.

Note: The values available for the Initial State, Final State, and Severity parameters reflect the values defined in HP Service Manager. BSM severity is correlated with HP Service Manager urgency.

Step 10: Include HP Service Manager CIs in Service Level Management Agreements

You can include HP Service Manager EMS Monitor CIs in your agreements in Service Level Management. Service Level Management contains KPIs and rules specifically configured for Service CenterHP Service Manager EMS Monitor CIs. The MTTR, MTBF, and MTBSI KPIs and the MTTR, MTBF, and MTBSI rules are dedicated for this integration.

You also configure the incident initial and final state in those rules. For details, see "Service Level Management KPIs for System Incidents" in the Service Level Management part of the *BSM Application Administration Guide*, and locate "Incident State and Severity Values".

Results

After the task is performed, HP Service Manager data is integrated into BSM. You can:

- **View HP Service Manager Data in Service Health and Service Level Management:**

  SiteScope automatically creates the appropriate topology when HP Service Manager data is integrated into BSM. HP Business Service Management adds the data to the Business Services, ServiceCenter, and Service Measurements views, and you can display these views in Service Health. The Business Service and EMS Monitor CIs are added to Service Level Management.

- **Drill down to HP Service Manager from Service Health views:**

  In Service Health, in the ServiceCenter, and Service Measurements views, use the **HP Service Manager** option available for **EMS Monitor** CIs under Business Service CIs, to access the relevant incident in the HP Service Manager application. For information about the HP Service Manager application, consult the HP Service Manager documentation.