Hewlett Packard
Enterprise

HPE Application Performance Management

Software Version: 9.30

APM - Service Manager Integration Guide

Document Release Date: August 2016
Software Release Date: July 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

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

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

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

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

iPod is a trademark of Apple Computer, Inc.

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

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

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

Support

Visit the HPE Software Support website at: **https://softwaresupport.hpe.com**

This website provides contact information and details about the products, services, and support that HPE Software offers.

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches

- Manage support contracts
- Look up HPE 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 HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

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

HPE Software Integrations, Solutions and Best Practices

Access the Hewlett Packard Enterprise Software Support site (**https://softwaresupport.hpe.com/manuals**) to search for a wide variety of best practice documents and materials.

Contents

Chapter 1: APM - Service Manager Integration Overview

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

> **Note:** In general, the following document is for integrating BSM/APM 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 APM and Service Manager.** APM enables you to forward downtimes (also known as outages) from APM to Service Manager, and from Service Manager to APM. The downtime defined in APM is converted to a request for change in Service Manager, and vice versa. For details, see "Downtime Exchange Between APM and HPE Service Manager" on page 8.
- **Incident exchange between Service Manager and Operations Manager i.** APM 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 Service Manager and Operations Manager i.
- **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 HPE Universal CMDB" on page 18 and "View Changes and Incidents in Service Health Using RTSM" on page 31.
- **Submit an incident through APM alerts.** Incidents are automatically opened incidents in Service Manager when a CI Status alert is triggered in APM. For details, see "Generate Incidents in Service Manager When a APM Alert is Triggered" on page 43.
- **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 APM, and Manage SLAs Based on Service Manager" on page 45.
- The **Business Impact Report** integration is described in the *Closed Loop Incident Process (CLIP)* Guide. When deployed as part of the APM 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: https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01663679.

> **Note:**
> - **Service Manager Query Security.** If you have set up an integration from APM to Service Manager,

there is a CI context menu that enables you to access Service Manager from APM Service Health. This drill-down option is not available if you have enabled Service Manager query security.

- **Troubleshooting Multiple Domains.** If APM 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 2: Downtime Exchange Between APM and HPE Service Manager

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

This section includes the following:

- "Integration Overview" below
- "Prerequisites" on the next page
- "Step 1: Send APM Downtime Events to Service Manager" on page 10
- "Step 2: Integrate Service Manager Downtimes With APM" on page 12

Integration Overview

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

- **Service Manager > APM.** 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 APM.

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

- **APM > Service Manager.** When you define downtimes using APM (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 APM trigger events, which create corresponding incidents in Service Manager.

  In this scenario, when a downtime starts, APM 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 APM > 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 9.05 CUP 5 and higher with content pack 11 update 2, uCMDB 10.01 with content pack 12, uCMDB 10.20 with CUP1, or uCMDB 10.22 CUP 22.
- Before deploying the adapter verify that CP11 is installed. If CP11 is not installed, install the content pack. (This should be done whether you have upgraded to BSM 9.22 or above, or if you installed a version of BSM that is greater than or equal to 9.22.)

  > **Note:** To see what version of RTSM is installed, access the RTSM JMX console: **http://<APM server>:21212/jmx-console/**. Click on **DAL services** and run **getCmdbVersion** to get the RTSM version. Click **Content Pack Services** and run **displayCurrentContentPackVersion** to get the content pack version.

- 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.
- If you have upgraded from BSM 9.1x, you need to manually redeploy the adapter. Open the Package Manager and delete the **BSMDowntimeAdapter** package. When it is deleted, redeploy the above package from the packages folder.

Installing the Content Pack for uCMDB 9.05

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

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

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

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

   The main APM folder in Linux is located in: /opt/HP/BSM.

2. Access the following location with your browser:

   ```
   http://<APM DPS or uCMDB 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://<APM hostname>:21212/jmx-console/HtmlAdaptor?action=
   inspectMBean&name=UCMDB:service=Multiple CMDB Instances Services
   ```

2. In the method **setAsGlobalIdGenerator()**, assign the value **1** to the parameter **customerID**, and click **Invoke**.

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

1. Access the following location with your browser: :

   ```
   http://<uCMDB hostname>:8080/jmx-console/HtmlAdaptor?action=
   inspectMBean&name=UCMDB:service=MultipleCMDB Instances Services.
   ```

2. In the method **setAsGlobalIdGenerator()**, assign the value **1** to the parameter **customerID**, and click **Invoke**.

Step 1: Send APM Downtime Events to Service Manager

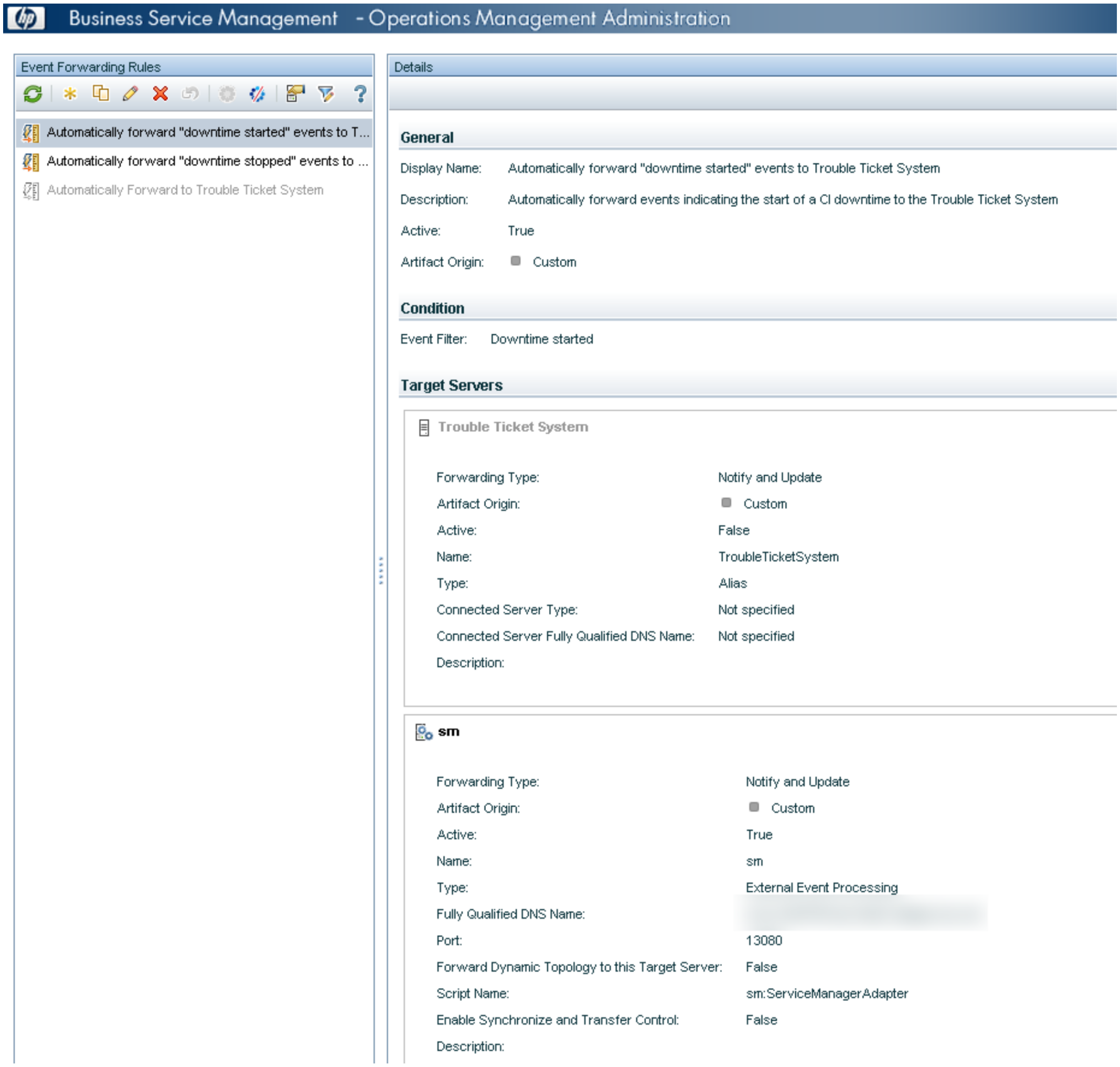
To enable APM to send downtime definitions to Service Manager, you must edit an infrastructure setting as described below. This procedure generates events in OMi; you can then use the event forwarding mechanism to generate incidents in Service Manager when a downtime in APM begins and ends.

> **Note:** These steps are related only to an internal RTSM under APM and not for an external UCMDB.

1. Access the following location in APM: **Infrastructure Settings > Foundations > Downtime**.
2. Change the value of the parameter **Downtime Send Event** to **true**.
3. Integrate OMi with APM (see Part II: Operations Manager i - Application Performance Manager Integration of the OMi Integrations Guide (https://softwaresupport.hpe.com/km/KM02256128/OMi_10.11_Integration_guide.pdf)).

A corresponding forwarding rule that configures forwarding downtime start and end events from APM 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”


Business Service Management - Operations Management Administration
Event Forwarding Rules
Details

Automatically forward "downtime started" events to T...
Automatically forward "downtime stopped" events to ...
Automatically Forward to Trouble Ticket System

General

Display Name: Automatically forward "downtime started" events to Trouble Ticket System
Description: Automatically forward events indicating the start of a CI downtime to the Trouble Ticket System
Active: True
Artifact Origin: Custom

Condition

Event Filter: Downtime started

Target Servers

Trouble Ticket System

Forwarding Type:	Notify and Update
Artifact Origin:	Custom
Active:	False
Name:	TroubleTicketSystem
Type:	Alias
Connected Server Type:	Not specified
Connected Server Fully Qualified DNS Name:	Not specified
Description:	

sm

Forwarding Type:	Notify and Update
Artifact Origin:	Custom
Active:	True
Name:	sm
Type:	External Event Processing
Fully Qualified DNS Name:	[redacted]
Port:	13080
Forward Dynamic Topology to this Target Server:	False
Script Name:	sm:ServiceManagerAdapter
Enable Synchronize and Transfer Control:	False
Description:	

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

Downtime events use the following formats:

- **Downtime Start**

Event field	APM Downtime
Severity	Normal
Category	Downtime Notification
Title	Downtime for <CI Type><Affected CI Name>started at <Downtime Start Time>
Key	<APM Downtime ID>:<Affected CI ID>:downtime-start

Event field	APM Downtime
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**

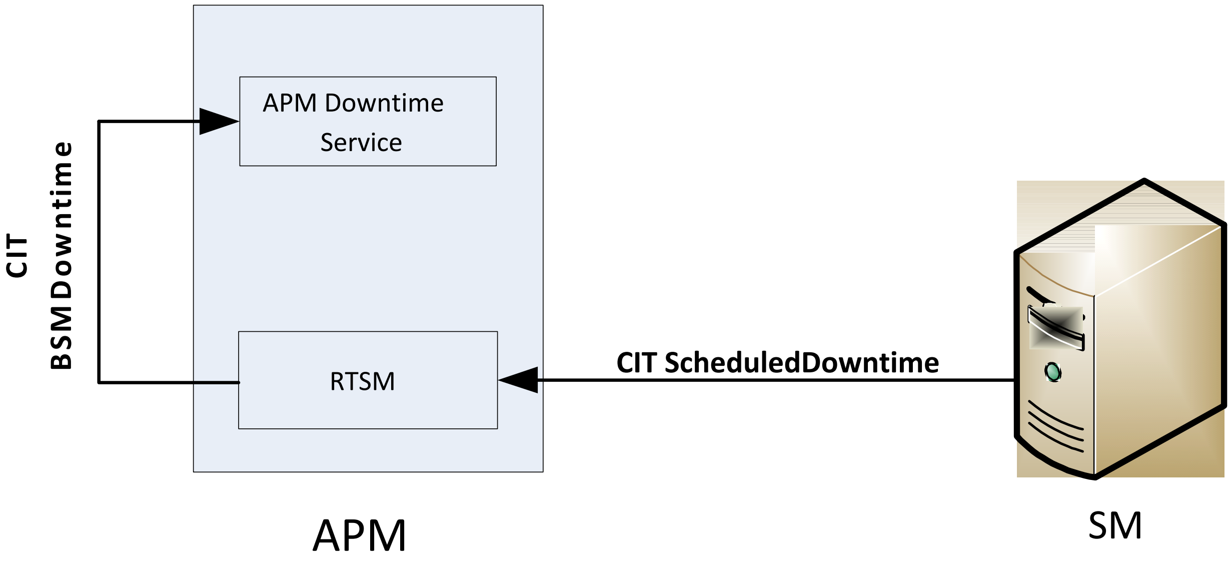
Event field	APM Downtime
Severity	Normal
Category	Downtime Notification
Title	Downtime for <CI Type><Affected CI Name> ended at < Downtime End Time>
Key	<APM Downtime ID>:<Affected CI ID>:downtime-stop
SubmitCloseKey	true
CloseKeyPattern	<APM Downtime ID>:<Affected CI ID>:downtime-start
EtiHint	downtime:end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

Step 2: Integrate Service Manager Downtimes With APM

Integrating Service Manager downtimes with APM consists of:

- Creating an instance of the **ScheduledDowntime** CIT in RTSM/uCMDB
- Creating an instance of the **BSMDowntime** CIT in APM

The following image shows the data flow when using RTSM:



Important:

- Following the initial integration, a large amount of data may be communicated from Service Manager to APM. We recommend that you perform this procedure during off-hours, to prevent negative impact on system performance.
- 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 > uCMDB/RTSM part, and then wait a long time before setting up the uCMDB/RTSM > APM adapter part, the number of downtimes communicated to APM initially may be extremely high.

Configuring HPE Service Manager to Send Downtimes

Note:

- The following provides the basic steps for HPE Service Manager configuration. For details, see the HPE Service Manager documentation.
- SMBSM_DOWNTIME is available in HPE Service Manager 9.32 and above.
- This document provides a basic description of how to configure SMBSM_DOWNTIME integration. For details, see the HPE Service Manager documentation.

1. Log in to HPE Service Manager as **System.Admin**.
2. Click **Tailoring > Integration Manager > Add** to add the Service Manager Integration Suite (SMIS) configuration for SMBSM_DOWNTIME. The Integration Template Selection page appears.
3. From the Integration Template drop-down list, select **SMBSM_DOWNTIME**, and click **Next**. The Integration Instance Information page appears.
4. In the **Interval Time(s)** field, type the running frequency data. Set this value based on your configuration item (CI) scheduled downtime data volume for the period.
5. In the **Max Retry Times** field, type the maximum number of retries. Since you are not connecting to another system, type **0**.

6. In the **Log File Directory** field, type the full path for the log file. By default, the log name is **sm.log**.
7. Click **Next**. The Integration Instance Parameters page appears.
8. Click the **General Parameters** tab.
9. Configure the SMIS settings.
   a. Assign a value for **WithdrawDowntime** (options are **true** or **false**). **True** means that when you make a change using **Change Phase**, if the change has a valid outage, a prompt appears enabling you to reject the outage.
   b. In the **Category** column, assign the value **Change** for change categories and **Task** for task categories.
   c. Assign values for the parameters in the **Change** category.

      If you only want outages of one change category after your desired phase has been approved, in the **Value** column, set the phase.

      If your category workflow has multiple paths with different final approval phases, use a semicolon (**;**) to separate the phases.
   d. Assign a unique identifier for your Service Manager deployment to the **sm.host** parameter. This identifier represents your Service Manager server.

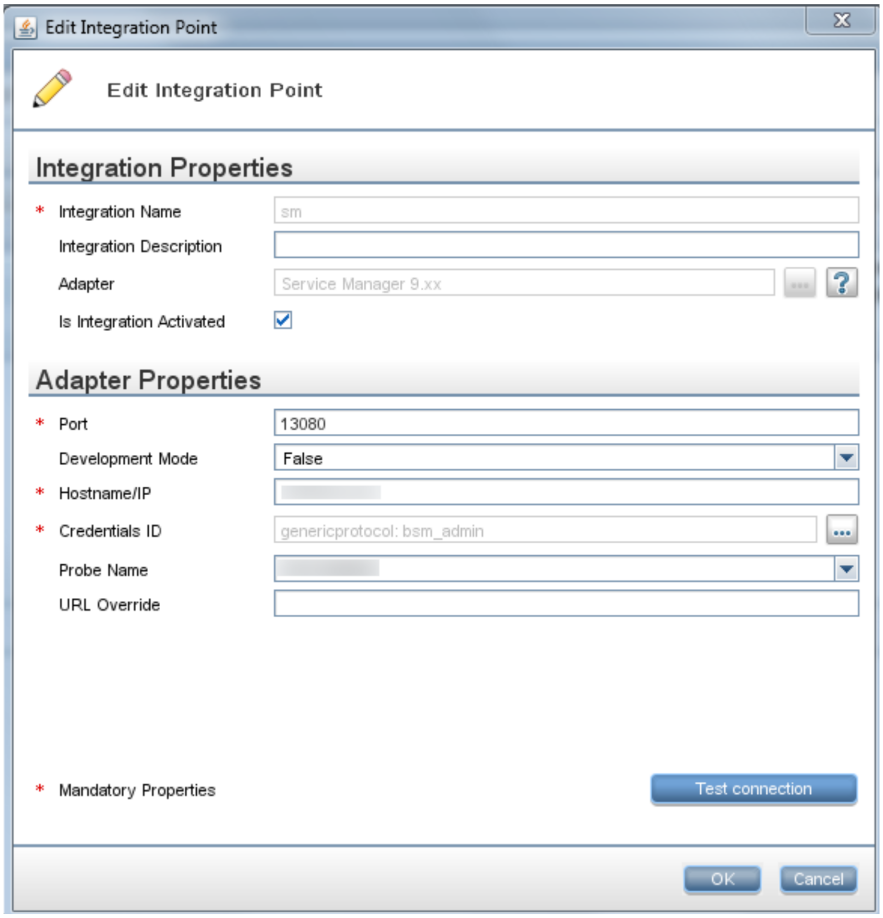
      Do not use a colon (:) in this field.
   e. Assign a value to the **sm.reference.prefix** parameter. This value is used to populate the External Process Reference of Scheduled Downtime CI in UCMDB.

      Service Manager automatically appends a colon (:) at the end of the value.
   f. Click **Next**, **Next**, **Finish**.
   g. Select the **SMIS**.
   h. Click **Enable**.
   i. Click **Yes**.

Integrating SM RFC Downtimes with RTSM/uCMDB

To integrate SM RFC downtimes with RTSM/uCMDB, populate (synchronize) RTSM/uCMDB with the downtime CIs.

1. Log in to RTSM/uCMDB.
   - In APM, access **Admin > RTSM Administration > Data Flow Management > Integration Studio**
   - In uCMDB, access **Administration > Data Flow Management > Integration Studio**
2. Verify that the integration point in front of the Service Manager exists and is active.



Edit Integration Point

Edit Integration Point

Integration Properties

- * Integration Name: sm
- Integration Description:
- Adapter: Service Manager 9.xx
- Is Integration Activated: ☑

Adapter Properties

- * Port: 13080
- Development Mode: False
- * Hostname/IP: [redacted]
- * Credentials ID: genericprotocol: bsm_admin
- Probe Name: [redacted]
- URL Override:

* Mandatory Properties

3. Click **Test connection** and verify that the connection succeeds.
4. In the **Population** tab, add the following integration jobs:
   - **DT Population** based on **CLIP Down Time Population** TQL
   - **DT Relationship** based on **CI To Down Time CI With Connection** TQL
5. Log in to the Service Manager server. Select the **Configuration Management** tab and select **Resources > Configuration Item Relationships**.
6. Add a relation between the **Upstream CI** (for example, any business service instance) and the **Downstream CI** (the affected CI), and click **Add**.
7. In the **Change Management** tab, select **Changes > Open New Change** to open a new request for change (RfC). Verify the **Service**, **Affected CI**, and **Scheduled DownTime Start/End** field are completed.

   > **Note:** The **Service** and **Affected CI** values should be equal to the **Upstream/Downstream CI** values you set in the previous step.

8. Click **More > Change Phase**. Move the **RfC** phase to the **Change Approval** phase.
9. Log in to Service Manager as user **Change.Approver**. Open the **Approval In** box and approve the change.
10. Wait for **SMBSM_DOWNTIME/DT Population/DT Relationship** to run. By default, it runs every minute.

11. Log in to RTSM/uCMDB.
    - In APM, access **Admin > RTSM Administration > Data Flow Management > Modeling Studio**
    - In uCMDB, access **Administration > Data Flow Management > Modeling Studio**
12. In Modeling Studio, search for **ScheduledDowntime CI**. A downtime CI is created with a relationship to the affected CI.

Push CIT ScheduledDowntime to CIT BSMDowntime by BSMDowntimeAdapter

1. If you are using uCMDB, deploy the adapter as follows:
   a. In uCMDB, access **Administration > Package Manager**.

      In APM, access **Admin > RTSM Administration > Administration > Package Manager**.
   b. Click **Deploy package to server**, and import the adapter's zip file from `<APM DPS installation path>\odb\conf\factory_packages\BSMDowntimeAdapter.zip`.
2. Create the integration point credentials:
   a. In uCMDB, access **Data Flow Management > Data Flow Probe Setup**.

      In APM, access **Admin > RTSM Administration > Data Flow Management > Data Flow Probe Setup**

      > **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 plus sign (Add new connection details) and enter the APM Gateway host name, Port 80, and the APM 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. In uCMDB, access **Data Flow Management > Integration Studio**.

      In APM, access **Admin > RTSM Administration > Data Flow Management > Integration Studio**.
   b. Click **New integration point**, enter a name and description of your choice, and select:
      - In APM: **BSMDowntimeAdapter**
      - In uCMDB: **SM scheduled Downtime Integration into APM**
   c. Enter the following information for the adapter:
      - APM Gateway hostname and port
      - Communication protocol
      - The integration point credentials you just created
      - 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. Click 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 failed, you can click the **Query Status** tab and double-click the failed job to view more details about the error.

Troubleshooting

- If there is an authentication error, verify that the APM credentials entered for the integration point are correct.
- An unclear error message with an error code generally indicates a communication problem. Check the communication with APM. If no communication problem is found, restart the MercuryAS process.

Note:

- A failed job is repeated until the problem is fixed.
- Each BSMDowntime can be found in APM Downtime Management (**Admin > Platform > Downtime Management**).

Chapter 3: View Changes and Incidents in Service Health Using Standalone HPE 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 HPE Universal CMDB.

This task describes how to configure the HPE Service Manager - APM 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:

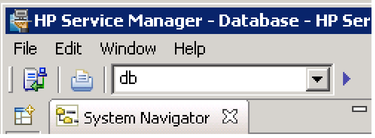
Prerequisites

- **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 APM 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 HPE Service Manager to use the SSL-based Trusted Sign-on protocol and LW-SSO, configure it according to the instructions in the HPE Service Manager online help if you have not already done so. In addition, see *Configuring HPE Service Manager to Use the SSL-based Trusted Sign-On and LW-SSO* in the Service Manager documentation library.

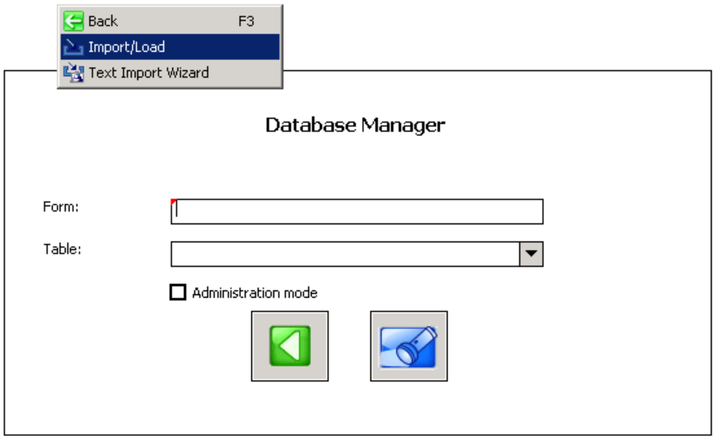
Step 1: Load .unl Files to Provide External Access to Service Manager

This procedure enables APM to query incidents and changes:

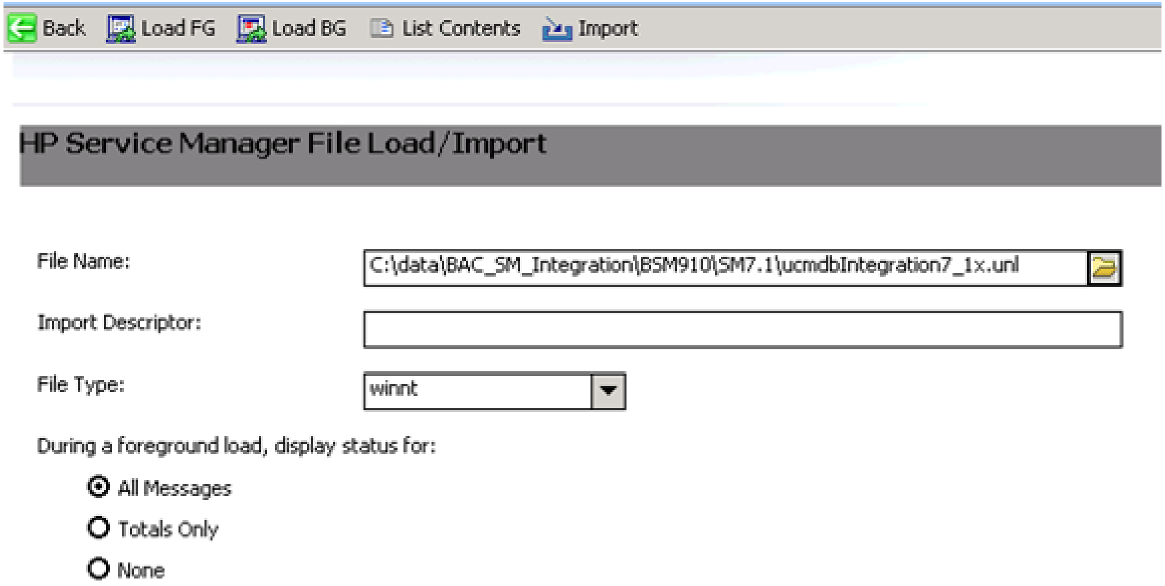
1. Copy the following files from the APM 9.x installation folder to a local directory:
   - SM_Integration/SM_Unloads/SM7.1/ucmdbIntegration7_1x.unl
   - SM_Integration/SM_Unloads/SM7.1/BACExtAccess_71_v1.unl
2. Before loading these .unl files, apply the fix described in https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM1015767. 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 APM. Select the file, and click **Open**.



File Name: C:\data\BAC_SM_Integration\BSM910\SM7.1\ucmdbIntegration7_1x.unl

Import Descriptor:

File Type: winnt

During a foreground load, display status for:

- ● All Messages
- ○ Totals Only
- ○ None

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:

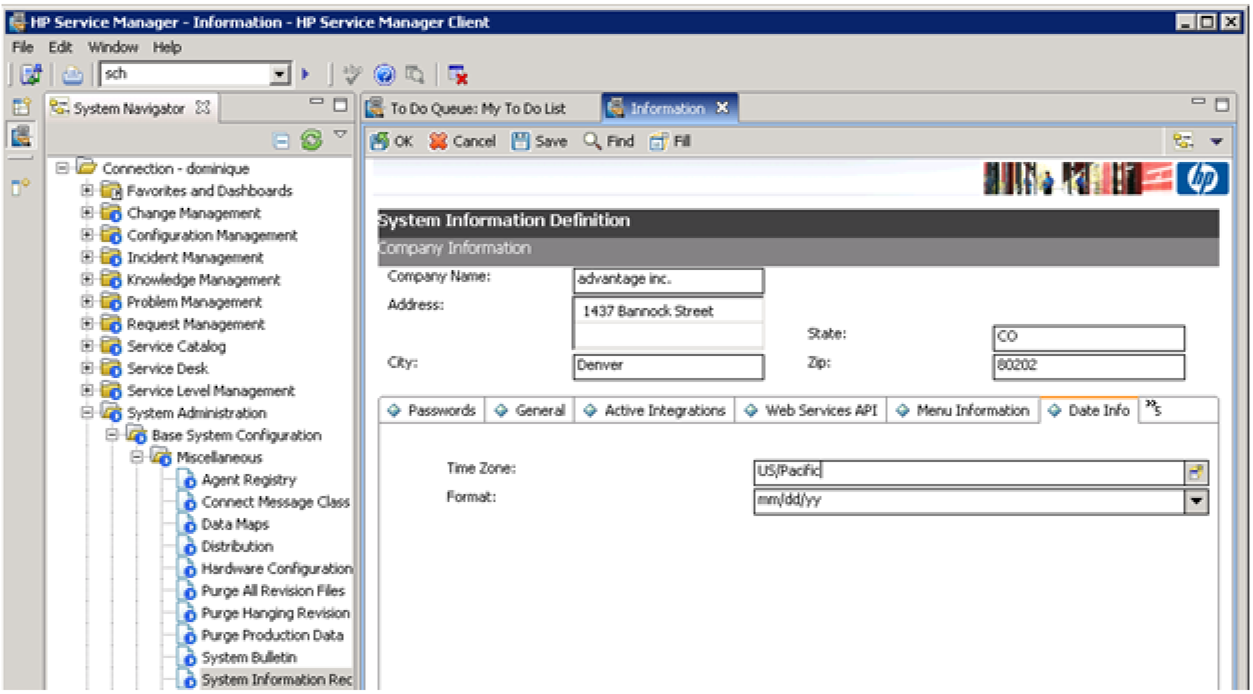
1. In Service Manager, select **Navigation pane > Menu navigation > System Administration > Base System Configuration > Miscellaneous > System Information Record**.

2. Within the **Date Info** tab, open the <APM 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.



System Information Definition

Company Information

Company Name: advantage inc.

Address: 1437 Bannock Street

City: Denver

State: CO

Zip: 80202

Time Zone: US/Pacific

Format: mm/dd/yy

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 APM, restart the APM server.)

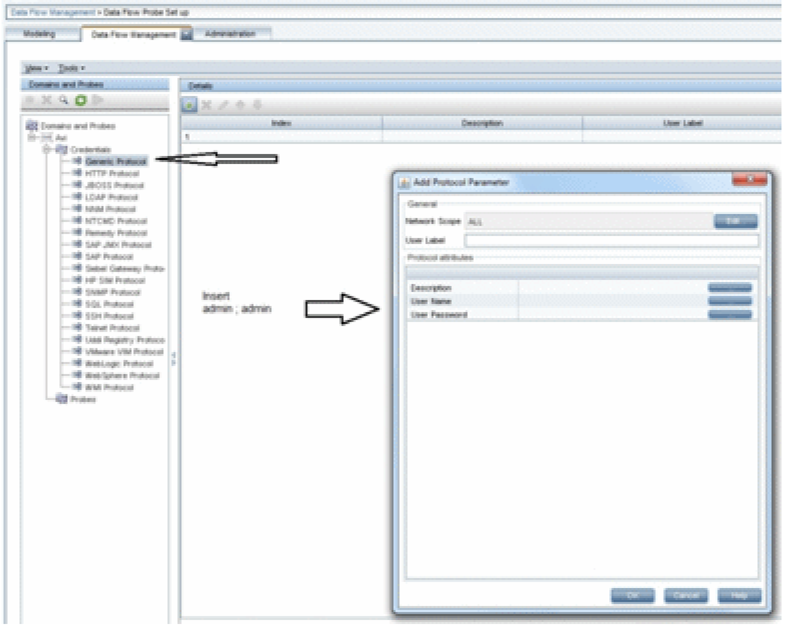
Step 3: Verify that the UCMDB is the Global ID Generator

1. Log in to the JMX Console (http://<UCMDB server>:8080/jmx-console/).
2. Go to **Multiple UCMDB Instances Services**.
3. Click **getIsGlobalIdGenerator**. Verify that the call returns **true**. For more details, refer to the RTSM Best Practices guide.

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 the next page.

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

1. In APM, 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.



Insert
admin ; admin

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**.

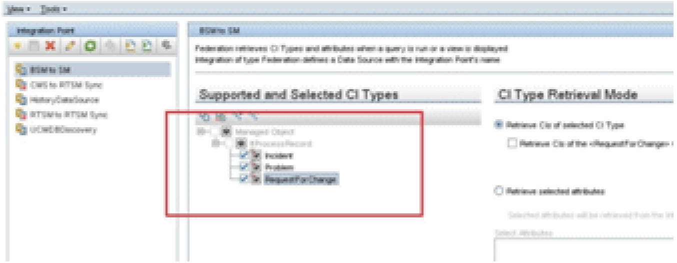
Step 6: Configure the SM-UCMDB Integration: Create an Integration Point

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 the 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 19).

> **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 APM-UCMDB Integration: Deploy CMS_to_RTSM_Sync.zip on UCMDB

1. Copy the file CMS_to_RTSM_Sync.zip located on the APM-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 APM-UCMDB Integration: Create an Integration Point on APM

1. Within the APM 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.

Name	Recommended Value	Description
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 *APM* (see "Prerequisites" on page 19).

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 APM, 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 APM-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 APM server, load balancer, or reverse proxy.
Port	**<user defined>**	The port through which you access APM, load balancer, or reverse proxy.

	Recommended	
Name	**Value**	**Description**
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 19).

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, APM 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 40.

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 APM, 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 APM CI that corresponds to the **Siebel Application** CIT in APM.
- 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.

Troubleshooting

If you are not seeing expected incidents in APM, perform the following:

1. On the Data Processing Server, search the **odb\odb\Error.log** file for **Error Code 802**.
2. In this error message, locate the following string: **property [<*category or incident_status*>=<*attribute value*>[STRING]] is defined as attribute**.

   This indicates that a certain attribute value is missing in RTSM.
3. Access **RTSM Administration > CI Type Manager**.
4. From the **CI Types** menu, select **System Type Manager**, and open **Category** or **Incident Status** (depending on the error message) for editing.
5. Click the Add button (+), and add the missing attribute value (exactly as it appears in the error message) to the list of values.

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 *APM User Guide*.

This section includes the following:

- "Prerequisite" below
- "Step 1: Configure the Service Desk Adapter Time Zone" below
- "Step 2: Create an Integration User Account in Service Manager" on the next page
- "Step 3: Add the APM Connection Information in Service Manager" on page 33
- "Step 4: Create an Integration Point in APM" on page 34
- "Step 5: Create New Jobs to Synchronize Between APM and Service Manager" on page 36
- "Step 6: Run the Job" on page 36
- "Step 7: Test the Configuration" on page 36
- "Step 8 (Optional): Add CI Types to the Service Health Changes and Incidents Component" on page 38
- "Troubleshooting" on page 39

Prerequisite

If you are using SM versions 9.30 or 9.31, before you begin you must install a data-flow probe with the APM 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

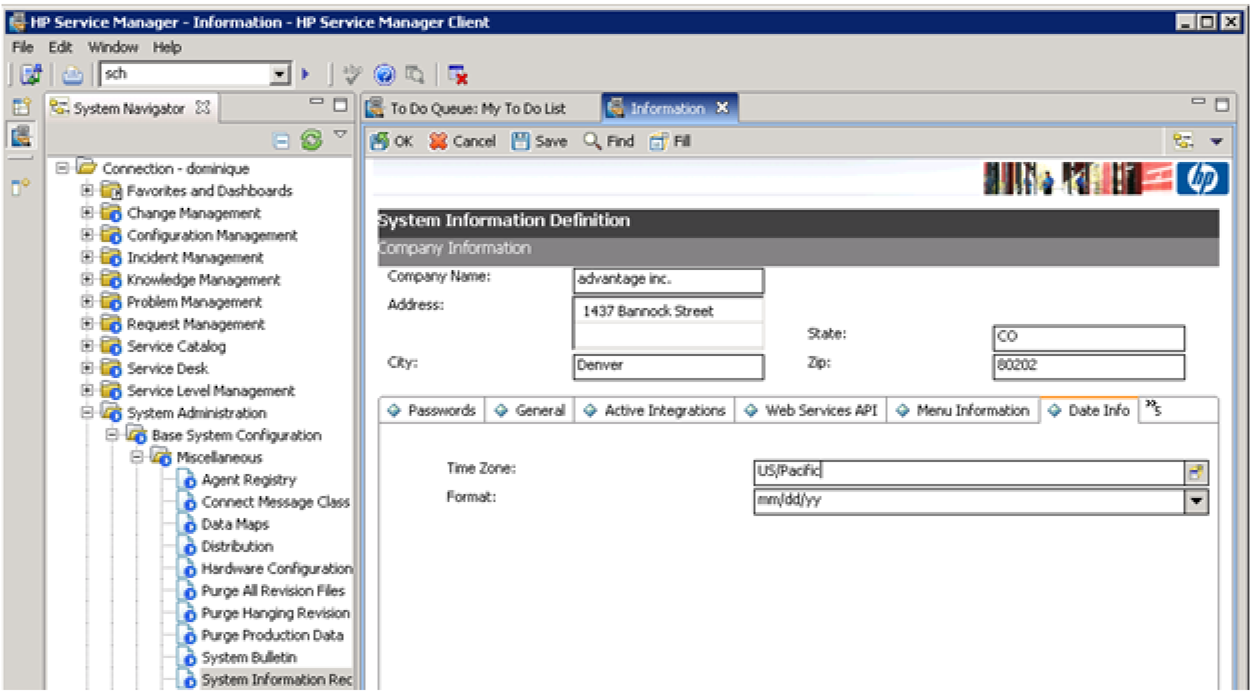
Configure the time zone so Incidents and Planned Changes have the correct time definitions:

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 <APM 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.



System Information Definition

Company Information

Company Name: advantage inc.

Address: 1437 Bannock Street

City: Denver

State: CO

Zip: 80202

Time Zone: US/Pacific

Format: mm/dd/yy

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 APM, restart the APM server.)

Step 2: Create an Integration User Account in Service Manager

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

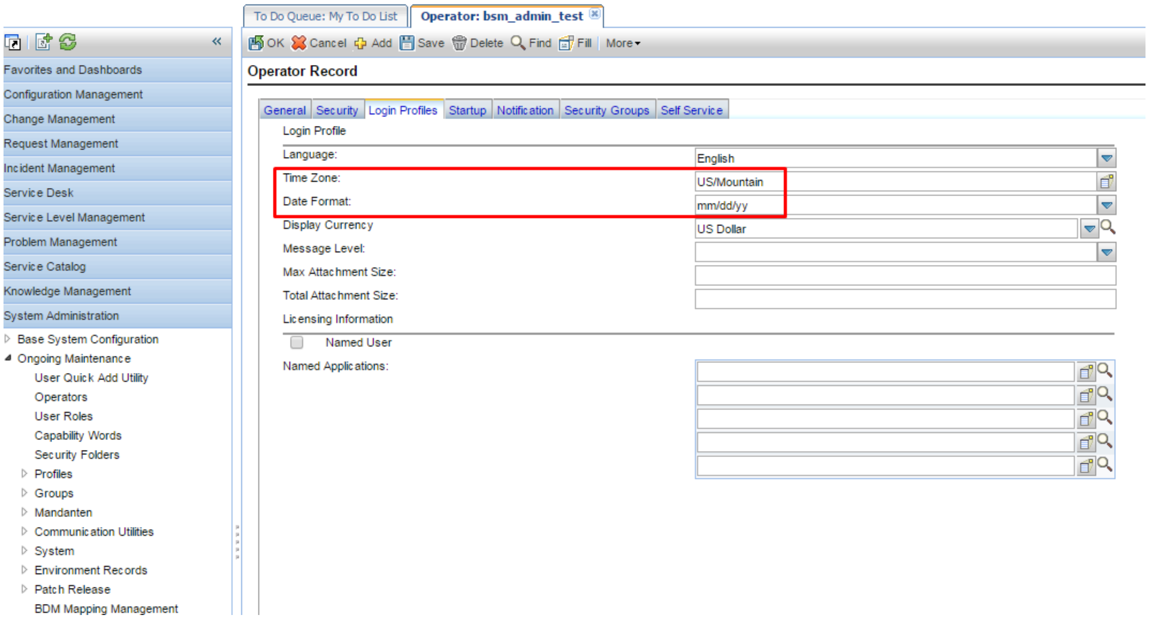
To create a dedicated integration user account in Service Manager:

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 the **Login Profiles** tab, and review the information in the **Time Zone** and **Date Format** sections. If necessary, update this information according to the Service Desk Adapter Time Zone configuration you performed in "Step 1: Configure the Service Desk Adapter Time Zone" on page 31.

      > **Note:** A Time Zone or Data Format mismatch could cause limited functionality in the integration.



Operator Record

Login Profile

Language: English

Time Zone: US/Mountain

Date Format: mm/dd/yy

Display Currency: US Dollar

Message Level:

Max Attachment Size:

Total Attachment Size:

Licensing Information

□ Named User

Named Applications:

   g. 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 APM Connection Information in Service Manager

The integration requires the APM connection information to obtain CI attribute information from the APM 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 HPE 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 APM server, and replace <port> with the communications port your APM server uses.
6. In **UserId** and **Password**, type the user credentials required to manage CIs on the APM 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 APM.

Step 4: Create an Integration Point in APM

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:

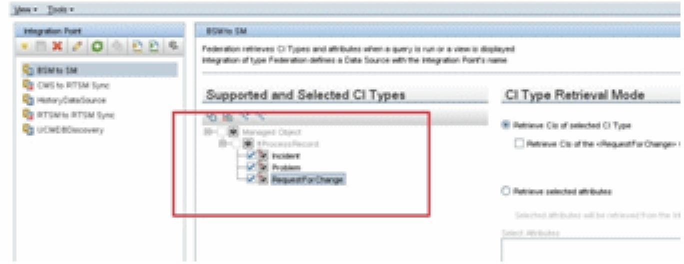
1. Access the JMX console (in case of distributed deployment) on the DPS server.
2. Navigate to **UCMDB:service=Security Services**.
3. Create a new user with the name and password that you created in SM, using the JMX **createUser**:
   - **CustomerId** = 1
   - **userName** = <userName>
   - **password** = <password>
4. Assign the user Administrator Role using the JMX **setRolesForUser** from the same section:
   - **CustomerId** = 1
   - **userName** = <userName>
   - **roles** = Admin
5. In APM, 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.
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 32, and then select it. This account must exist in both Service Manager and APM.
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.



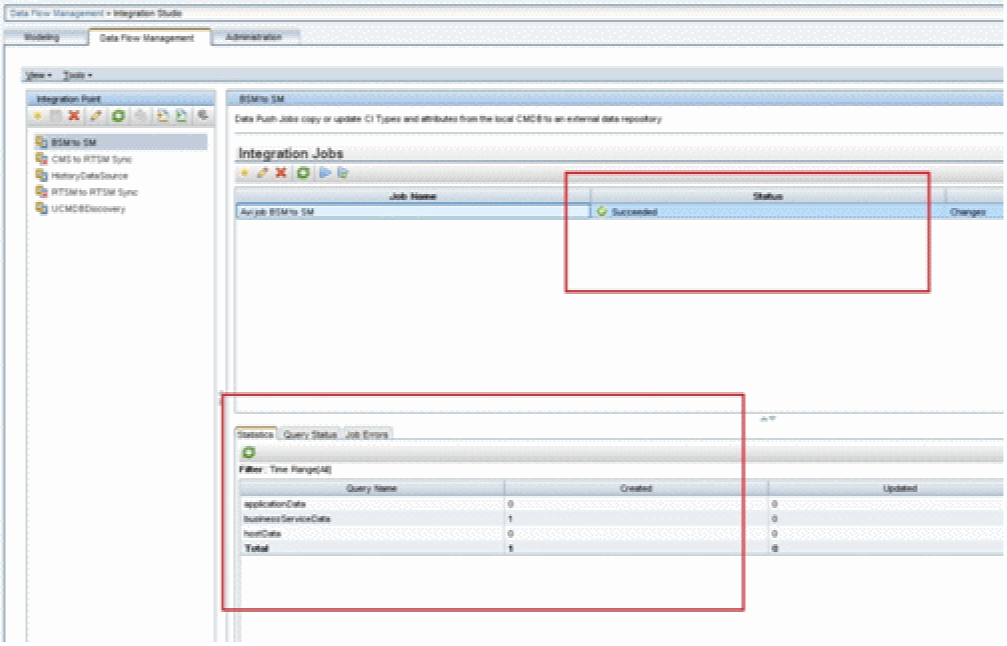
Federation retrieves CI Types and attributes when a query is run or a view is displayed
Integration of type Federation defines a Data Source with the integration Point's name

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



Data Push Jobs copy or update CI Types and attributes from the local CMDB to an external data repository

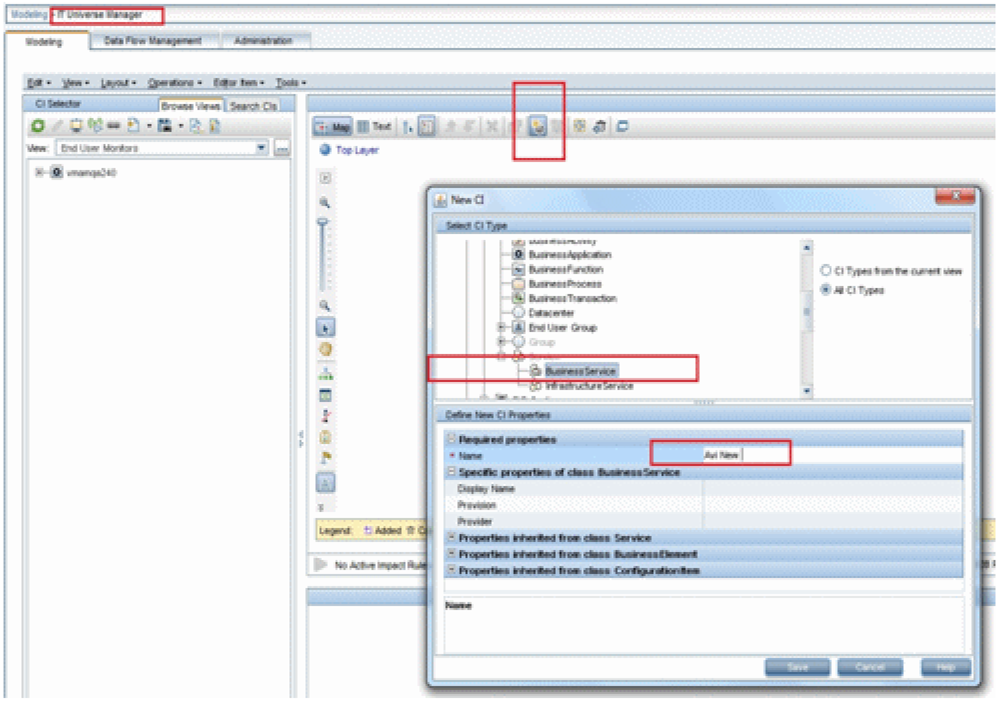
Job Name	Status	
Avi job BSM to SM	Succeeded	Changes

Filter: Time Range[All]

Query Name	Created	Updated
applicationData	0	0
businessServiceData	1	0
hostData	0	0
Total	1	0

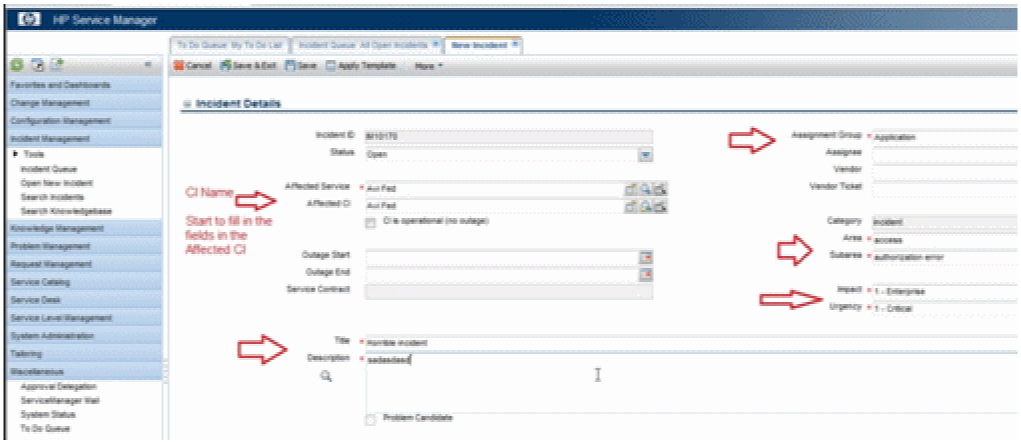
Step 7: Test the Configuration

1. In APM, 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.



* Name	Avi New

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.

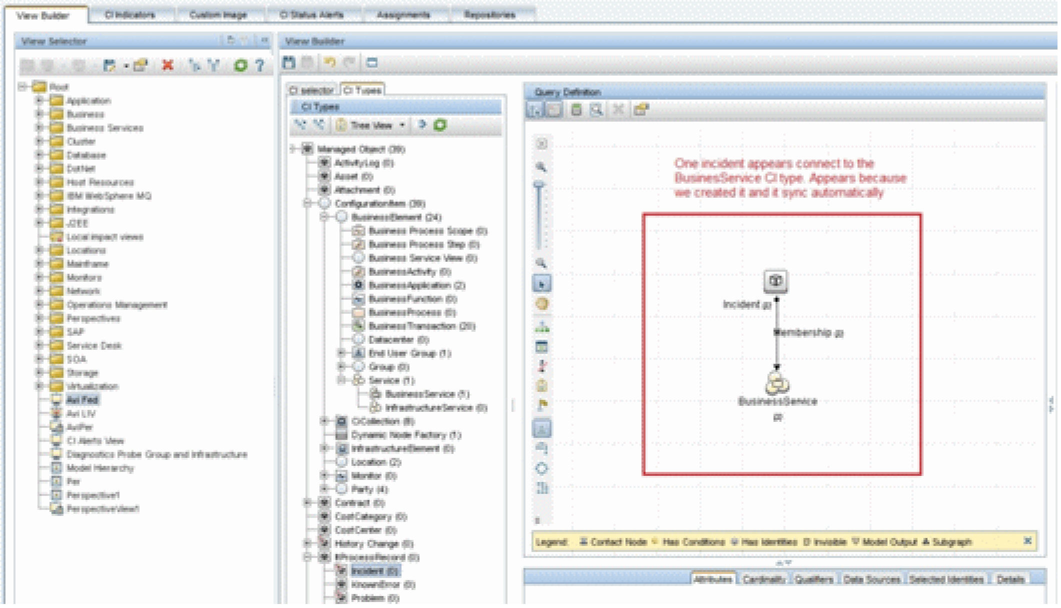


Incident ID	IM10170
Status	Open
Affected Service	Avi Fed
Affected CI	Avi Fed
Outage Start	
Outage End	
Service Contract	
Title	Horrible incident
Description	sadasdasd
Assignment Group	Application
Assignee	
Vendor	
Vendor Ticket	
Category	incident
Area	access
Subarea	authorization error
Impact	1 - Enterprise
Urgency	1 - Critical

The incident is automatically attached to the CI.

8. In APM, create a TQL with the CI Type you created connected to the Incident CI Type in a membership relationship link.

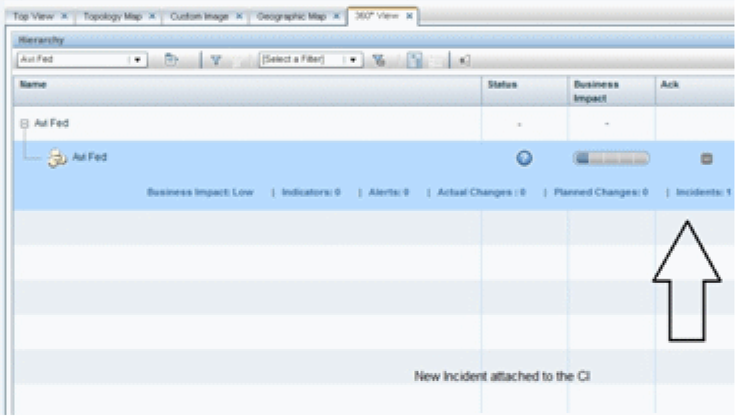
9. Click the **Calculate** ▣ button. One incident appears connected to the BusinessService CI Type because this test created it and it is synchronized automatically.



One incident appears connect to the BusinessService CI type. Appears because we created it and it sync 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.



Business Impact: Low | Indicators: 0 | Alerts: 0 | Actual Changes : 0 | Planned Changes: 0 | Incidents: 1

New Incident attached to the CI

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

By default, APM 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 40.

Troubleshooting

If you are not seeing expected incidents in APM, see "Troubleshooting" on page 30

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 the 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

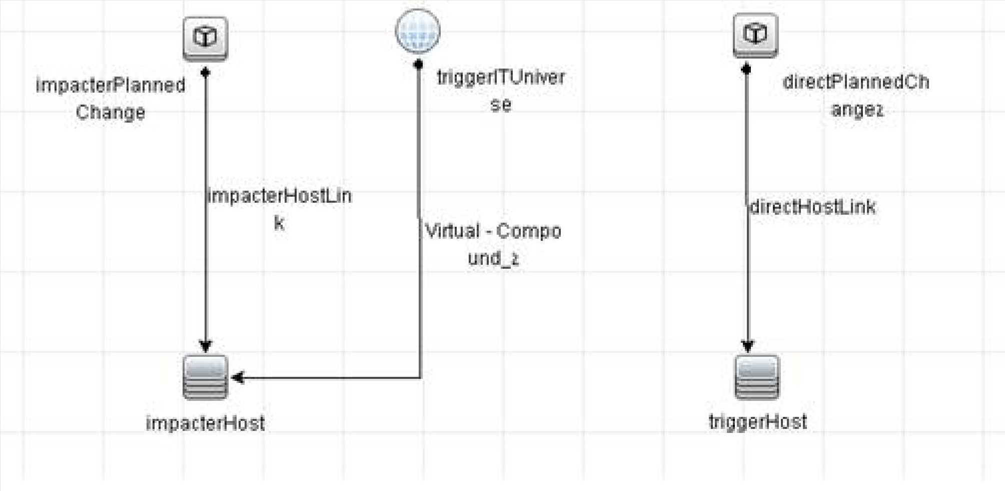
The following naming constraints should be followed in the request for change *without* impact TQL (see the TQL example below, on the right side of the image):

- 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

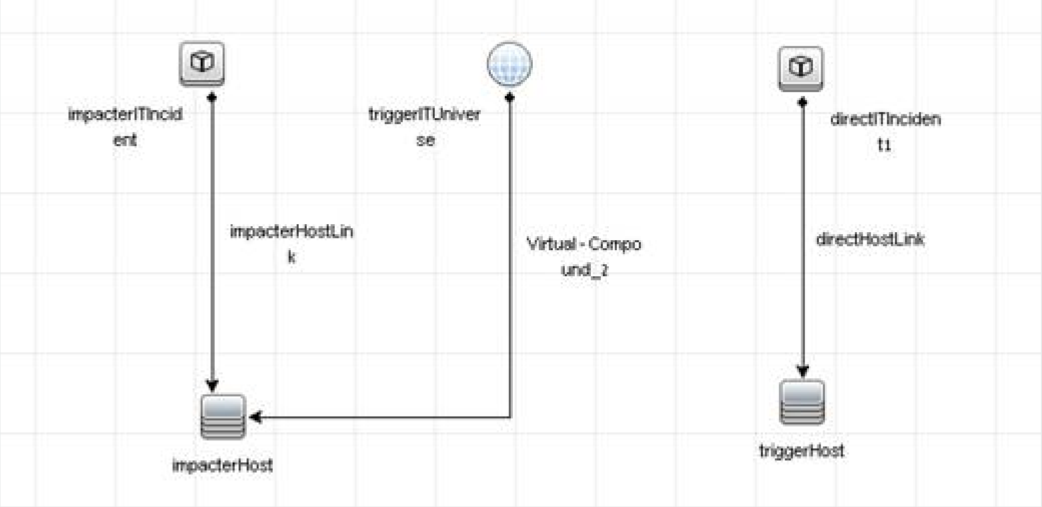
The following naming constraints should be followed in the incidents *without* impact TQL (see the TQL example below, on the right side of the image):

- 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 APM 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 HPE 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 HPE Service Manager to proactively alert the operator about a problem in the system.

To automatically forward an event when an alert is triggered,

1. Integrate OMi with APM (see Part II: Operations Manager i - Application Performance Manager Integration of the OMi Integrations Guide (https://softwaresupport.hpe.com/km/KM02256128/OMi_10.11_Integration_guide.pdf)).
2. Follow the steps described in this section.

This section includes the following:

- "CI Status Alerts" below
- "SLA Alerts" below
- "EUM Alerts" on the next page

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 *APM 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 *APM 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 *APM 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 *APM Application Administration Guide*.

Chapter 7: View Incident Data in APM, 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.

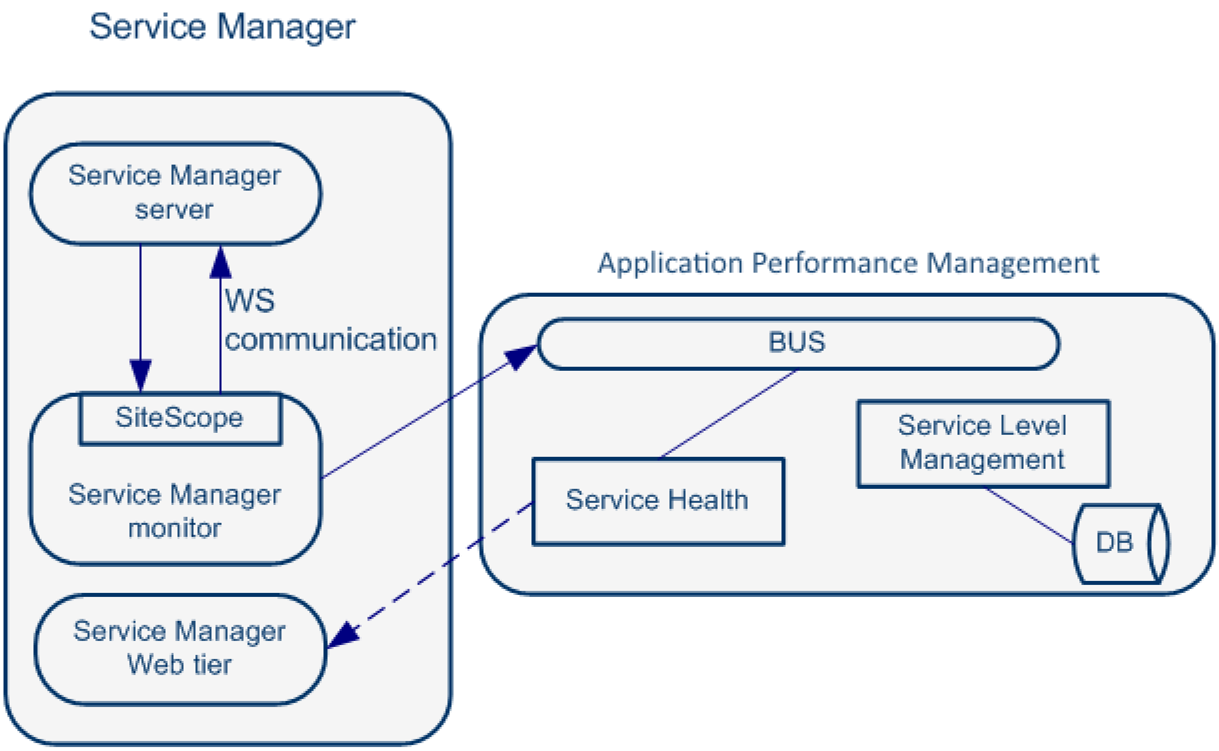
This section includes the following:

Overview: Understanding the Integration with EMS

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

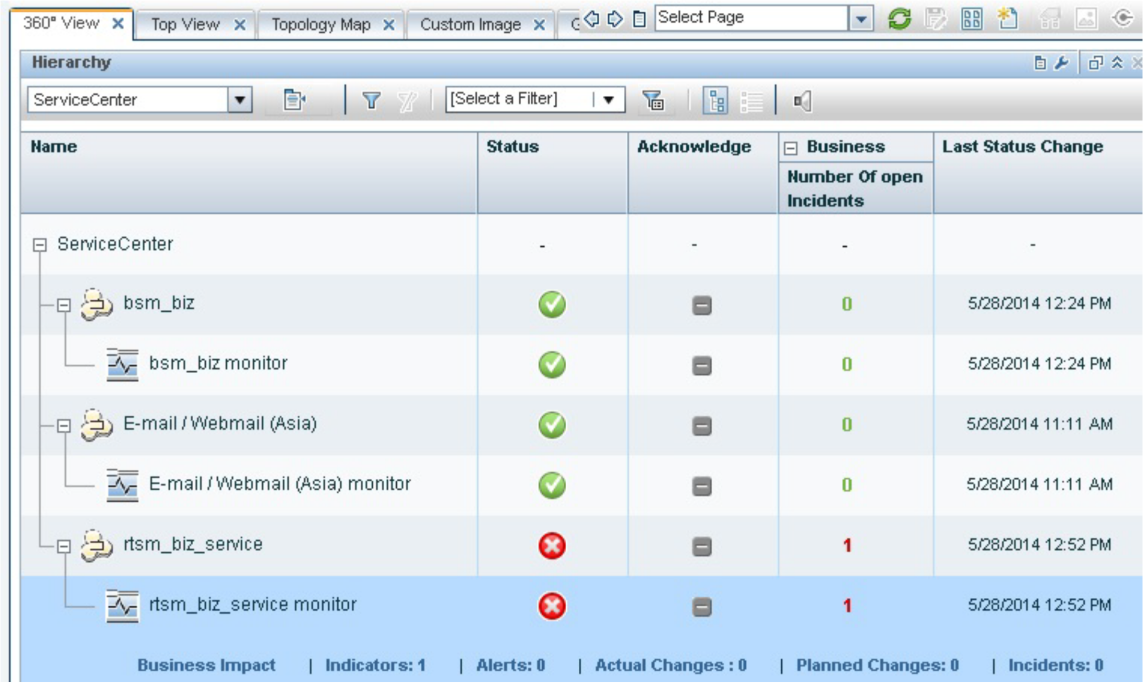
Architecture

The architecture of the integration of Service Health and Service Level Management with HPE 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 HPE Service Manager) at the business service level in the APM Service Health views and reports. For details about the views, see "View Topology" in the Service Health part of the *APM User Guide*. For example: the Operator/Application support can get visibility and alerts based on the Number of Open Incidents in APM Service Health alongside operational KPIs.
- **Drill down to HPE Service Manager from EMS monitor level CIs.** You can drill down from Service Health views at the EMS monitor level business service level to HPE 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 *APM User Guide*. For example: the support person can drill down to HPE 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.



Name	Status	Acknowledge	Business	Last Status Change
			Number Of open Incidents	
ServiceCenter	-	-	-	-
bsm_biz	✓	▬	0	5/28/2014 12:24 PM
bsm_biz monitor	✓	▬	0	5/28/2014 12:24 PM
E-mail / Webmail (Asia)	✓	▬	0	5/28/2014 11:11 AM
E-mail / Webmail (Asia) monitor	✓	▬	0	5/28/2014 11:11 AM
rtsm_biz_service	✗	▬	1	5/28/2014 12:52 PM
rtsm_biz_service monitor	✗	▬	1	5/28/2014 12:52 PM

Business Impact | Indicators: 1 | Alerts: 0 | Actual Changes : 0 | Planned Changes: 0 | Incidents: 0

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 *APM 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 HPE Service Manager. For details, see "Agreements" in the Service Level Management part of the *APM Application Administration Guide*.

For example: the HPE Service Manager manages SLAs with operational KPIs (Availability, Performance, or other KPIs) and serviceability KPIs (MTTR, MTBF, or MTBSI KPIs) using APM Service Level Management. The HPE 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 HPE Service Manager

The HPE Service Manager integration creates the following elements:

Element	Service Health	Service Level Management

CIs	EMS Monitor CIs for the monitored HPE Service Manager system, based on the samples sent by the SiteScope HPE 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 HPE 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 *APM 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 *APM Application Administration Guide*.
KPIs	Number of Open Incidents KPI. For details, see "List of Service Health KPIs" in the Service Health part of the *APM 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 *APM 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 APM by the EMS system. For details on the rule, see List of Calculation Rules in Service Health" in the Service Health part of the *APM Application Administration Guide*.	Each HPE Service Manager KPI (attached to an EMS Monitor CI) uses its own monitor rule. For details on the rules, see "List of Service Level Management Business Rule Parameters" in the Service Level Management part of the *APM Application Administration Guide*.

Context Menu	The HPE SC Menu. For details on the context menu, see "List of Context Menus" in the Service Health part of the *APM 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 *APM 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.

Prerequisites

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

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

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

> **Note:** Plan to put both the HPE 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 HPE Service Manager From Within Service Health

Disable the query security of the HPE Service Manager application to enable accessing the application, through the right-click HPE 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 HPE 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 HPE Service Manager home directory under the Apache home directory. The web.xml file can be located at:**\<J2EE webserver path>\webapps\<webtier>\WEB-INF**.
2. In the file, locate the **<!-- Specify the Service Manager server host and port location -->** section. This section should appear after the **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 HPE 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 HPE 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 HPE Service Manager, manually within HPE Service Manager if the tables are used for other external internal integrations. For details, refer to the HPE Service Manager documentation.
- Using the configuration file supplied with HPE 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 in the electronic download package, and copy it to a local directory.
  b. Open the HPE Service Manager client and connect to the server.
  c. Select **Tailoring > 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 HPE Service Manager so that the values are the same as in the below table (for details on how to do that, see HPE 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 HPE Service Manager client, select **Tailoring > Web Services > Web Service Configuration**, enter **Clocks** in the **Service Name** field, and click **Search**.
2. Click the **Fields** 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 HPE 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 HPE Service Manager version is populating these fields and the integration works even after you upgrade to HPE 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 HPE Service Manager Monitor accessed in APM by clicking **Admin > Integrations > EMS Integration Admin**. Only incidents that were opened after this step are displayed in APM Service Health.

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

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

1. Select **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 **More** 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 HPE Service Manager User

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

1. Create a dedicated user in HPE Service Manager. The user should be used solely for the purposes of the HPE Business Service Management/SiteScope integration.
2. Make sure that the HPE Service Manager machine and the SiteScope machine share the same time zone.
3. Make sure that the HPE 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 HPE Service Manager.

Step 6: Configure the HPE Service Manager Monitor in SiteScope

Configure the HPE Service Manager monitor in SiteScope as follows:

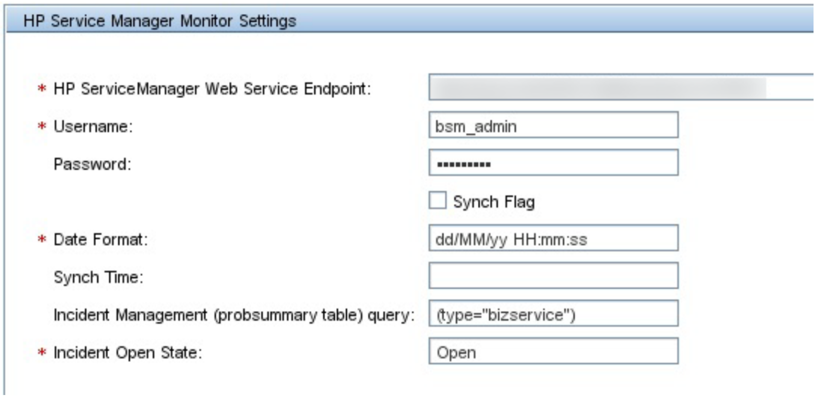
1. Synchronize HPE Service Manager and SiteScope so their time zones are the same. Match their System Time in the Windows or Unix operating system.
2. Make sure that the user you are using in SiteScope is the user you defined in "Step 5: Create a Corresponding HPE Service Manager User" above.
3. Make 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 HPE 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 HPE Service Manager monitor using the following fields:

   - **Web Service**: <protocol>://<SMhost>:<SMport>/sc62server/PWS/
   - **user name**: <user name defined in "Step 5: Create a Corresponding HPE Service Manager User" on the previous page>
   - **user pass**: <password of user created in "Step 5: Create a Corresponding HPE Service Manager User" on the 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**.



HP Service Manager Monitor Settings

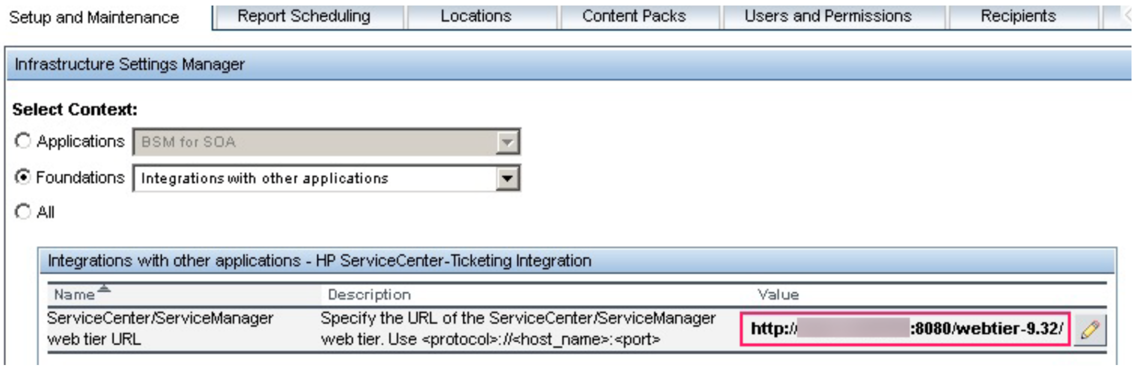
* HP ServiceManager Web Service Endpoint:
* Username: bsm_admin
Password: *********
□ Synch Flag
* Date Format: dd/MM/yy HH:mm:ss
Synch Time:
Incident Management (probsummary table) query: (type="bizservice")
* Incident Open State: Open

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

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

1. To specify the HPE Service Manager URL, in APM, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, select **Foundations**, and select **Integrations with other applications**.
2. In the Integrations with other applications - HPE 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 HPE Service Manager server, **port** is the port number of the HPE Service Manager server, and **web_app_name** is the name of the application.

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



Infrastructure Settings Manager

Select Context:

○ Applications BSM for SOA

● Foundations Integrations with other applications

○ All

Integrations with other applications - HP ServiceCenter-Ticketing Integration

Name	Description	Value
ServiceCenter/ServiceManager web tier URL	Specify the URL of the ServiceCenter/ServiceManager web tier. Use <protocol>://<host_name>:<port>	**http://[redacted]:8080/webtier-9.32/**

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

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

1. **Configure the HPE Service Manager Monitor – Optional.** The monitor is used to retrieve data from the EMS system using System Availability Management Administration. The HPE 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 HPE Business Service Management is established. For details, go to "How to Work with the HPE 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 HPE Service Manager integration. The integration forwards the retrieved data captured from the HPE Service Manager system by the SiteScope HPE Service Manager monitor to APM, 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 *APM 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 APM, 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 APM, 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 *APM Application Administration Guide*.

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

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

You can include HPE Service Manager EMS Monitor CIs in your agreements in Service Level Management. Service Level Management contains KPIs and rules specifically configured for HPE 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 *APM Application Administration Guide*, and locate "Incident State and Severity Values".

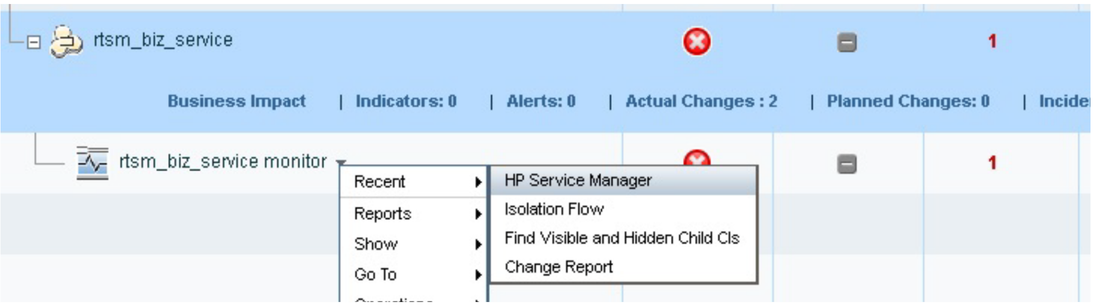
Results

After the task is performed, HPE Service Manager data is integrated into APM. You can:

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

  SiteScope automatically creates the appropriate topology when HPE Service Manager data is integrated into APM. HPE 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 HPE Service Manager from Service Health views:**

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


rtsm_biz_service
1
Business Impact | Indicators: 0 | Alerts: 0 | Actual Changes : 2 | Planned Changes: 0 | Incide
rtsm_biz_service monitor
1
Recent
Reports
Show
Go To
HP Service Manager
Isolation Flow
Find Visible and Hidden Child CIs
Change Report

Send Documentation Feedback

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

Feedback on APM - Service Manager Integration Guide (Application Performance Management 9.30)

Just add your feedback to the email and click send.

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

We appreciate your feedback!