HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.52

HP Business Availability Center - HP Service Manager/ HP ServiceCenter Integration Guide

Document Release Date: January 2009
Software Release Date: January 2009

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.

Third-Party Web Sites

HP provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. HP makes no representations or warranties whatsoever as to site content or availability.

Copyright Notices

Trademark Notices

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

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

Java™ is a US trademark of Sun Microsystems, Inc.

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

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

This guide's title page contains the following identifying information:

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

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

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

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

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

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

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

Support

You can visit the HP Software Support 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 Support Online 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 HP Software 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 find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Table of Contents

PART II: INTEGRATION WITH CI STATUS ALERTS

PART III: PROBLEM ISOLATION

1

Introduction to HP Service Manager/ HP ServiceCenter Integration with HP Business Availability Center

This chapter describes the HP Service Manager/HP ServiceCenter integration.

Note: HP Business Availability Center integrates with both HP ServiceCenter and HP Service Manager though only HP Service Manager is mentioned in this chapter. For details about the supported versions, see "HP ServiceCenter and HP Service Manager Integration Overview" on page 10.

This chapter includes:

Concepts

Tasks

HP ServiceCenter and HP Service Manager Integration Overview

The purpose of this guide is to provide the updates and additions to the HP Business Availability Center 7.5 documentation set that describe the additional integration support added for HP Business Availability Center version 7.52.

This section describes the main concepts of the HP Service Manager integration with HP Business Availability Center.

HP Service Manager software is a comprehensive and fully integrated IT service management suite that helps you decrease the time it takes to resolve problems. ITIL-based best practices and a highly scalable service-oriented architecture let you deploy consistent, integrated processes throughout your IT organization. HP Service Manager provides the following capabilities:

- Automate service management processes for incident, problem, change, configuration, availability, release, contract, catalog-based requests and service level management.
- Use built-in workflows to document, route and escalate issues for IT service management processes.
- Gain access to comprehensive configuration data through a powerful Universal CMDB (Universal Configuration Management database).
- Deploy solution easily across heterogeneous environments using an open architecture and web-based framework.

The support matrix is as follows:

Integration Matrix	Integration Type	HP Business Availability Center 7.52	HP Business Availability Center 7.50	HP Business Availability Center 7.00
HP Service Manager 7.02	Incident submission	Yes	Yes	No
	Problem Isolation	Yes	Yes	No
	EMS (Dashboard, Service Level Management)	Yes (SiteScope 10.00)	Yes (SiteScope 10.00)	Yes (SiteScope 10.00)
HP Service Manager 7.01	Incident submission	Yes	Yes	No
	Problem Isolation	No	No	No
	EMS (Dashboard, Service Level Management)	Yes (SiteScope 10.00)	Yes (SiteScope 9.50)	Yes (SiteScope 10.00)
HP ServiceCenter 6.26	Incident submission	Yes	Yes	No
	Problem Isolation	No	Yes	No
	EMS (Dashboard, Service Level Management)	Yes (SiteScope 10.00)	Yes (SiteScope 9.50)	Yes (SiteScope 9.00)

This section includes the following topics:

HP Service Manager Integration with HP Business Availability Center Components

You can integrate separately HP Service Manager with several components of HP Business Availability Center:

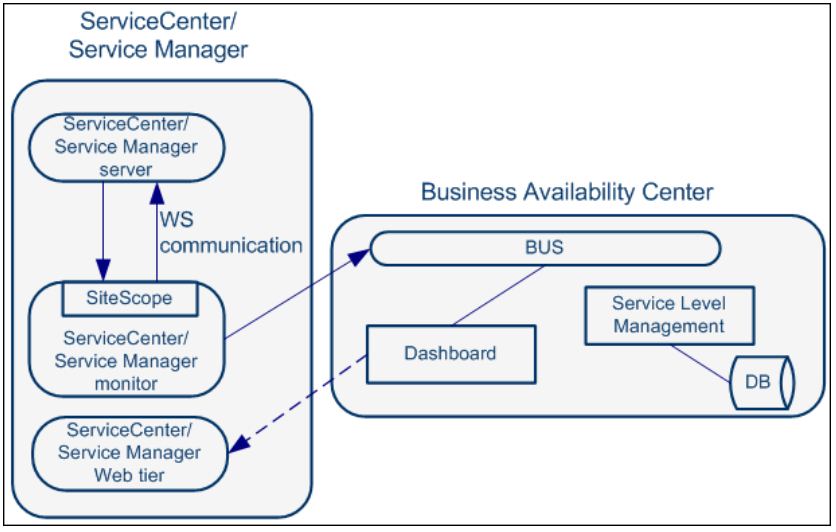
- **Dashboard**
- **Service Level Management**
- **Alerts**
- **Problem Isolation**

For details about how to perform the integration with the HP Business Availability Center components listed above, see “Set Up Integrations of HP Service Manager Data with HP Business Availability Center Components - Workflow” on page 16.

The integration enables the import of CIs from HP Service Manager into the UCMDB.

Integration with Dashboard

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



You can view the Number of Open Incidents KPI (based on data from HP Service Manager) at the business service level in the Dashboard views and reports. For details about the views, see "View Components" in *Using Dashboard*. For example: the Operator/Application support can get visibility and alerts based on the Number of Open Incidents in HP Business Availability Center Dashboard alongside operational KPIs.

You can drill down from Dashboard views at the EMS monitor level to HP Service Manager to view the details of the related incidents. For details about the available drill downs, see "Menu Options" in *Using Dashboard*. 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 ServiceCenter 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.

Integration with Service Level Management

You can define SLAs based on Serviceability KPIs (MTTR, MTBF, or MTBSI KPIs) that are calculated based on incidents that come from HP Service Manager. For details, see "Agreements in Service Level Management" in *Using Service Level Management*.

For example: the HP Service Manager manages SLAs with operational (Availability, Performance, or other KPIs) and serviceability (MTTR, MTBF, or MTBSI KPIs) using HP Business Availability Center Service Level Management. The HP Service Manager can review the SLAs statuses according to the service Availability, Performance, MTTR and MTBF side-by-side.

Integration with Alerts (Incident Submission)

HP Service Manager retrieves information, using the CI Alert Retrieval Service, about CI Status alerts triggered in HP Business Availability Center and automatically manages (open, update, or close) a corresponding incident in HP Service Manager.

For details, see "Open Incidents Using the CI Alert Retrieval Service" or "Open an Incident in HP Service Manager Using the Legacy URL" in *Alerts*.

Integration with Problem Isolation:

You can:

- Attach a problem in Problem Isolation to an existing or new incident or problem in HP Service Manager.
- Attach a problem snapshot to the incident in HP Service Manager.
- Drill down from the incident context in HP Service Manager to the appropriate problem in Problem Isolation.
- Proactively manage problems using the correlation of incidents and requests for change in HP Service Manager with the operational matrix like Availability or Performance that are integrated from different sources like End User Management, into Problem Isolation

  For details on Problem Isolation, see "Problem Isolation and HP Service Manager Integration" in *Using Problem Isolation*.

View Elements Created by the Integration with HP Service Manager

The HP Service Manager integration creates:

Element	Dashboard	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 Dashboard in the Business Services ServiceCenter, and the Service Measurements views, and the CIs are available to add to SLAs in Service Level Management.	
KPIs	"Number of Open Incidents" in *Using Dashboard*	"MTTR (Mean Time to Repair)", "MTBF (Mean Time Between Failures)", and "MTBSI (Mean Time Between System Incidents)" in *Using Service Level Management*
Rules	The Number of Open Incidents KPI (attached to an EMS Monitor CI) uses the Number of Open Incidents monitor rule in Dashboard. The rule handles the samples sent to HP Business Availability Center by the EMS system. For details on the rule, see "Number of Open Incidents" in *Using Dashboard*.	Each HP 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 Rules" in *Using Dashboard*
Context Menu	"HP SC Menu" in *Using Dashboard*	N/A
Context Menu Item	"HP Service Manager" in *Using Dashboard*.	N/A
Tooltip	"Number of Open Incidents Sentence" in *Using Dashboard*	N/A

Set Up Integrations of HP Service Manager Data with HP Business Availability Center Components - Workflow

You can integrate HP Service Manager with Dashboard, Service Level Management, Problem Isolation, and Alerts to provide the following capabilities:

- Collect performance and availability data from an existing HP Service Manager server and view the data in the Dashboard and the Service Level Management applications and enable the import of CIs from HP Service Manager into the UCMDB.
- Open incidents in HP Service Manager when an alert is triggered in HP Business Availability Center.
- Integrate Problem Isolation with HP Service Manager to link isolation data (from Problem Isolation) with incident or problem data (from HP ServiceCenter), to create a complete problem management lifecycle.

Each integration is performed separately.

For more information about the integration with HP Business Availability Center components, see "HP ServiceCenter and HP Service Manager Integration Overview" on page 10.

Note: Each step in the following workflow is optional.

This task includes the following steps:

- "Configure the Dashboard, Service Level Management and HP Service Manager Integration" on page 17
- "Configure HP Service Manager to Open an Incident When a CI Status Alert is Triggered in HP Business Availability Center" on page 17
- "Configure the Problem Isolation and HP Service Manager Integration" on page 17
- "Results" on page 17

1 Configure the Dashboard, Service Level Management and HP Service Manager Integration

You can collect data from an existing HP Service Manager Server and view the data in Dashboard and Service Level Management applications.

For details, see "View HP Service Manager Data in Dashboard and Service Level Management" on page 576.

2 Configure HP Service Manager to Open an Incident When a CI Status Alert is Triggered in HP Business Availability Center

You can set up HP Service Manager to retrieve information about CI Status alerts triggered in HP Business Availability Center.

For details, depending on the HP ServiceCenter, HP Service Manager, and HP Business Availability Center versions you are working with, see "Open Incidents Using the CI Alert Retrieval Service" or "Open an Incident in HP Service Manager Using the Legacy URL" in *Alerts*.

3 Configure the Problem Isolation and HP Service Manager Integration

You can integrate Problem Isolation with HP Service Manager to link isolation data (from Problem Isolation) with incident or problem data (from HP ServiceCenter), to create a complete problem management lifecycle. For details, see "Configure Problem Isolation and HP Service Manager Integration" in *Using Problem Isolation*.

4 Results

The integration of HP Service Manager with HP Business Availability Center CI Status alerts, Problem Isolation, Universal CMDB, Dashboard, and Service Level Management enables you to view HP Service Manager data in Dashboard and Service Level Management, to open incidents in HP Service Manager when alerts are triggered in HP Business Availability Center, and to isolate the problem in Problem Isolation.

For a detailed scenario of the complete integration, see "View HP Service Manager Data in HP Business Availability Center - Scenario" on page 18.

View HP Service Manager Data in HP Business Availability Center - Scenario

This section provides a scenario for the complete integration of HP Service Manager with Alerts, Dashboard, Problem Isolation, and Universal CMDB.

The CRM application owner, asks the HP Business Availability Center administrator to configure one alert for the CI representing her application. The alert is configured to trigger when the status of the Performance KPI attached to the CI worsens.

The CRM application owner is the alert recipient.

The alert is configured to open an incident in HP Service Manager when it is triggered.

1. Some time after the alert is put in production, the status of the CI's KPI changes to **Warning** and the alert is triggered.
2. When HP Service Manager automatically invokes the CI Alert Retrieval Service (in the next cycle), an incident is created for the application CI with a low urgency.
3. A few minutes later, the status of the Performance KPI attached to the CI changes to **Critical**. The CRM application owner received a notification that the alert was triggered.
4. When HP Service Manager automatically invokes the CI Alert Retrieval Service (in the next cycle), the incident severity is updated to **Critical** and all of the alert details are appended to the incident.
5. The Tier 1 support, looks at the opened incidents in HP Service Manager, and detects that a new incident was submitted. When he reviews the incident details, he understands that the CRM business service has a critical performance issue that was triggered recently. He also notices that the incident was automatically submitted by HP Business Availability Center.
6. The Tier 1 support takes ownership of the incident and decides to triage it. Using HP Service Manager, he launches the Problem Isolation application directly in the context of the CRM application. The isolation of the problem starts at the relevant CI as the CI ID is part of the data sent by HP Business Availability Center to HP Service Manager when the alert was triggered and is associated with the incident.

7. Using the isolation process, the Tier 1 support finds that the problem resides in the Database. He decides to send the incident to the DBAs. The Tier 1 support generates a Snapshot report with all the isolation details and attaches it to the incident, so the DBAs have all the required information for further analysis.
8. The DBAs solve the issue.
9. The status of the Performance KPI attached to the CI representing the CRM application changes to **OK**. The CRM application owner receives a notification.
10. The triggered alert opens an incident in HP Service Manager with the same identity but with the **OK** status. The incident is updated with the new data, which overrides the existing data, and its status changes to **Close**.
11. The CRM application owner views the CRM business service health through the HP Business Availability Center Dashboard. She can view, in real time, the status of the availability and performance of the CRM application as well as the number of open incidents.
12. As she reviews the status of the CRM application, she notices that the number of open incidents is increasing. Using Dashboard, she can review the incident's details to better understand the situation and take appropriate action.

Before you Upgrade HP Service Manager From Previous Versions

It is recommended to back up the following files before performing the upgrade procedure to HP Service Manager 7.02. For details on the upgrade see HP Service Manager documentation.

- **ServiceCenter Server**
  - <ServiceCenter Server Home>/RUN/sc.ini
  - <ServiceCenter Server Home>/RUN/cacerts
  - <ServiceCenter Server Home>/RUN/trustedclients.jks
  - <ServiceCenter Server Home>/RUN/hostname.devlab.ad.keystore (this filename varies by machine)

- **ServiceCenter Webtier**
  - <SC.WAR DIR>/WEB_INF/cacerts
  - <SC.WAR DIR>/WEB_INF/ hostname.devlab.ad.client.keystore (this filename varies by machine)
  - <SC.WAR DIR>/WEB_INF/web.xml
  - <SC.WAR DIR>/WEB_INF/classes/application-context.xml
  - <SC.WAR DIR>/WEB_INF/classes/lwssofmconf.xml
- **Symphony Adapter**
  - < SymphonyAdapter.war DIR>/WEB_INF/classes/ hostname.devlab.ad.client.keystore (this filename varies by machine)
  - < SymphonyAdapter.war DIR>/WEB_INF/classes/cacerts
  - < SymphonyAdapter.war DIR>/WEB_INF/classes/lwssofmconf.xml
  - < SymphonyAdapter.war DIR> /WEB_INF/classes/ SymphonyAdapter.properties

The Data files are not overwritten. To start with clean data, you need to delete the Data folder. After you reapply the **BAC_PA_62_v1.unl** you must reconfigure the two URL settings.

Part I

Integration with Dashboard and Service Level Management

2

HP Service Manager/HP ServiceCenter Integration with Dashboard and Service Level Management

This chapter describes the HP Service Manager/HP ServiceCenter integration with Dashboard and Service Level Management.

Note: HP Business Availability Center integrates with both HP ServiceCenter and HP Service Manager though only HP Service Manager is mentioned in this chapter. For details about the supported versions, see "HP ServiceCenter and HP Service Manager Integration Overview" on page 564.

This chapter includes:

Tasks

View HP Service Manager Data in Dashboard and Service Level Management

You can collect data from an existing HP Service Manager Server and view the data in Dashboard and Service Level Management applications.

Note: Complete each step before beginning the next step.

This task includes the following steps:

- "Configure HP Service Manager/HP ServiceCenter" on page 24
- "Configure the HP Service Manager/HP ServiceCenter Monitor in SiteScope" on page 25
- "Specify the HP Service Manager URL in the Infrastructure Settings" on page 25
- "Configure the HP Service Manager Integration" on page 26
- "Enable Accessing HP Service Manager from Within Dashboard" on page 27
- "Specify the State and Severity of Open Incidents to Be Displayed" on page 27
- "Include Service Center CIs in Service Level Management Agreements" on page 28
- "Results" on page 28

1 Configure HP Service Manager/HP ServiceCenter

You must configure HP ServiceCenter/HP Service Manager so it integrates with Dashboard and Service Level Management. For details, see "Configure HP ServiceCenter or HP Service Manager for Integration with Dashboard and Service Level Management" on page 29.

2 Configure the HP Service Manager/HP ServiceCenter Monitor in SiteScope

In SiteScope, you must configure the HP ServiceCenter/HP Service Manager monitors. For details, see "HP Service Manager Monitor" in *Using System Availability Management*.

You **must** synchronize HP ServiceCenter/HP Service Manager and SiteScope.

You must make sure that you are using in SiteScope the user you defined in "Create a Corresponding HP Service Manager User" on page 42. For details about the user, see "Configure HP ServiceCenter or HP Service Manager for Integration with Dashboard and Service Level Management" on page 29.

3 Specify the HP Service Manager URL in the Infrastructure Settings

To specify the HP Service Manager URL, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, select **Foundations**, select **Integrations with other applications**, and, 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.

For example:

- When working with HP ServiceCenter 6.26, the URL for HP ServiceCenter would be: <protocol>://<host_name>:<port>/sm62/). For example, http://fando:8080/sm62/.
- When working with HP Service Manager 7.01, the URL for HP ServiceCenter would be: <protocol>://<host_name>:<port>/sm70/). For example, http://fando:8080/sm70/.

4 Configure the HP Service Manager Integration

The HP Service Manager integration adapter is predefined.

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

a **Configure the HP Service Manager Monitor.** The monitor is used to retrieve data from the EMS system using System Availability Management Administration. You add the HP Service Manager Monitor 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 Availability Center is established. For details, see "HP Service Manager Integration – Workflow" in *Using System Availability Management*.

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.

b **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 HP 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 HP Business Availability Center, and creates the appropriate topology that is used to display the data in Dashboard. For details on the possible customizations, see "Define Assignment Configuration Dialog Box" on page 550.

5 Enable Accessing HP Service Manager from Within Dashboard

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

To enable accessing HP Service Manager from within Dashboard:

a Edit the **web.xml** file. The location of the file depends on the type of web application server the web tier is deployed on.

b In the file, locate the **<!-- Specify the ServiceCenter server host and port location** --> section.

c Add the following strings into the section:

```
<context-param>
<param-name>sc.querysecurity</param-name>
<param-value>false</param-value>
</context-param>
```

6 Specify the State and Severity of Open Incidents to Be Displayed

To specify 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.** Select **Admin** > **Dashboard** > **KPIs**, select the 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.** Select **Admin** > **Dashboard** > **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 "Number of Open Incidents" in *Using Dashboard*.

Note: The values available for the Initial State, Final State, and Severity parameters reflect the values defined in HP Service Manager.

---

7 Include Service Center CIs in Service Level Management Agreements

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

You must also configure the incident initial and final state in those rules. For details, see "Incident State and Severity Values" in *Using Service Level Management*.

For details on the integration, see "Integration with HP Service Manager" in *Using Service Level Management*.

8 Results

After the task is performed, HP Service Manager data is integrated into HP Business Availability Center as described in this section.

➤ **View HP Service Manager Data in Dashboard and Service Level Management:**

SiteScope automatically creates the appropriate topology when HP Service Manager data is integrated into HP Business Availability Center. HP Business Availability Center adds the data to the Business Services, ServiceCenter, and Service Measurement views, and you can display these views in Dashboard and Service Level Management.

➤ **Drill down to HP Service Manager from Dashboard views:**

In Dashboard, in the Business Services, ServiceCenter, and Service Measurement views, use the **HP ServiceCenter** option available for HP Service Manager CIs to access the relevant incident in the HP Service Manager application. For information about the HP Service Manager application, consult the HP ServiceCenter documentation.

Configure HP ServiceCenter or HP Service Manager for Integration with Dashboard and Service Level Management

This section describes how to configure HP ServiceCenter or HP Service Manager before performing its integration with Dashboard and Service Level Management.

Note: HP Business Availability Center integrates with specific versions of HP ServiceCenter. For details about the supported versions, see "HP ServiceCenter and HP Service Manager Integration Overview" on page 564.

This task describes how to configure HP Service Manager.

This task includes the following steps:

1 Prerequisites

- The ServiceCenter server, ServiceCenter Web tier, and ServiceCenter Windows client components of HP ServiceCenter must be installed. For details, see ServiceCenter Installation guide.
- Optional. If you want HP ServiceCenter to use the SSL-based Trusted Sign-on protocol, configure it according to the instructions in the HP ServiceCenter on-line help.

Note: Plan to put both the ServiceCenter Web tier and the Symphony Adapter webapp in the same container, so you can use the same certificate for both.

---

2 Set Up the sc.cfg File

Note: Perform this step if you use HP ServiceCenter 6.26. Skip this step if you use other versions.

Once the server is installed, you can start and stop it using the Windows services utility, or by using **net start** and **net stop** commands. It is recommended that you do the following immediately upon completion of the installation and configuration dialogs:

a Stop the server using a net stop ServiceCenter command.

b Edit the **sc.cfg** file found in the RUN folder of the Server installation folder. Typically the location of this folder is **c:\Program Files\Peregrine Systems\ServiceCenter 6.2\Server\RUN**

c Enable the servlet and the listener for connect-it on port 12670, the other parameters should be commented out to disable unnecessary processes that might slow down startup and shutdown and to avoid cluttering the **sc.log** file with lots of unnecessary messages.

Make sure that the bolded lines in the modified **sc.cfg** file are as follows (the line **scenter -listener:<listener_port>** should provide the port of the listener):

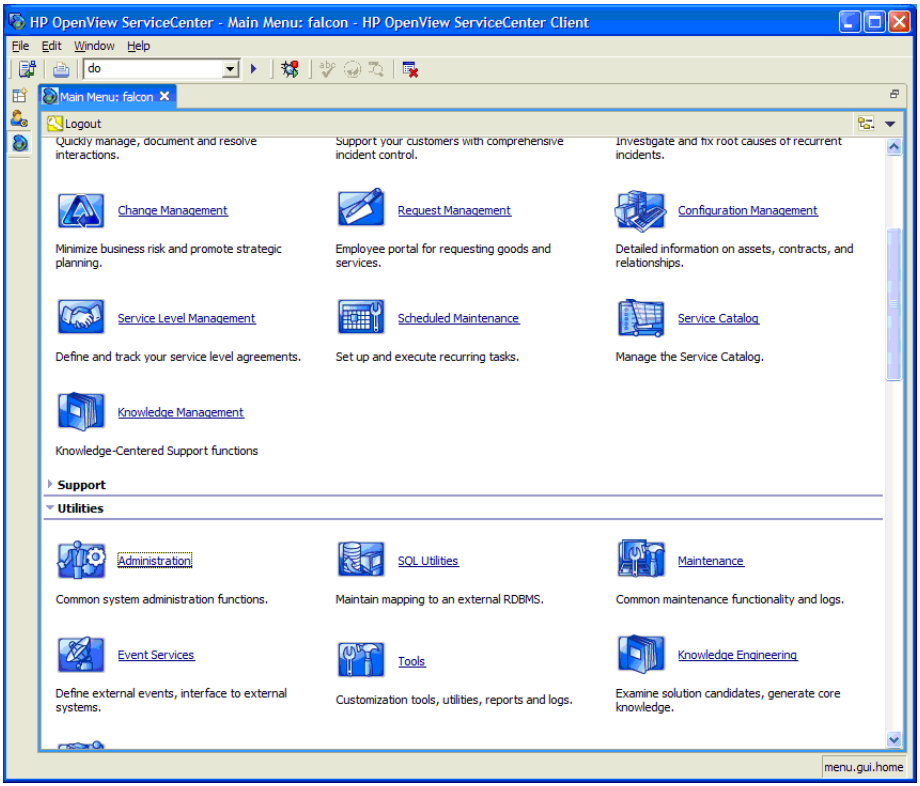
```
#
# ServiceCenter Server Configuration File
#
# Used by ServiceCenter service to start the ServiceCenter processes.
#
#########################################################################
#
# Copyright 1994-2007 Hewlett-Packard Development Company, L.P.
# All Rights Reserved
#
#########################################################################
#
# start a J2EE/servlet listener for HTTP clients: Windows, web, SOAP-API
#
scenter -servletcontainer -httpPort:13080 -httpsPort:13443
#
# Start a listener for Get-It, Connect-It, ODBC driver
#
scenter -listener
#
# start a listener for SCAuto
#
scenter -listener:12670
#
# start background schedulers
#
#scenter system.start
```

3 Configure URLs for the Integration

To configure the integration, use the following steps:

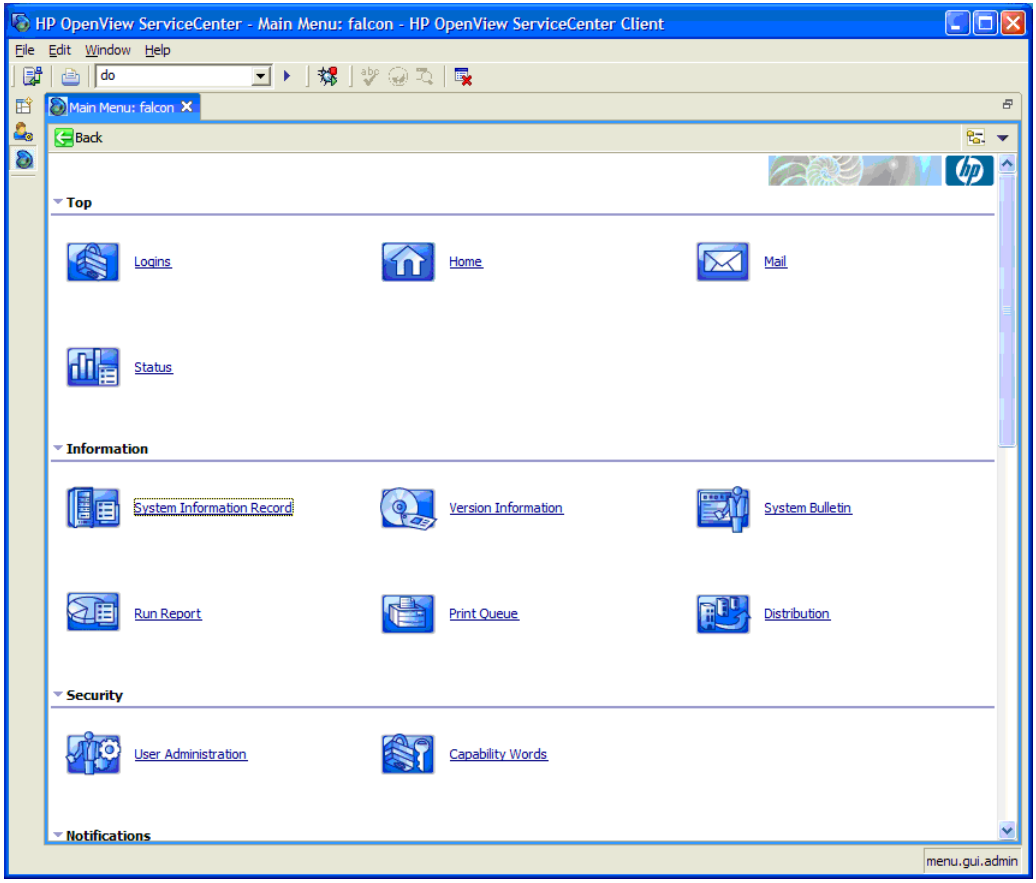
a Select **Utilities** > **Administration menu**:

The picture below is for HP ServiceCenter 6.2 x only.



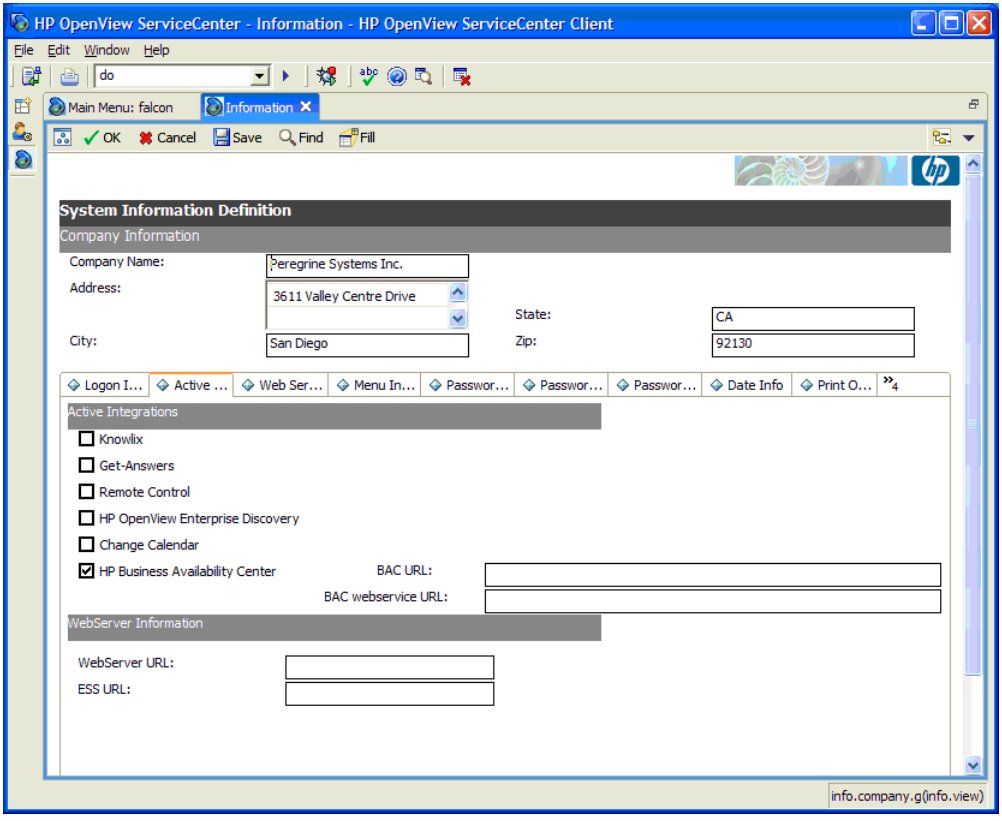
b Click the **System Information Record** menu:

The picture below is for HP ServiceCenter 6.2 x only.



c Click the **Active Integrations** tab:

The picture below is for HP ServiceCenter 6.2 x only.



d Select the **HP Business Availability Center** checkbox.

e In the **BAC URL** box enter the URL to the BAC Gateway server (for example: **http://<HP Business Availability Center Gateway host>/topaz/framework/topaz_frames.jsp**). This setting is used when launching Problem Isolation (the hostname should be the FQDN).

f In the **BAC webservice URL** box enter the URL for the EntityNotification endpoint (for example:
http://<HP ServiceCenter web tier host>:<PORT>/SymphonyAdapter/outbound/ws?endpoint=http://<HP Business Availability Center Gateway host>/topaz/services/EntityNotificationPort (the hostnames should be the FQDN).

Note: If you are using the SymphonyAdapter for LW-SSO single sign-on, the URL for the EntityNotification endpoint must be specified as the endpoint parameter of the SymphonyAdapter outbound URL (for example: http://FQDNsymphonyadapterhost:8080 /SymphonyAdapter/outbound/ws?endpoint=http://FQDNbachost:80/topaz/services/EntityNotificationPort

---

g Click **Save**.

4 Modify the web.xml File

This step is needed for the integration of HP ServiceCenter and HP Business Availability Center.

After installing and configuring LW-SSO, you must modify the **web.xml** file.

a Access the **web.xml** file (for example, the web.xml file can be located at: **\Apache Software Foundation\Tomcat 5.5\webapps\sc\WEB-INF** for HP ServiceCenter or at **\Apache Software Foundation\Tomcat 5.5\webapps\sm7\WEB-INF** for HP Service Manager) and change the value of <param_value> to **false** as indicated in bold in the code below (for **sc.querysecurity** for HP ServiceCenter or **querysecurity** for HP Service Manager.

```
<!-- Enables submission of form when the user presses the ENTER key. -->
      <init-param>
         <param-name>sc.autosubmit</param-name>
         <param-value>true</param-value>
      </init-param>

   <!-- Change value (e.g. 1, or 2) to increase horizontal spacing, useful for avoiding
     clipping problems with localized versions -->
      <init-param>
         <param-name>sc.hscale</param-name>
         <param-value>0</param-value>
      </init-param>

   <!--
   ********************************************************
    The following parameters can't be supplied in the URL: they can only be changed in
web.xml
   ********************************************************
   -->
      <init-param>
        <param-name>sc.querysecurity</param-name>
        <param-value>false</param-value>
      </init-param>

     <!-- Control the encryption of network communication between the application server
       and the ServiceCenter server -->
      <init-param>
        <param-name>sc.ssl</param-name>
        <param-value>false</param-value>
      </init-param>
```

b Restart the Tomcat container using the **Net stop tomcat** and **Net start tomcat** commands.

5 Configure the Symphony Adapter for HP ServiceCenter

Note: Perform this step if you use LW-SSO. Skip this step if you do not use LW-SSO.

This section describes how to configure the Symphony Adapter for HP ServiceCenter:

a Locate the **web-inf\classes** folder for the SymphonyAdapter webapp.

b Copy the **cacerts** file and **client keystore** file you created using the **makeadaptercert** script into the **web-inf\classes** folder of the SymphonyAdapter webapp. For details, see the HP ServiceCenter on-line help.

c Edit the **SymphonyAdapter.properties** file to correct these settings for your installation:

- **servicecenter.ws.targetLocationURL.** Edit the host and port as appropriate for your installation. You should use the fully qualified domain name to specify the host.
- **servicecenter.webtier.URL.** Update this property to make the hostname and port correct for the current Tomcat container. You must provide the fully qualified domain name, because this information is going to be used to rewrite URLs, which is sent back to HP Business Availability Center with a 307 redirect. DO NOT SPECIFY LOCALHOST. If you do, HP Business Availability Center tries to launch the ServiceCenter web user interface locally, which does not work!
- **clientcerts.keystore.** Update this parameter to point to the client keystore you created using **makeadaptercert**. You must use a full path name starting from the C: drive and using double slashes, for example:

  D:\\Program Files\\Apache Software Foundation\\Tomcat 5.5\\webapps\\SymphonyAdapter\\WEB-INF\\classes\\<machine name>.client.keystore

- **clientcerts.keystore.password.** Specify the correct pass-phrase for the client keystore specified above.

- **truststore.** Specify the full path to the updated **cacerts** file you created.
- **truststore.password.** Specify the pass-phrase for the **cacerts** file. If you did not change it, it should still be **changeit**.

  Note: If a single sign-on technology is configured (LW-SSO or SiteMinder), the ServiceCenter login panel is not displayed.

d In the Acegi configuration in the ServiceCenter web tier or Symphony Adapter for LW-SSO, edit the **lwssofmconf.xml** file in **WEB-INF/classes** directory of the location where the ServiceCenter webtier was deployed.

Locate the <domain> element under <web-lwsso>:

```
<web-lwsso>
        <lwsso startLWSSO="enabled">
            <domain>my.domain.com</domain>
             <crypto cipherType="symmetricBlockCipher"
            engineName="AES" paddingModeName="CBC"   keySize="256"
            encodingMode="Base64Url"initString="password">
            </crypto>
             <expirationPeriod>60</expirationPeriod>
 </lwsso>
```

Replace the bolded strings in the file with the fully qualified domain to which the web tier servers belong and where those servers are sharing authentication credentials via LW-SSO.

In addition, replace the bolded password string with the password to the server where the ServiceCenter webtier was deployed; it has to match between the systems that are sharing credentials using LW-SSO in their respective config files. For example, if your HP ServiceCenter web tier is installed on sc.mydomain.com and HP Business Availability Center is set up on bac.mydomain.com, the domain you would use in this configuration file is **mydomain.com** (both in the **<lwsso><domain>mydomain.com</domain>** part and under the **<protectedDomains><url>mydomain.com</url></protectedDomains>**) below.

Add your domains to the <protectedDomains> element as follows:

```
<protectedDomains>
      <url>fully_qualified_domain</url>
      <url>fully_qualified_domain</url>
      <url>fully_qualified_domain</url>
</protectedDomains>
```

Save changes.

6 Modify the application-context.xml File

Note: Perform this step if you use LW-SSO. Skip this step if you do not use LW-SSO.

This section describes how to modify the applicaton-context.xml file:

a You must modify the **application-context.xml** file in WEB-INF/classes directory of the ServiceCenter webtier. Make sure that the filterChainProxy bean definition contains the **lwSsoFilter** string as shown in the sample:

```
<bean id="filterChainProxy" class="net.sf.acegisecurity.util.FilterChainProxy">
  <property name="filterInvocationDefinitionSource">
    <value>
      CONVERT_URL_TO_LOWERCASE_BEFORE_COMPARISON
      PATTERN_TYPE_APACHE_ANT
      /**=httpSessionContextIntegrationFilter,lwSsoFilter,anonymousProcessingFilter
    </value>
  </property>
</bean>
```

b Make sure that the following lines are available (uncommented) at the bottom of the application-context.xml:

```
   <bean id="lwSsoFilter"
class="com.peregrine.eclipse.web.lwsso.LwSsoPreAuthenticationFilter">
    <property name="authenticationManager">
     <ref bean="authenticationManager"/>
    </property>
    <property name="defaultRole">
     <value>ROLE_PRE</value>
    </property>
   </bean>

   <bean id="lwSsoIntegrationBean"
class="com.peregrine.eclipse.web.lwsso.LwSsoIntegration"/>  </bean>
```

For detailed instructions on configuring LWSSO refer to the LWSSO documentation. Save changes.

c Restart the Tomcat container using **Net stop tomcat** and **Net start tomcat** commands.

7 Initial Sample Event in HP ServiceCenter

Open the HP ServiceCenter application and perform the following steps:

a From the System Navigator, select **Menu Navigation** > **Tailoring** > **Database Manager**.

b Select the **Administrative Mode** option.

c Enter **apm.global.list.entry** in the **Form** box.

d Click **Search** to open a blank record from the **globallists** file.

e Click **Search** to display a list of lists.

f Select **Mass Update**. A blank update screen opens. This form is identical in appearance to the lister record, but contains different option buttons.

g Set the date in the **Expiration** box to any date in the past, for example, 01/01/90.

h Click **Simple Update** to reset the expiration date of all the lists in the **globallists** file.

i Return to the home menu.

j Enter ***aapm.server.initer** in the command line and click **Enter**.

k Log out of HP ServiceCenter and log in again.
All the lists in the system are regenerated and HP ServiceCenter processes all the current records.

8 Set Up and Configure Connect-IT

Note: Perform this step if you use HP ServiceCenter 6.26. Skip this step if you use other versions.

You must set up and configure Connect-IT for the integration with HP Business Availability Center if you want to automatically open tickets in HP ServiceCenter when relevant alerts are triggered in HP Business Availability Center. For details, see the BAC KPI Monitoring to Incident Management Integration guide.

9 Define HP Service Manager Tables for External Access

To enable the integration, you must provide external access to the clocks table and the probe_summary table in HP Service Manager. This can be done:

- 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 Availability Center. For details on how to perform this task, see "Enable External Access to the clocks and probe_summary Tables – Details" on page 42.

10 Configure the HP Service Manager Monitor

You must configure the HP Service Manager monitor. For details, see "HP Service Manager Integration – Workflow" in *Using System Availability Management*.

11 Create a Corresponding HP Service Manager User

You must create a dedicated user in HP Service Manager that should be used solely for the purposes of this HP Business Availability Center/SiteScope integration.

The HP Service Manager machine and the SiteScope machine **must** share the same time zone. They **must** also use the same date format (SiteScope date format): **dd/mm/yy**.

Use the value for the **Username** and **Password** fields when configuring the monitor that you created in HP Service Manager.

12 Perform the Integration

After you finish configuring HP ServiceCenter you must complete the integration task. For details, see "Configure the HP Service Manager/ HP ServiceCenter Monitor in SiteScope" on page 25.

Enable External Access to the clocks and probe_summary Tables – Details

The following are the steps necessary to enable external access to the clocks and probe_summary tables.

To use the configuration file to enable external access to the clocks and probe_summary tables:

1. Locate the configuration file **Ticketing_Integration_extaccess_def.unl** on the HP Business Availability Center DVD and copy it to a local directory.
2. Open the HP Service Manager client that is attached to the server used for the integration.
3. Select **Toolkit** > **Database Manager**.
4. In the menu on the upper right side of the Database Manager, select **Import/ Load**.
5. Select the **Ticketing_Integration_extaccess_def.unl** file (for HP ServiceCenter 6.26) or the **Clocks_extaccess_sm702_10Nov08.unl** file (for HP Service Manager 7.01 or 7.02).
6. Click the **Load FG** button.

7 Verify that the clocks table has the values described below. If the values do not match, edit the clocks table in ServiceCenter/Service Manager so that the values are the same as in the below table.

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

Before you Upgrade HP Service Manager From Previous Versions

It is recommended to back up the following files before performing the upgrade procedure to HP Service Manager 7.5.2. For details on the upgrade see HP Service Manager documentation.

- **ServiceCenter Server**
  - <ServiceCenter Server Home>/RUN/sc.ini
  - <ServiceCenter Server Home>/RUN/cacerts
  - <ServiceCenter Server Home>/RUN/trustedclients.jks
  - <ServiceCenter Server Home>/RUN/hostname.devlab.ad.keystore (this filename varies by machine)
- **ServiceCenter Webtier**
  - <SC.WAR DIR>/WEB_INF/cacerts
  - <SC.WAR DIR>/WEB_INF/ hostname.devlab.ad.client.keystore (this filename varies by machine)
  - <SC.WAR DIR>/WEB_INF/web.xml

- <SC.WAR DIR>/WEB_INF/classes/application-context.xml
- <SC.WAR DIR>/WEB_INF/classes/lwssofmconf.xml

- **Symphony Adapter**
  - < SymphonyAdapter.war DIR>/WEB_INF/classes/ hostname.devlab.ad.client.keystore (this filename varies by machine)
  - < SymphonyAdapter.war DIR>/WEB_INF/classes/cacerts
  - < SymphonyAdapter.war DIR>/WEB_INF/classes/lwssofmconf.xml
  - < SymphonyAdapter.war DIR> /WEB_INF/classes/ SymphonyAdapter.properties

The Data files are not overwritten. To start with clean data, you need to delete the Data folder. After you reapply the **BAC_PA_62_v1.unl** you must reconfigure the two URL settings.

Troubleshooting and Limitations

This section includes the following topics:

Severity Change in an Incident

An incident in HP Service Manager that changes its severity from low to high is not included in the Number of Tickets KPI in Business Availability Center. To include the incident, you must re-synchronize the SiteScope monitor.

Changes to the Tresholds of the Number of Open Incidents KPI

If you modify the thresholds of the Number of Open Incidents KPI in Dashboard administration, the value displayed by the Number of Open Incidents KPI in Dashboard views is 0 as the number of incidents is reset.

Problem

All the SiteScope samples that are sent to Business Availability Center, provide the number of changes that were added after SiteScope ran the last time before you made the threshold changes. other SiS samples which arrives, giving to BAC only number of changes which were added after SiS ran at last time.

Solution

Enable the Sync flag of the SiteScope monitors to re-import all the changes that happened before you changed the threshold.

Inaccurate Forecast Results

The Forecast information for SLAs, which include Ticketing KPIs whose status is imported from HP Service Manager using the HP Service Manager monitor, is not correct.

Part II

Integration with CI Status Alerts

3

Open Incidents in HP Service Manager using the CI Alert Retrieval Service

This chapter provides information on opening incidents in HP Service Manager, using the CI Alert Retrieval Service, when CI Status alerts are triggered in HP Business Availability Center 7.5.2.

Note: HP Business Availability Center integrates with both HP ServiceCenter and HP Service Manager though only HP Service Manager is mentioned in this chapter. For details about the supported versions, see "Opening Incidents in HP Service Manager" on page 50.

This chapter includes:

Concepts

Tasks

➤ Upgrade from the Previous Version of HP Service Manager Integration with Alerts on page 85

Troubleshooting and Limitations on page 86

Integration with HP Service Manager – Overview

You can open incidents in HP Service Manager or in HP ServiceCenter that correspond to CI Status alerts triggered in Business Availability Center. For details, see "Open Incidents Using the CI Alert Retrieval Service" on page 67 or in "Open an Incident in HP Service Manager Using the Legacy URL" on page 141.

Opening Incidents in HP Service Manager

You can automatically manage (open, update, or close) an incident in HP Service Manager when a CI Status alert is triggered in Business Availability Center.

Depending on the version of HP ServiceCenter or HP Service Manager, the method used to manage the incident is different.

HP ServiceCenter and HP Service Manager Versions	Procedure used to Open Incidents in HP Service Manager when a CI Status Alert is Triggered
HP ServiceCenter 6.26 HP Service Manager 7.01	**Legacy URL** For details, see "Open an Incident in HP Service Manager Using the Legacy URL" on page 141
HP Service Manager 7.02 + smbac patch	**CI Alert Retrieval Service** For details, see "Open Incidents Using the CI Alert Retrieval Service" on page 67

Incidents Opened in HP Service Manager by CI Status Alerts Using the CI Alert Retrieval Service

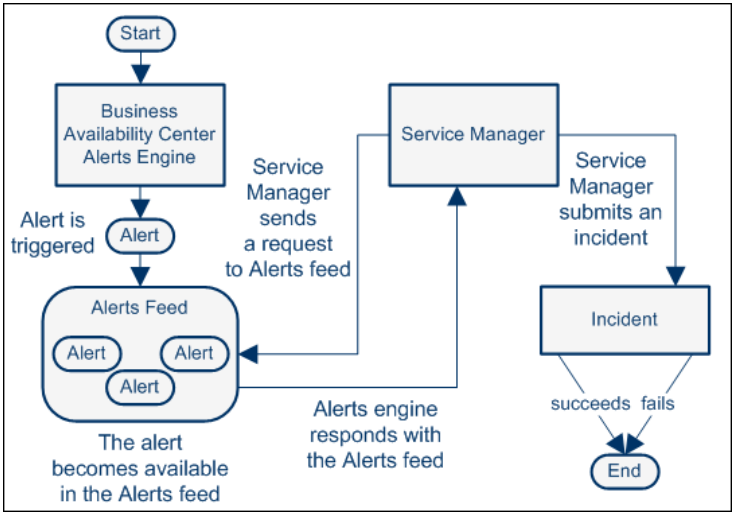
You can automatically open an incident in HP Service Manager when a CI Status alert is triggered using the CI Alert Retrieval Service.

This section includes the following topics:

How HP Service Manager Retrieves Alert Information

The Business Availability Center engine triggers a CI Status alert when the specified conditions occur. The alert is sent to the Alerts feed.

By default, every 5 minutes, HP Service Manager retrieves information about the CI Status alerts triggered in Business Availability Center, from the Alerts feed, using the CI Alert Retrieval Service. For details, see "CI Alert Retrieval Service API Overview" on page 96. HP Service Manager uses the information to submit an incident.



You can modify the default retrieval time period in HP Service Manager. For details, see HP Service Manager documentation.

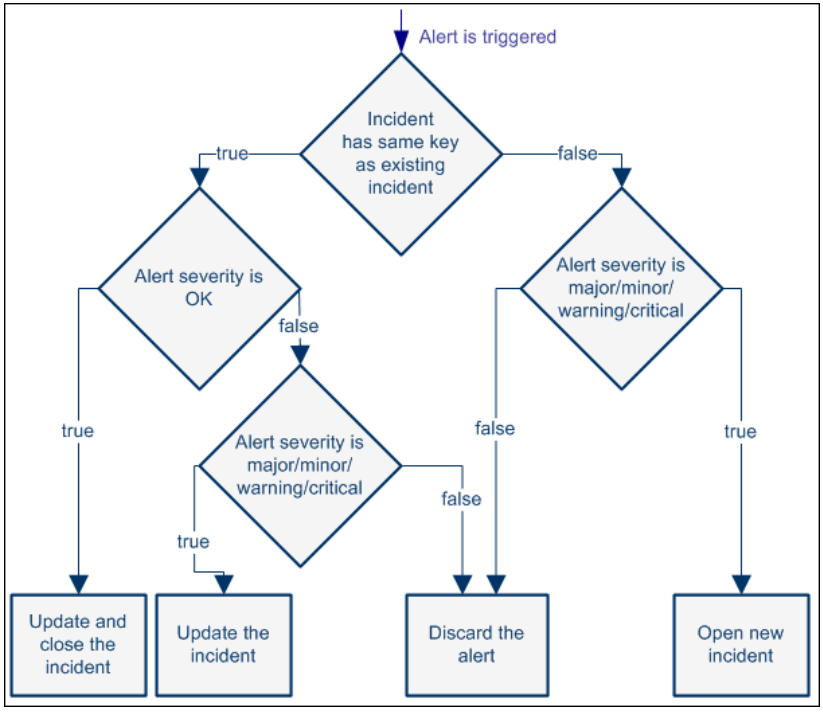
For each alert retrieved from the Alerts feed, and depending upon the configuration of the HP Service Manager, the content of a retrieved alert and the state of existing incidents are handled differently. For details see "How HP Service Manager Handles Alerts" on page 53.

How HP Service Manager Handles Alerts

An incident is identified by its key, which is composed of the CI ID and the KPI name of the CI whose change of status triggered the alert.

An incident previously opened is updated with new alert data when a CI Status with the same identifying information is triggered.

HP Service Manager handles alerts as shown in the following diagram:



All correlations (checking the identity of the incident) is done using the combination of the CI ID and the KPI name.

The default mapping between Business Availability Center to HP Service Manager is as follows:

Business Availability Center	**HP Service Manager**
Critical	Critical
Major	High
Minor	Average
Warning	Low
No Data /Uninitialized/Stop/ Downtime/No Data	**Default:** Discard You can customize the default to any other value. You can also create an unknown HP Service Manager severity and map it to **Discard**. For details, see HP Service Manager User's Guide
OK	Update and close the incident

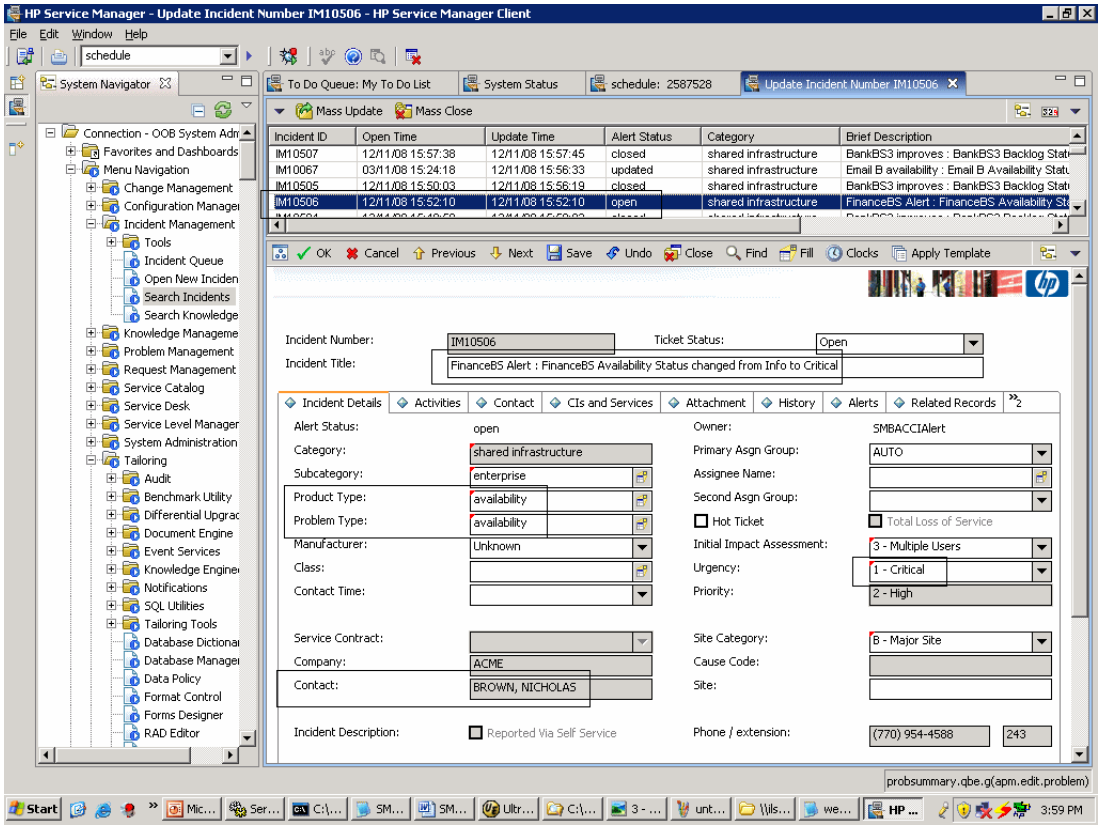
The default mapping can be modified in HP Service Manager.

For details about how HP Service Manager handles alerts, see "Life-Cycle of an Incident Triggered by a CI Status Alert in HP Service Manager – Scenario" on page 55.

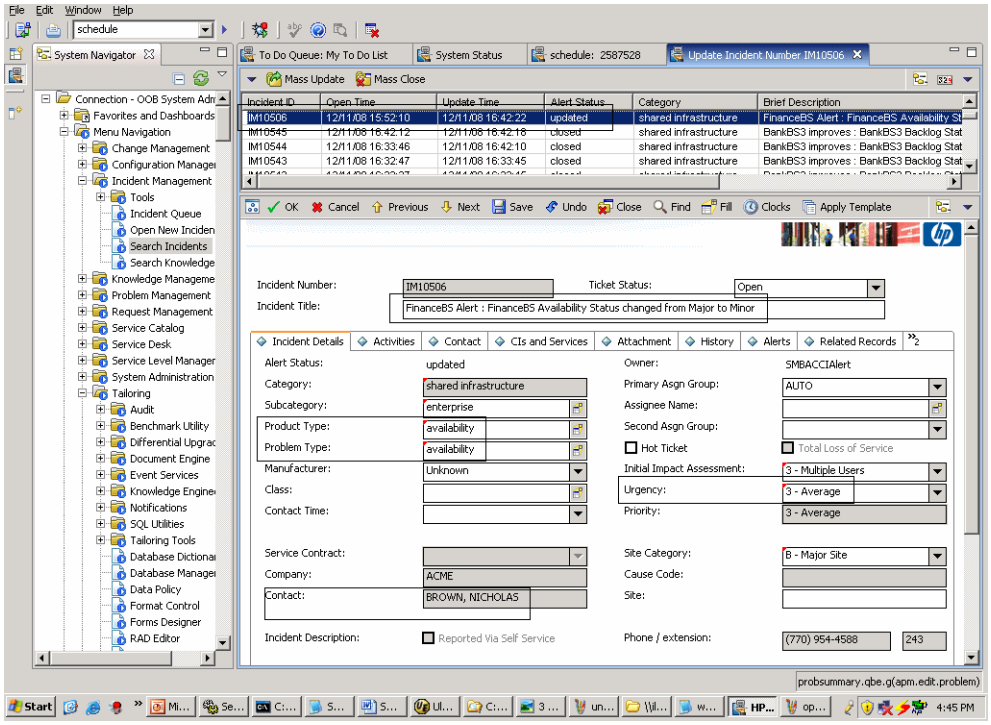
Life-Cycle of an Incident Triggered by a CI Status Alert in HP Service Manager – Scenario

The scenario is as follows: a CI Status alert is triggered in Business Availability Center, and at the scheduled time HP Service Manager retrieves the alert information from Business Availability Center and creates an incident. The alert is then updated and closed in Business Availability Center. You can view what happens in HP Service Manager as follows:

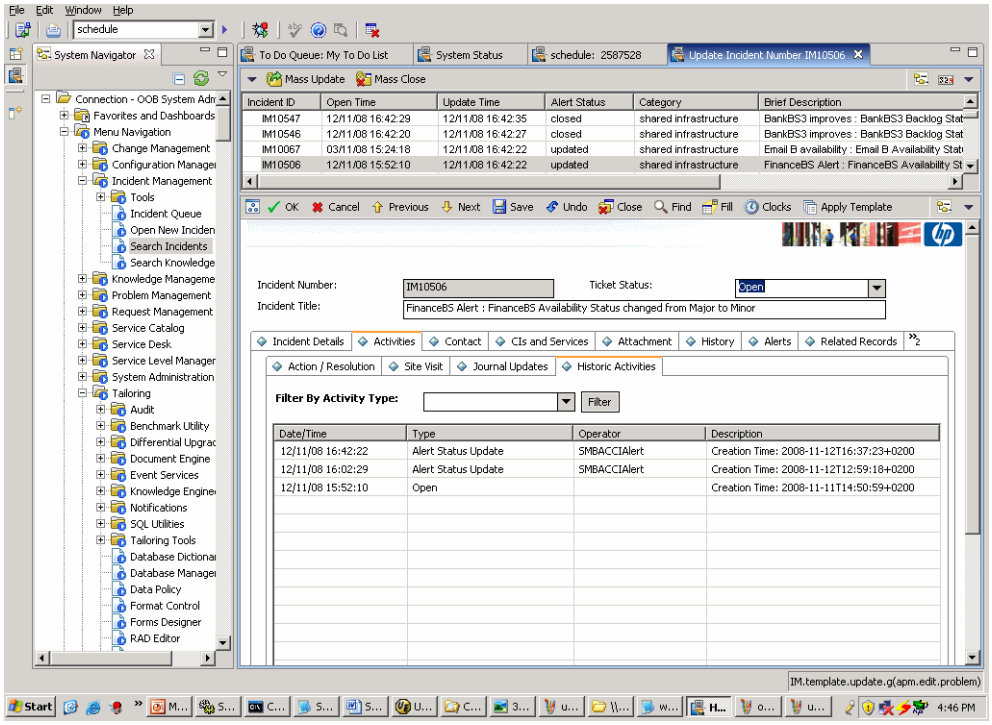
➤ **An incident is created.** The Incident Details tab displays the fact that an alert triggered because the FinanceBS CI status changed to Critical was retrieved by HP Service Manager and as a result a new incident was opened in HP Service Manager where the Urgency is Critical, the Product Type and Problem Type as availability, and the contact person is Nicholas Brown. The log indicates that the incident was opened.



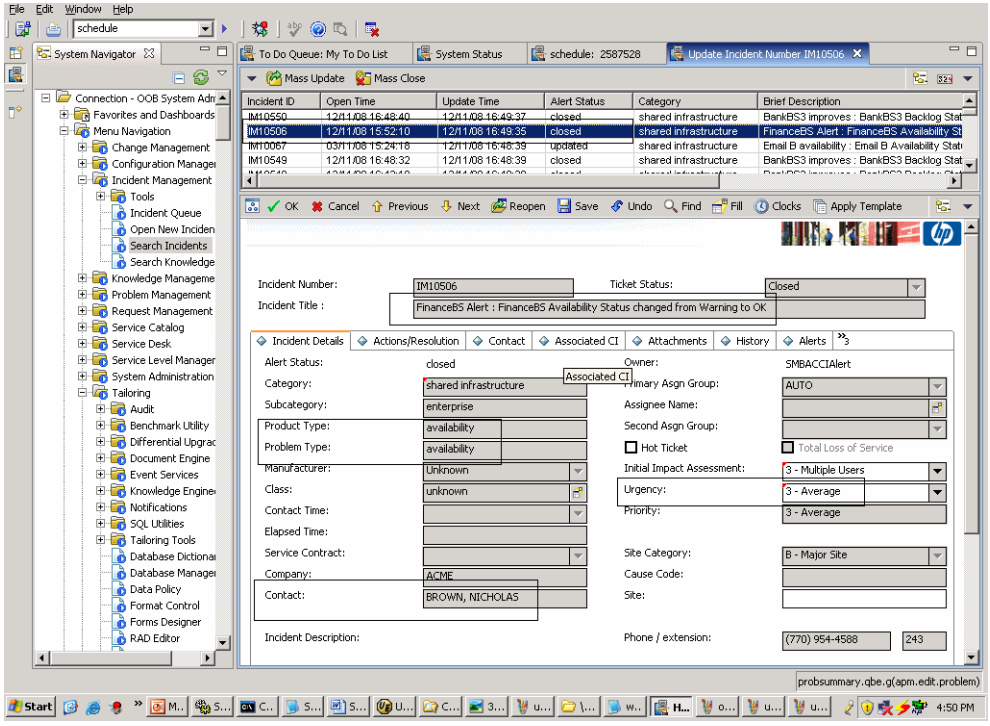
➤ **An incident is updated**. The Incident Details tab displays the fact that an alert triggered because the FinanceBS CI status changed from Major to Minor, was retrieved by HP Service Manager and as a result the previous incident was updated in HP Service Manager. The Urgency changed to Average. The other parameters stayed the same. The log indicates that the incident was updated.



You can view the incident history by clicking on each entry in the log.



➤ **An incident is closed.** The Incident Details tab displays the fact that an alert triggered because the FinanceBS CI status changed from Warning to OK was retrieved by HP Service Manager and as a result the incident was closed in HP Service Manager. The Urgency is Average. The other parameters stayed the same. The log indicates that the incident was closed.



Mapping of Business Availability Center CI Types to HP Service Manager CI Types

The mapping is as follows:

Business Availability Center CI Type	HP Service Manager CI Type
Application	Application
Business Service	bizservice
Host	Computer
NT	Computer **Note:** You can customize this mapping. For details, see HP Service Manager User's Guide.
UNIX	Computer **Note:** You can customize this mapping. For details, see HP Service Manager User's Guide.

Rule and Field Mapping in HP Service Manager

This section describes the rule and the field mapping used in the integration of HP Service Manager with Business Availability Center.

Note: This section is for advanced users.

This section includes the following topics:

Business Availability Center Alert/HP Service Manager Incident Correlation Rules

In the Business Availability Center Alert Feed process workflow, rules are used to search, create, update and close incidents.

The rules are configured in the Business Availability Center Alert Integration Configuration page. (To access the page, you must have installed the Out-of-Box solution of SMBAC, and in the HP Service Manager client, select **Menu Navigation >System Administration >BAC Alert Integration >BAC Alert Integration Configuration**.)

For details about the correlation rules, see "Business Availability Center Alert/HP Service Manager Incident Correlation Rules" on page 114.

How the Rules Work

When an Business Availability Center CI Status alert is retrieved, the HP Service Manager database searches for a keyword (CI ID and the KPI name of the CI whose change of status triggered the alert) that is part of the data retrieved with the alert. The keyword is used to determine if the corresponding incident already exists in the database and thus should be updated or closed or if the incident does not exist and should be created. The search is done as follows:

- The search process uses information from the alert. The Correlation Rule is appended to the search clause. If there is no compatible information, the process searches again using the legacy Correlation Rule.
- If a target incident is not found, the process creates a new incident using the fields in the alert.

➤ If a target incident is found, the process checks if one of the three rules matches the alert retrieved from Business Availability Center (target incident is **true).**

  ➤ If no rule matches, the rule **failed** and the target incident cannot be updated. The process then checks if the target incident is **true** to the Close Rule. If it is **true**, the process closes the action for target incident; if it is not **true**, the target incident is **Dropped**

  ➤ If a rule matches, its action is performed. For example, if the incident matches the Update Rule the process updates the existing incident in HP Service Manager with the alert information.

For additional details, see Opening Incidents in HP Service Manager on page 50.

Note: The three rules use the severity value as the condition value, so when the three rules are changed, the severity value should be taken into consideration. The severity values are set in the **Value Mapping.**

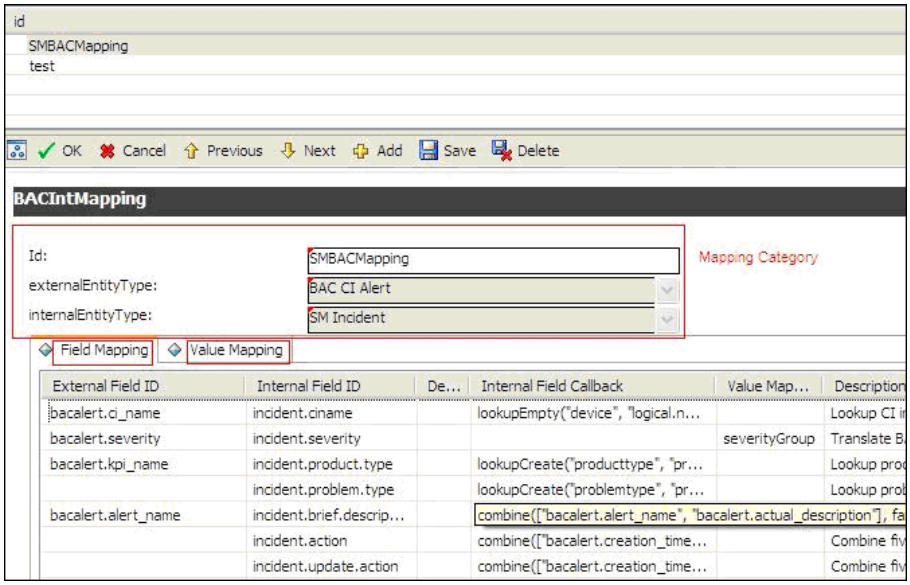
Field Mapping Relationship

A field mapping relationship includes the following components:

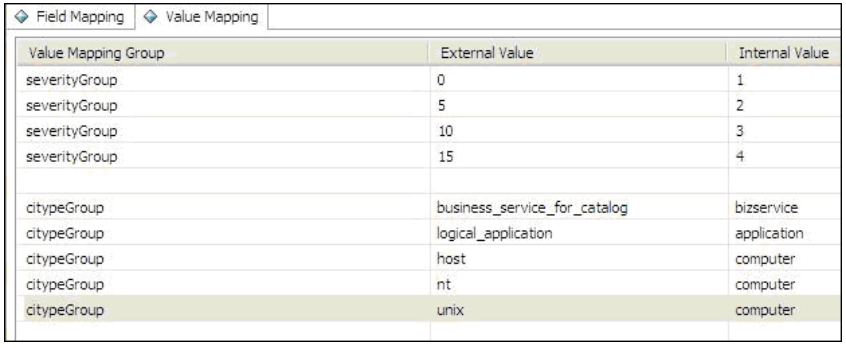
Components	Description
Entity	Defines the side to be mapped as an Entity. For example, HP Business Availability Center CI Status alert is one entity, the HP Service Manager incident is another entity. For details, see "Entity" on page 128.
Field	Each entity has many fields used to define it. This component defines the fields of each entity (defined above). Each field has several properties detailed in the Mapping component description. For details, see "Field" on page 124.

Components	Description
Mapping	Both the Entity and Field components represent the basic data of the Mapping Component. The Mapping Component uses Entity and Field to show the relationship between the special entities. For details, see "Field Mapping" on page 129. The Mapping Component includes the following: **Mapping Category** ➤ It defines the main properties of this Mapping. ➤ It specifies the external entity and the internal entity. **Field Mapping** ➤ It defines the fields mapping relationship between the internal system and external entity. ➤ It also defines the default value used if the external field does not exist or if it does not have a value. ➤ It provides the Callback function for the assignment of default value. Five callback functions are defined in this process. These functions are invoked to assign a value to the field of HP Service Manager. For details about the callback function, see "Callback Functions" on page 133. These functions can be used for field mapping instead of values. **Value Mapping** ➤ It defines the fields that have the Enumerate values in both systems and how they are mapped between the internal system and external system.

Example of Mapping category and field mapping:



Example of value mapping:



How to Build a Field Mapping Relationship

Field Mapping represents the relationship between the Business Availability Center Alert Field and HP Service Manager Incident.

When you want to build a Field Mapping relationship you need two fields: a new Business Availability Center Alert field and a new HP Service Manager Incident field. After the two fields have been prepared, proceed as explained in "Configure HP Service Manager for Integration with Business Availability Center Alerts" on page 68.

For details on adding a field, see "Maintain the BAC Alert Integration Field" on page 90.

Rules for Building Field Mapping Relationship

When build the new Field Mapping, the following rules should be followed.

➤ **Rule of the Callback Function in the Internal Field Callback column**:

Condition	Description
No callback is used	This means that the **Internal Field Callback** column is empty. ➤ If the external (Business Availability Center Alert) field has value, set this value. ➤ If the value is empty, use the default value in the **Default Internal Field Value** column. **Example:** The example is based on the out-of-the-box data. Select **System Administration** -> **Base System Configuration** -> **BAC Alert Integration Field Mapping** and check the record line that includes **bacalert.ci_id**. In this scenario, the value in **bacalert.ci_id** is used as the value for **incident.bac.ci.id**. For example, check as above, the record line that includes **incident.category**. In this scenario, the default value in **Default Internal Field Value** is used as the value for **incident.category**.
The **lookup** Callback is used	➤ The **lookup** Callback sets the value. ➤ If the lookup fails, the Callback uses the value passed from the external field (Business Availability Center Alert). ➤ If the value is empty, the Callback uses the default value in the **Default Internal Field Value** column. **Example:** The example is based on the out-of-the-box data. Select **System Administration** -> **Base System Configuration** -> **BAC Alert Integration Field Mapping** and check the record line that includes **incident.category**. In this scenario, the value in **bacalert.ci_id** is used as the value for **incident.category**. For example, check as above, the record line that includes **incident.site.category**. In this scenario, if the lookup is successful, the looked up value is used as the value for **incident.site.category**; if lookup fails, the default value is used.

Condition	Description
The **setValue** Callback is used	➤ If this function only has one parameter, the Callback sets the value from Business Availability Center only when the current action corresponds to the action specified by the parameter; if this value is empty, set the default value. ➤ If this function has two parameters, the current action uses the second parameter to set the value of the current field, and the value from Business Availability Center or the default value is ignored. **Example:** The example is based on the out-of-the-box data. Select **System Administration -> Base System Configuration -> BAC Alert Integration Field Mapping** and check the record line that includes **incident.resolution.code** In this scenario, the value **User Closure** is used as the value for **incident.resolution.code**.
Other callback functions are used	These functions include: ➤ **lookupCreate** ➤ **lookupEmpty** ➤ **setValue** ➤ **combine** They handle the value assignment. The **External Field ID** and **Default Internal Field Value** are ignored. **Example:** The example is based on the out-of-the-box data. Select **System Administration -> Base System Configuration -> BAC Alert Integration Field Mapping** and check the record line that includes **incident.brief.description**. In this scenario, the **combine** Callback sets the value for **incident.brief.description**, independently of the value passed from Business Availability Center. For details about the callback functions, see "Callback Functions" on page 133.

➤ **Rule of the Severity.** If you modify the severity (in the Value Mapping tab), the mapping between HP Service Manager severity and Business Availability Center status might affect the processes, so the corresponding rule (Create, Update, and Close rules) might have to be modified. Please refer the content of chapter **BAC Alert/SM Incident Correlation Rules** in HP Service Manager documentation.

Open Incidents Using the CI Alert Retrieval Service

You can automatically manage (open, update, or close) an incident in HP Service Manager when a CI Status alert is triggered in Business Availability Center.

HP Service Manager retrieves the information about the alert from Business Availability Center using the CI Alert Retrieval Service. For details, see "CI Alert Retrieval Service API Overview" on page 96.

For details on the mechanism used to open an incident in HP Service Manager when a CI Status alert is triggered, see "Opening Incidents in HP Service Manager" on page 50.

This task includes the following steps:

- "Configure HP Service Manager" on page 67
- "Check the Setting of the Enable Legacy Integration with Service Manager Parameter" on page 68
- "Define CI Status Alerts" on page 68
- "Results - View Incidents in HP Service Manager" on page 68

1 Configure HP Service Manager

You must configure HP Service Manager before performing its integration with Business Availability Center. For details, see "Configure HP Service Manager for Integration with Business Availability Center Alerts" on page 68.

2 Check the Setting of the Enable Legacy Integration with Service Manager Parameter

When you perform the integration of the Alerts application with HP Service Manager using the CI Alert Retrieval Service you must make sure that the **Enable legacy integration with Service Manager** is set to **false**.

To check if the parameter is set to **false**, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and locate the **Enable legacy integration with Service Manager** entry in the Integrations with other applications - Alerts-Service Manager Integration table.

3 Define CI Status Alerts

Define CI status alerts. For details, see "Create a CI Status Alert Scheme and Attach it to a CI" on page 65.

Select the Open incident in Service Manager option in the Actions page in the CI Status Alerts wizard. For details, see "Actions Page" on page 98.

4 Results - View Incidents in HP Service Manager

View, in HP Service Manager, the incidents related to the CI Status alerts in Business Availability Center. For details, see HP Service Manager documentation.

Configure HP Service Manager for Integration with Business Availability Center Alerts

This section describes how to deploy and administer HP Service Manager for integration with Business Availability Center before the integration with Business Availability Center.

This task includes the following steps:

- "Import the Core Unload File" on page 69
- "Click the bac.ci.id Field to the probsummary Table" on page 70
- "Perform the Automatic Default Configuration" on page 70

1 Import the Core Unload File

The core Unload file includes the basic logic of the integration with Business Availability Center integration.

Import the core Unload file as follows:

a Click **Menu Navigation** > **Tailoring** > **Database Manager**.

Right-click the detail button and select **Import/Load**.

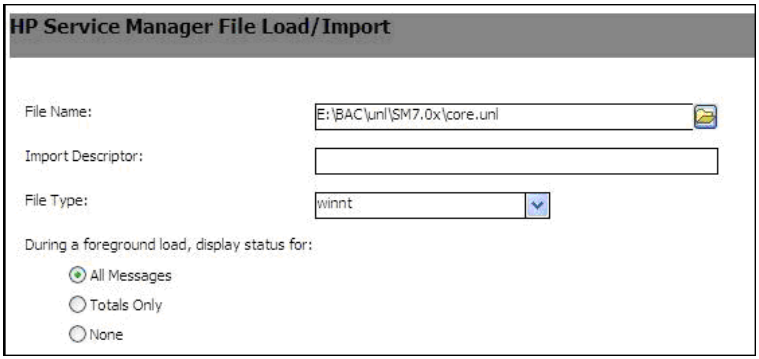
b In the HP Service Manager File Load/Import, click **Specify File** to locate the **smbac_coreXXX.unl** file (where XXX represents different versions). The file is loaded via the file browser.

c Enter the description in the **Import Description** box.

d Select **winnt** in the **File Type** list.

e Select a display option.

f Click **Load FG** to start loading.



2 Click the bac.ci.id Field to the probsummary Table

Add one field to the **probsummary** table:

a Click **System Definition** > **Tables** > **probsummary** > **Fields.**

b Click the **New Field** button to add a new field.

c Enter **bac.ci.id** in the **Field Name** box.

d In the General Properties area, select **Character** in the **Data Type** list.

e Click the **Save** button to save the new field.

3 Perform the Automatic Default Configuration

This step describes how to import the **smbac_out-of-boxXXX.unl** file (where XXX represents different versions) to create the default configuration.

Note: You can also perform the equivalent procedure manually. For details, see "Mapping of Business Availability Center CI Types to HP Service Manager CI Types" on page 59.

---

a Click **Menu Navigation** > **Tailoring** > **Database Manager**.

Right-click the detail button and select **Import/Load**.

b In the HP Service Manager File Load/Import page, click **Specify File** to locate the **smbac_out-of-boxXXX.unl** file (where XXX represents different versions). The file is loaded via the file browser.

c Enter the description in the **Import Description** box.

d Select **winnt** in the **File Type** list.

e Select a display option.

f Click **Load FG** to start loading.

After the deployment, the following components are affected as follows:

Contents	Description
Data about creating menu	The corresponding manual task is described in "Add a Main Menu" on page 88. The corresponding manual task is described in "Add a Details Menu" on page 89.
Business Availability Center alert integration entity data	The corresponding manual task is described in "Maintain a BAC Alert Integration Entity" on page 89.
Business Availability Center alert integration field data	The corresponding manual task is described in "Maintain the BAC Alert Integration Field" on page 90.
Business Availability Center alert integration field mapping data	The corresponding manual task is described in "Maintain the Business Availability Center Alert Integration Field Mapping" on page 90.
Schedule data	The corresponding manual task is described in "Create Schedule" on page 92.
Link Customization	For details, see "Link Customization" on page 93.

4 Verify the Deployment

To verify that the deployment completed correctly, use the following methods:

Verify Item	Method
Schedule	1 Go to the **Schedule** form (for details, see "Create Schedule" on page 92). 2 Enter **SMBAC CI Alert Integration** in the **Name box.** 3 Click **Search**. 4 Check the data against the "Create Schedule" on page 92.
Menu	1 Go to the **Menu** form (for details, see "Add a Main Menu" on page 88). 2 Enter **SYSTEM ADMINISTRATION** in the **Menu Name box** to check the Main menu data against "Main Menu Folder" on page 119. 3 Go to the **Menu** form (for details, see "Add a Main Menu" on page 88). 4 Enter **SMBAC Alert Integration** in the **Menu Name** box to check the Details menu data against "Detail Menu Items" on page 119.
BAC Alert Integration Entity	1 Go to **BAC Alert Integration Entity** form (for details, see "Maintain a BAC Alert Integration Entity" on page 89). 2 Click **Search** to check the data. (Refer to the "Field" on page 124 for details).
BAC Alert Integration Field	1 Go to **BAC Alert Integration Field** form (for details, see "Maintain the BAC Alert Integration Field" on page 90). 2 Click **Search** to check the data. (Refer to the "Entity" on page 128 for details).
BAC Alert Integration Field Mapping	1 Go to **BAC Alert Integration Field Mapping** form (for details, see "Maintain the Business Availability Center Alert Integration Field Mapping" on page 90). 2 Click **Search** to check the data. (Refer to the "Entity" on page 128 and "Field Mapping" on page 129 for details).
Link Customization	For details, see "Link Customization" on page 93.

5 Modify Business Availability Center Alert Integration Configuration

After the deployment is complete, you can configure the system to fit the customer's system environment.

HP Service Manager retrieves information about the CI Status alerts from Business Availability Center using the CI Alert Retrieval Service. For details, see "CI Alert Retrieval Service API Overview" on page 96.

a Click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Configuration**.

b Set up the CI Alert Retrieval Service API

The URL is used to access Business Availability Center. For details about the URL, see "CI Alert Retrieval Service API Overview" on page 96.

- Enter **bac.cialert.rest.url** in the **Name** box.
- Click **Search** to display the target configuration.
- Modify the value of this configuration to match your own URL. (Change the <**hostname**> to your own **CI Alert Retrieval Service API**)

c Set up the username

This username used to access the CI Alert Retrieval Service.

- Enter **username** in the **Name** field.
- Click **Search** to display the target configuration.
- Modify the value of this configuration. Change **<username>** to the available user name

d Set up the password

The password used to access the CI Alert Retrieval Service.

- Enter **password** in the **Name** field.
- Click **Search** to display the target configuration
- Modify the value of this configuration.
- Change the **<password>** to match the username above.

e Set up the BAC CI Alert Update Time

- Enter **update.time** in the **Name** field.
- Click **Search** to display the target configuration.
- Modify the value of this configuration; this time represents the time when HP Service Manager receives the Business Availability Center alert. Make sure you use the same format as in the original value.

6 Modify BAC Alert Integration Field Mapping

Display the currently-used Mapping ID (default: **SMBACMapping**) on the Configuration page and type the Description as **BAC-SM Mapping ID**.

a Click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Field Mapping**.

b Enter **SMBACMapping** in the **Id** box on the Field Mapping page, and click **Search**.

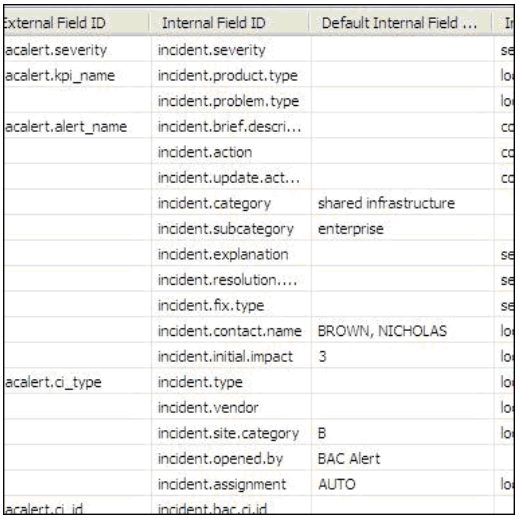
c Locate the cells under the Default Internal Field Value column. They should look like the table below (The default values must be populated, but the values may be different for different version of HP Service Manager.).

d Follow the Comments in the table to Insert/Modify the value. (When the field of a HP Service Manager incident is not matched, the callback function does not return a value, the default listed in the Default Internal Field Value column is used.)

Internal Field ID	Default Internal Field Value (Recommend)	Comments
incident.category	shared infrastructure	Can be changed to another value that exists in HP Service Manager. You can change the default value **shared infrastructure**. The new default value must exist in HP Service Manager. To check if the value exists, select Incident Management >Tools > Categories.
incident.subcategory	enterprise	Can be changed to another value that exists in HP Service Manager. You can change the default value **enterprise**. The new default value must exist in HP Service Manager. To check if the value exists, select Incident Management >Tools > Subcategories.
incident.contact.name		No recommended value. Enter an existing contact name.
incident.initial.impact	3	1-Enterprise 2-Site/Dept 3-Multiple Users 4-User
incident.site.category	B	A-Critical Site B-Major Site, C-Satellite Site D-Home Site, remote-Remote

Internal Field ID	Default Internal Field Value (Recommend)	Comments
incident.opened.by	HP Business Availability Center Alert	Any significant value.
incident.assignment	AUTO	Can be changed to another value that exists in HP Service Manager.

Example



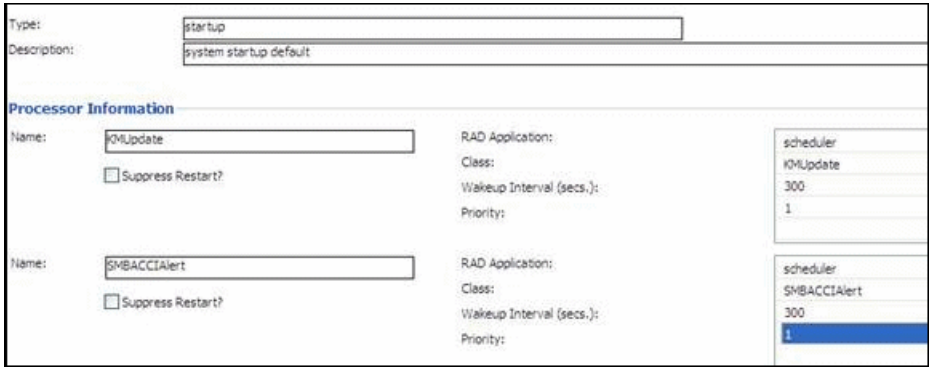
External Field ID	Internal Field ID	Default Internal Field ...	I
acalert.severity	incident.severity		se
acalert.kpi_name	incident.product.type		lo
	incident.problem.type		lo
acalert.alert_name	incident.brief.descri...		cc
	incident.action		cc
	incident.update.act...		cc
	incident.category	shared infrastructure	
	incident.subcategory	enterprise	
	incident.explanation		se
	incident.resolution....		se
	incident.fix.type		se
	incident.contact.name	BROWN, NICHOLAS	lo
	incident.initial.impact	3	lo
acalert.ci_type	incident.type		lo
	incident.vendor		lo
	incident.site.category	B	lo
	incident.opened.by	BAC Alert	
	incident.assignment	AUTO	lo
acalert.ci_id	incident.bac.ci.id		

7 Set Up the SMBAC Scheduler

To make sure the SMBAC scheduler auto-starts/restarts after HP Service Manager stars/restarts, check that scheduler starts at the right time. To do so, type the **info** command in the Service Manager command line, and enter **startup** in the **Type** box. Click **Search**, in the Processor Information area, scroll down to SMBACCIAlert, and check that the data is like in the following table. If needed, click **Add** to save the changes.

Field	Value	Description
RAD application	scheduler	
Class	SMBACCIAlert	The same class as the one in the above table.
Wakeup Interval (Seconds)	300	The time that is converted into seconds by the Repeat Interval field in the table above.
Priority	1	

The Processor Information user interface is as follows:



8 Modify the Language Used to Display the Service Invocation Results

The language you selected for the browser is used to display the Service Invocation results. It causes the CI Alert Retrieval service to retrieve the description and condition description of the alert for this language, from Business Availability Center. If you are not using a browser to display the Service Invocation results, you must specify the requested language in the header of the HTTP request.

You set the supported language in BAC Alert Integration Configuration form: select **System Administration> Base System Configuration > BAC Alert Integration Configuration**, and modify the value of the **Accept-Language** configuration. The default value is **en**.

For details about the languages are supported by Business Availability Center, see "Working in Non-English Locales" in *Reference Information*.

9 Configure the Security – Optional

To ensure the communication security between the CI Alert Retrieval Service (HP Service Manager site) and Business Availability Center CI Alert Retrieval Service web server (Business Availability Center site), the system supports using HTTP over SSL or HTTPS.

The CI Alert Retrieval Service web server URL is contained in the Configuration component.

The HTTP request Header, which is sent to the Business Availability Center CI Alert Retrieval Service Server, includes the username and password for the HTTPS communication which are not needed for HTTP communication.

For additional details, see "Examples of Security Configuration" on page 82.

To support HTTPS communication:

a Generate a public/private key pair with the following keytool, using the following command:
keytool -genkey -keystore sm_keystore.jks -alias sm

You are prompted to type in the password and private key for the keystore, and your last name and first name. You must type in the FQDN (full qualified domain name) of your server when you are prompted for your last name and first name.

b Generate the certificate signing request, using the following command:
keytool -certreq -keystore sm_keystore.jks -alias sm -file sm.csr

c Sign by the Certificate Authority (CA).

- **Sign the certificate by trusted CA.** You must use a trusted CA private key to sign the certificate. You send your own CSR (**sm.csr**) to the trusted CA. It returns a certification as **sm.cer**.

- **Sign the Certificate by the Self-signed CA.** See the "Sign the Certificate by the Self-signed CA (optional)" on page 83 section to get more information.

d Import the CA root certificate to the keystore, using the following command:
keytool -import -file ca.cer -trustcacerts -keystore sm_keystore.jks -alias ca

e Import the **certificate reply** back to key store, using the following command:
keytool -import -file sm.cer -trustcacerts -keystore sm_keystore.jks -alias sm

The alias name used in this command must be the same as the alias name used in the first step so that the signed certificate reply can be paired with the original private key correctly.

Create a directory to hold your key store, for example, **%SM_SERVER%/RUN/security**, and save the **sm_keystore.jks** file in this directory.

f Enable SM SSL Setting

Open sm.ini in the directory where you install the HP Service Manager server, and set the setting as below. For details, see "Parameters Setting in the sm.ini File" on page 116.

```
# SSL configuration
ssl:0
ssl_reqClientAuth:1
sslConnector:1
httpsPort:13443

# Certificates
truststoreFile:security/sm_keystore.jks
truststorePass:password
keystoreFile:security/sm_keystore.jks
keystorePass:password
```

g Restart the HP Service Manager server service. In the HP Service Manager server machine, select **Start** > **Settings** > **Control Panel** > **Administrative tools** > **Services**, and restart HP Service Manager 7.XX Server.

Important:

- If you have already set up HP Service Manager SSL with a certificate signed by the CA trusted by Business Availability Center, you do not need to make changes.
- If you have already set up HP Service Manager SSL with a certificate signed by a CA not trusted by Business Availability Center, you have two choices: to import the CA root certificate to Business Availability Center or to perform the steps above to create a new key pair and sign it with the CA root certificate which Business Availability Center trusts.
- HP Service Manager supports only the JKS format (PKCS12 format is not supported).
- The keystore password and the private key password must be the same.
- The Certificate has an expiry date; make sure you update your certificate periodically.
- Your key store and trust certificate store can be one JKS format store.
- You must specify the FQDN instead of IP address anytime you use HTTPS/SSL.

Examples of Security Configuration

➤ **Generate public/private key pair with keytool:**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>keytool -genkey -keystore sm
_keystore.jks -alias sm

Enter keystore password: vinson
Re-enter new password: vinson
What is your first and last name?
  [Unknown]:  vinson
What is the name of your organizational unit?
  [Unknown]:  hp
What is the name of your organization?
  [Unknown]:  hp
What is the name of your City or Locality?
  [Unknown]:  shanghai
What is the name of your State or Province?
  [Unknown]:  shanghai
What is the two-letter country code for this unit?
  [Unknown]:  cn
Is CN=vinson, OU=hp, O=hp, L=shanghai, ST=shanghai, C=cn?
  [no]:  y
Enter key password for <sm>
(RETURN if same as keystore password):vinson
```

➤ **Generate the certificate signing request**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>keytool -certreq -keystore s
m_keystore.jks -alias sm -file sm.csr
Enter keystore password: vinson
```

➤ **Sign it with the CA**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>openssl x509 -req -days 365
-in sm.csr -out sm.cer -CA ca.cer -CAkey cakey.pem –Cacreateserial

Loading 'screen' into random state - done
Signature ok
subject=/C=cn/ST=shanghai/L=shanghai/O=hp/OU=hp/CN=vinson
Getting CA Private Key
Enter pass phrase for cakey.pem:
```

➤ **Import the CA root certificate to keystore**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>keytool -import -file ca.cer
  -trustcacerts  -keystore sm_keystore.jks -alias ca

Enter keystore password: vinson
Owner: EMAILADDRESS=mail@mail.com, CN=vinson, OU=hp, O=hp, L=hp,
ST=shanghai, C=cn
Issuer: EMAILADDRESS=mail@mail.com, CN=vinson, OU=hp, O=hp, L=hp,
ST=shanghai,C=cn
Serial number: e611ad0fd5bc9e10
Valid from: Fri Oct 10 11:12:39 CST 2008 until Fri Jul 08 11:12:39 CST 2011
Certificate fingerprint:
      MD5: B5:D8:9F:A4:8B:24:70:79:DD:4D:0D:5A:44:12:F1:37
      SHA1: 7B:55:63:95:C7:14:F9:3B:C8:57:B6:81:24:A0:4F:00:78:CD:D1:94
Trust this certificate [no]:  y
Certificate was added to keystore
```

➤ **Import the "certificate reply" back to key store**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>keytool -import -file sm.cer  -
trustcacerts  -keystore sm_keystore.jks -alias sm
Enter keystore password: Vinson
Certificate reply was installed in keystore
```

➤ **Sign the Certificate by the Self-signed CA (optional)**

This step generates the signed certification sm.cer.

➤ Generate the key pairs (private/public key):

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>openssl genrsa -des3 -out
cakey.pem 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus .............+++.............+++e is
65537 (0x10001)
Enter pass phrase for cakey.pem: Vinson
Verifying - Enter pass phrase for cakey.pem: vinson
```

➤ Generate the self-signed CA:

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>openssl req -config
openssl.conf -new -x509 -days 1001 -key cakey.pem -out ca.cer

Enter pass phrase for cakey.pem:
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:cn
State or Province Name (full name) [Some-State]: shanghai
Locality Name (eg, city) []: shanghai
Organization Name (eg, company) [Internet Widgits Pty Ltd]: hp
Organizational Unit Name (eg, section) []: hp
Common Name (eg, YOUR name) []: vinson
Email Address []:mail@mail.com
```

➤ Sign the certificate by the self-signed CA:

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>openssl x509 -req -days 365 -
in sm.csr -out sm.cer -CA ca.cer -CAkey cakey.pem –Cacreateserial

Loading 'screen' into random state – done
Signature ok
subject=/C=cn/ST=shanghai/L=shanghai/O=hp/OU=hp/CN=Vinson
Getting CA Private Key
Enter pass phrase for cakey.pem: vinson
```

Upgrade from the Previous Version of HP Service Manager Integration with Alerts

If you have installed the previous version of the integration of HP Service Manager with Alerts you must perform the following step to upgrade to the new version.

This task includes the following steps:

- "Uninstall the Legacy HP ServiceCenter/HP Service Manager Integration" on page 85
- "Modify the Enable Legacy Integration in Business Availability Center Infrastructure Setting" on page 85

1 Uninstall the Legacy HP ServiceCenter/HP Service Manager Integration

To uninstall the legacy HP ServiceCenter/HP Service Manager integration, proceed as follows:

a Stop the connected service.

b Undeploy the **smbac-1.00.war** from the web server.

c Maybe need manually deleted all of the scripts and tables created by the two unload files.

2 Modify the Enable Legacy Integration in Business Availability Center Infrastructure Setting

Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integrations with other applications**, and locate the **Enable Legacy Integration in Service Manager** entry in the Integrations with other applications - Alerts - Service Manager Integration table. Make sure the value is **false**.

Troubleshooting and Limitations

This section describes how to troubleshoot HP Service Manager deployment.

This section includes the following topics:

Business Availability Center Integration

Problem	Error Message	Root Cause	Solution
Error when performing an HTTP request	Error when doHTTPRequest. Please check the bac.cialert.rest.url in the configuration.	Error when Sending HTTP request to the REST server	Check the configuration of the server URL. Modify URL to the correct URL. The name of this configuration is **bac.cialert.rest.url**
HP Business Availability Center alert feed not found	BAC alert feed not found, please check the Json format of BAC server response.	There is no **feed** attribute in the response file (json) from REST server	Check the json data format. If needed, check the Business Availability Center Server
BACRestClient parse error	BACRestClient parse error; Please check the json data format.	Json data cannot be parsed correctly	Check the json data format. If needed, check the Business Availability Center Server

Problem	Error Message	Root Cause	Solution
HP Business Availability Center fields validation fail	BAC fields validation fail! Please check the mapping settings with data from BAC Server.	The data from Business Availability Center Server is not consistent with mapping settings.	Check the Field Mapping and the Value Mapping.
Cannot find Mapping	Cannot find Mapping in SMBACMapping table with ID.	Mapping ID configured not found in SMBACMapping table.	Check the configuration of the Mapping ID. Modify the Mapping ID wiht the correct Mapping ID. The configuration name is **BAC-SM Mapping ID**.

Security (SSL)

Problem	Error Message	Root Cause	Solution
java.io.IOException: Cannot recover key	java.io.IOException: Cannot recover key at org.apache.tomcat.util.net.jsse.JSSE14SocketFactory.init(JSSE14SocketFactory.java:125).	The key entry password is different from the keystore password.	Make the two passwords consistent.
java.io.IOException: Cannot recover key	java.security.cert.CertificateNotYetValidException: NotBefore.	The server time is not correct. It is not included in the certificate valid time.	Modify the server time to match the certificate valid time.

Manually Install Out-of-Box Unload

All the configurations described in this section are provided by the out-of-box Unload (see "Perform the Automatic Default Configuration" on page 70) and typically require no modifications.

This section's steps serve as a reference and are only required if the Out-of-box Unload is not used or requires modification.

This task includes the following steps:

- "Add a Main Menu" on page 88
- "Add a Details Menu" on page 89
- "Maintain a BAC Alert Integration Entity" on page 89
- "Maintain the BAC Alert Integration Field" on page 90
- "Maintain the Business Availability Center Alert Integration Field Mapping" on page 90
- "Create Schedule" on page 92
- "Link Customization" on page 93

1 Add a Main Menu

This step describes how to add the Main Menu.

a Enter **menu** in the HP Service Manager command line.

b Go to the **Menu** page.

c Enter **SYSTEM ADMINISTRATION** in the **Menu Name** box to search the menu list.

d Add the data in "Main Menu Folder" on page 119 as one record to the **SYSTEM ADMINISTRATION** menu.

e Click **Save**.

The main menu records are as follows:

27	Ongoing Mainten...	Communication Utilities		menu.manager	name	COMM UTILITIES	index("SysAdmin", $lo.ucapex)>0
28	Ongoing Mainten...	System		menu.manager	name	SYSTEM	index("SysAdmin", $lo.ucapex)>0
29	Ongoing Mainten...	Environment Records		menu.manager	name	ENV RECORDS	index("SysAdmin", $lo.ucapex)>0
	Base System Co...	BAC Alert Integration		menu.manager	name	SMBAC Alert Integ...	index("SysAdmin", $lo.ucapex)>0

2 Add a Details Menu

This step describes how to add the Details Menu.

a Type **menu** in the HP Service Manager command line.

b Go to the **Menu** page.

c Type **SMBAC Alert Integration** in the **Menu Name** box, and type **menu.gui.base.bacalert** in the **Format** box.

d Click **Add** button to add this as a new menu.

e Add the data in "Detail Menu Items" on page 119 as the records to the new menu.

f Click **Save**.

The details menu records is as follows:

O..	G	Description	C.	Application	Pa...	Parameter Value	T	Condition
1		BAC Alert Integration Conf...		database	name	SMBACConfiguration		index("SysAdmin", $lo.ucapex)>0
2		BAC Alert Integration Entity		database	name	SMBACEntityType		index("SysAdmin", $lo.ucapex)>0
3		BAC Alert Integration Field		database	name	SMBACField		index("SysAdmin", $lo.ucapex)>0
4		BAC Alert Integration Field...		database	name	SMBACMapping		index("SysAdmin", $lo.ucapex)>0

3 Maintain a BAC Alert Integration Entity

This step describes how to maintain the Entity. For information about the possible values, see "Entity" on page 128.

a Click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Entity**.

b Proceed as follows:

- To add one entity, fill the **ID** and **Description** boxes, select the **BAC Entity** checkbox if necessary, and click **Add**.
- To update/remove one Entity, type the keyword of one or more fields, click **Search** to display the Entities to be updated/removed, modify the fields, and click **Save/Delete**.

4 Maintain the BAC Alert Integration Field

This step describes how to maintain the Field. For information about the possible values, see "Field" on page 193.

Click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Field**:

- To add one field, fill the **ID** and **Description** boxes and click **Add**.
- To update/remove one field, type the keyword of one or more attributes, click **Search** to display the Fields to be updated/removed, modify the attributes, and click **Save/Delete**.

When you select the field type, take into consideration the real data type in file (table). Take the Field with the **incident.citype** id for example, you should check the real data type of the **type** field name in the **probsummary** file (select **System Definition** >**Tables** > **probsummary**) and match the real data type in the table (string, number, date, or Boolean).

The Max string length and multivalue attributes are for future use.

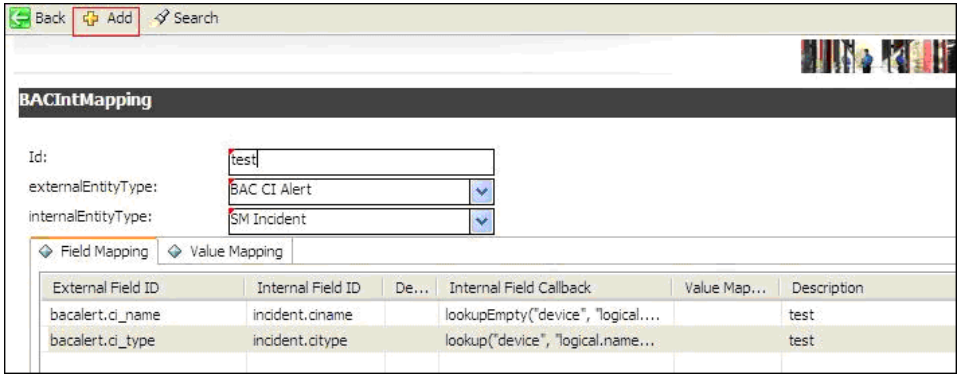
5 Maintain the Business Availability Center Alert Integration Field Mapping

This step describes how to maintain the Field Mapping. For information about the possible values, see "Field Mapping" on page 129 and "Value Mapping" on page 132.

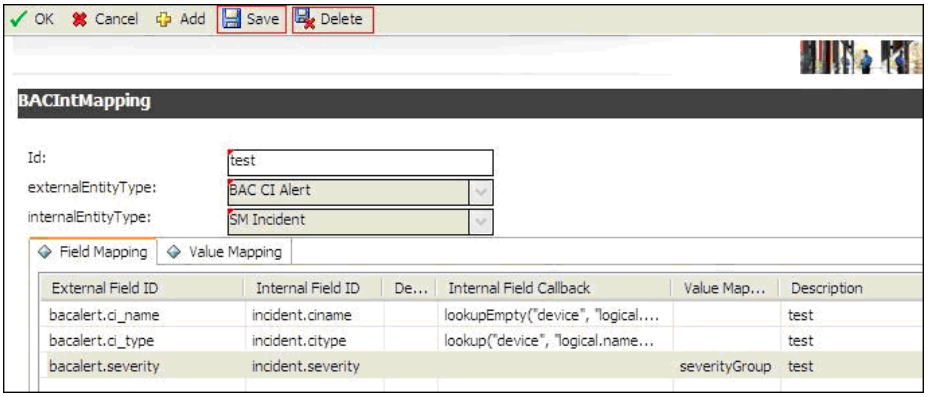
a Click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Field Mapping**.

b Proceed as follows:

- To add one Field Mapping, fill the **Id** box, select one value from the drop list of **externalEntityType** and **internalEntityType**, for the cells in the picture below: select one value in **External Field ID** drop list, select one value in Internal **Field ID**, fill the **Internal Field Callback** and fill the other cells if needed, and click **Add** button to add the new Field mapping.
- To update one Field Mapping, get the target Field Mapping record via search system, modify the any fields value or table cells value, Or add records to the table **Field Mapping** and **Value Mapping**, and click **Save** to save the modification.
- To remove one Field Mapping, get the target **Field Mapping** record via search system, and click **Delete** to remove the modification.
  Example of adding one field mapping:



Example of field mapping:



6 Create Schedule

This step describes how to maintain the Schedule. The schedule is used to start up the process.

Click **Menu Navigation** > **Tailoring** > **Database Manager**, type **schedule.looksee** in the **Form** field, go to the schedule editor, and use the data shown in the following table to setup the schedule:

Field	Default Value	Comments
Name	SMBAC CI Alert Integration	
Class	SMBACCIAlert	
Expiration		Choose a time
Action Time		Choose a time
Description	SMBAC CI Alert Integration	The field is in the Description tab.
Repeat Interval	00:05:00	The field is in the Description tab. It means the schedule runs every 5 minutes.
	var bacClient = new system.library.SMBACAlert Client.SMBACAlertClient(); bacClient.startup();	Enter the value in the Javascript tab.

7 Link Customization

Note: Perform this step if you are working with HP Service Manager 7.02. Skip this step if you are working with other versions.

To update the expression of the **contact.name** field and the two **logical.name** fields as **Source Field Name**:

a Click **Tailoring** > **Tailor Tools** > **Links**.

b Type **probsummary** as the Name and click **Search**.

c Find the line with **contact.name** as the **Source Field Name.**

d Right-click this line and select **SelectLine**.

e Modify the **contact.name** expression.

f Add one clause expression:
;if (nullsub($G.BACAlert, false)=true) then ($fill.recurse=false) else ($fill.recurse=true)

g Use the steps above to modify the expressions of the two **logical.name** fields.

4

CI Alert Retrieval Service

This chapter provides information on the CI Alert Retrieval service.

This chapter includes:

Concepts

Reference

CI Alert Retrieval Service API Overview

The CI Alert Retrieval Service can be used to retrieve information from the Alerts feed where CI Status alerts are stored after they are triggered. You access the service using URLs. The alert information is displayed in HTML, XML, or JSON format.

For details on how to open an incident in HP Service Manager, see "Open Incidents Using the CI Alert Retrieval Service" on page 67.

CI Alert Retrieval Service - Invocation

A typical URL used to invoke the CI Alert Retrieval Service, which retrieves alerts from Business Availability Center, has the following structure:

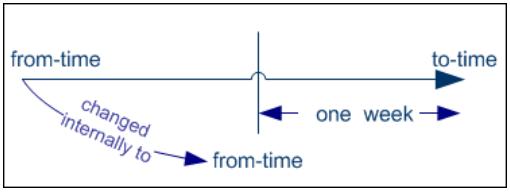
```
http://<host>/topaz/services/<security>/customers/1/alerts/ci?
alt=<alt>&mode=<mode>&ci-id=<ci-id>&extended-info=<extended-info>
&target-type=<target-type>&from-time=<from-time>
&to-time=<to-time>&severity=<severity>
```

Note: In the invocation URL, 1 is the customer ID (Business Availability Center supports more than one customer; the customer with ID=1 is the default client in a regular installation).

Parameters Passed to the Invocation URL

The following parameters are passed to the URL when invoking the CI Alert Retrieval Service:

Parameter Name (A - Z)	Remarks	Mandatory?
alt	Use one of the following media types: ➤ **application/atom%2Bxml** to return the alert information in XML format. ➤ **application/json** to return the alert information in JSON format. ➤ **text/html** to return the alert information in HTML format. For details, see "CI Alert Retrieval Service - Invocation" on page 96. For details on the alert information, see "Content Description" on page 110.	Mandatory
ci-id	Enter the list of CI IDs, separated with commas, that you want to use to filter the service invocation results. **Example:** A6912224862B7F15FC2081, C6612224862B7F15FC20813 To access the ID of a CI, select **Admin** > **Universal CMDB** > **Modeling** > **IT Universe Manager**, right-click the CI and select **Properties**, the CI ID is displayed.	Optional
extended-info	Use one of the following: ➤ **true** to return the CI type and CI Name in the Service Invocation results during additional processing time. ➤ **false** not to return the CI type and CI Name in the Service Invocation results.	Optional **Default:** false

Parameter Name (A - Z)	Remarks	Mandatory?
from-time	Enter the time from which the alerts are returned using the following format: **yyyy-mm-ddThh:mmZGMT_time_zone**. **Example:** 2007-11-15T21:19Z +03:00 **Note:** If the period of time between **from-time** and **to-time** is more than one week, **from-time** is moved to exactly one week before **to-time**. 	Optional **Note:** If you do not specify a value, the default is 24 hours before the current time when the URL is launched but no more than 500 alerts are displayed on a page.
mode	Use: ➤ **serial.** Use this mode when you want the recipient to receive the alerts triggered from the time indicated by the **Updated** field in the last Service Invocation results. The recipient receives the alerts one by one and does not receive alerts from overlapping time periods, after invoking the service. When you use **serial**, you do not have to enter a value for the **to-time** parameter. ➤ **regular.** Default. Use this mode when you want the recipient to receive all the alerts triggered between the **from-time** and **to-time** period.	Mandatory
security	Use: ➤ **technical** when only the super user is allowed to retrieve the alerts. ➤ **business** when user authentication is required and security is handled by LWSSO.	Mandatory
severity	Enter a list of severities, separated with commas, to filter the information returned in the Service Invocation results. For details about the correspondence between the severities and the Business Availability Center statuses, see “Severity and Business Availability Center Status” on page 99.	Optional **Default:** All severities

Parameter Name (A - Z)	Remarks	Mandatory?
target_type	Use: ➤ **Incident.** To return only the alerts marked with the **Open incident in Service Manager** option in the CI Status Alert wizard. ➤ **All.** To return all the alerts.	Optional **Note:** If you do not specify a value, the default is **all**.
to-time	This represents the time after which the alerts are not returned in the Service Invocation results. **Example:** 2007-11-15T21:19Z +03:00	Optional **Note:** If you do not specify a value, the default is the current time when the URL is launched.

Severity and Business Availability Center Status

The correspondence between the HP Service Manager severity and the Business Availability Center status is as follows:

HP Business Availability Center Status	Severity
downtime	-4
stop	-3
no data	-2
uninitialized	-1
critical	0
major	5
minor	10
warning	15
OK	20

CI Alert Retrieval Service User Interface

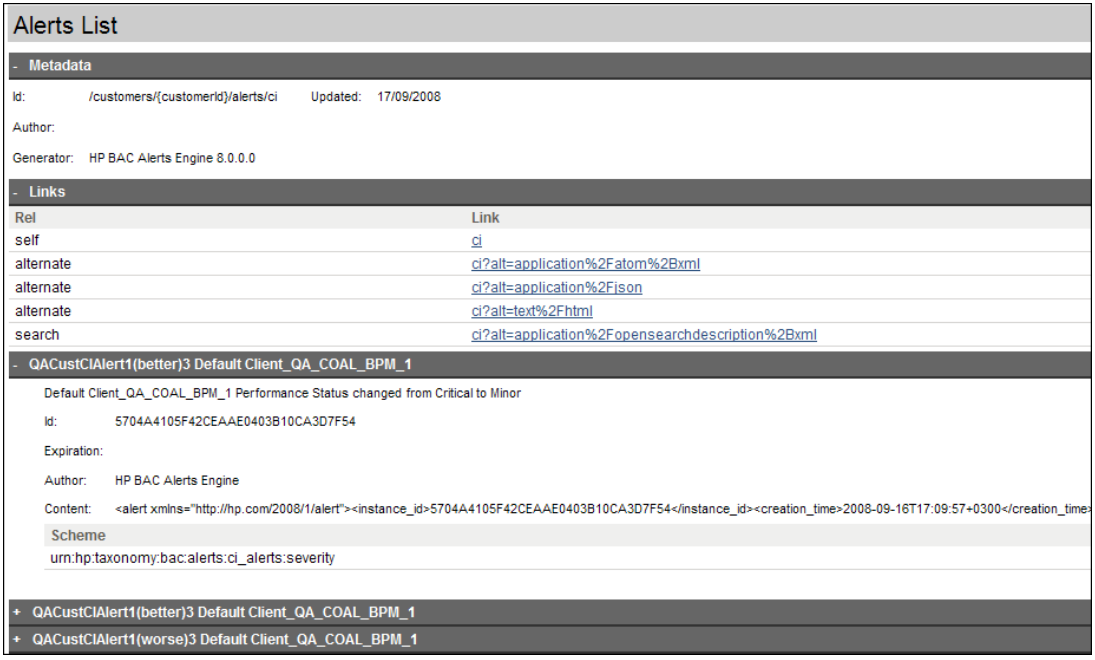
This section describes:

CI Alert Retrieval Service Invocation Report

Description	Displays the results of the CI Alert Retrieval Service Invocation in HTML, XML, or JSON format depending on your selection in the **alt** parameter: **To access:** Invoke the CI Alert Retrieval Service.
Important Information	Example of URLs used to invoke the service: ➤ To display the report in HTML format, use: http://<server>/topaz/services/technical/customers/1/alerts/ci?alt=text%2Fhtml ➤ To display the report in XML format, use: http://<server>/topaz/services/technical/customers/1/alerts/ci?alt=application%2Fatom%2Bxml ➤ To display the report in JSON format, use: http://<server>/topaz/services/technical/customers/1/alerts/ci?alt=application%2Fjson
Included in Tasks	"CI Alert Retrieval Service API Overview" on page 96 "Open Incidents Using the CI Alert Retrieval Service" on page 67
Useful Links	➤ "Opening Incidents in HP Service Manager" on page 50 ➤ "CI Alert Retrieval Service API Overview" on page 96

Report Content in HTML Format

The following is an example of the CI Alert Retrieval Service Invocation in HTML format.



Alerts List

- Metadata

Id: /customers/{customerId}/alerts/ci Updated: 17/09/2008

Author:

Generator: HP BAC Alerts Engine 8.0.0.0

- Links

Rel	Link
self	ci
alternate	ci?alt=application%2Fatom%2Bxml
alternate	ci?alt=application%2Fjson
alternate	ci?alt=text%2Fhtml
search	ci?alt=application%2Fopensearchdescription%2Bxml

- QACustCIAlert1(better)3 Default Client_QA_COAL_BPM_1

Default Client_QA_COAL_BPM_1 Performance Status changed from Critical to Minor

Id: 5704A4105F42CEAAE0403B10CA3D7F54

Expiration:

Author: HP BAC Alerts Engine

Content: <alert xmlns="http://hp.com/2008/1/alert"><instance_id>5704A4105F42CEAAE0403B10CA3D7F54</instance_id><creation_time>2008-09-16T17:09:57+0300</creation_time>

Scheme

urn:hp:taxonomy:bac:alerts:ci_alerts:severity

+ QACustCIAlert1(better)3 Default Client_QA_COAL_BPM_1

+ QACustCIAlert1(worse)3 Default Client_QA_COAL_BPM_1

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<CI_name>	The report includes a <CI_name> section for each CI selected in the CI Alert Retrieval Service invocation. **Note:** The <CI_name> sections are ordered by the alert time of occurrence. This section includes the following information: ➤ **Summary** provides a summary of the reason why the CI Status alert was triggered. ➤ **Id** displays the ID of the alert. ➤ **Expiration** is empty. ➤ **Author** displays the name of the Alerts Engine. ➤ **Content** displays information about the alert. For details about the displayed information, see "Content Description" on page 110. ➤ **Scheme** displays internal information.
Links	This section includes the following links: ➤ **self** provides a link to the OpenSearch description document. ➤ **alternate** provides a link to the current report in XML, HTML, or JSON format. ➤ **search** provides a link to the OpenSearch description document.

GUI Element (A-Z)	Description
Metadata	This section includes general information about the invocation: ➤ **Id.** The permanent URI where the feed can be read. ➤ **Next link.** This field is returned if during the query time period, more alerts exist than the maximum alerts allowed in the response (500). The field is used as a link for paging to the next 500 alerts. ➤ **Author.** For future use. ➤ **Generator.** The version of the Alerts Engine. ➤ **Updated.** The field returns the index of the last alert included in the field (the time when the most recent alert was retrieved from Business Availability Center by HP Service Manager). The next invocation starts retrieving alert information from the time specified in the **Updated** field. If the alert's REST invocation is empty, the **updated** field returns the **from-time** value

Report Content in XML Format

The following is an example of the CI Alert Retrieval Service Invocation in XML format.

```
- <feed xmlns="http://www.w3.org/2005/Atom">
    <id>/customers/{customerId}/alerts/ci</id>
    <updated>2008-09-17T07:46:50+03:00</updated>
    <title type="text" xml:lang="en">Alerts List</title>
    <link href="ci" rel="self" />
    <link href="ci?alt=application%2Fatom%2Bxml" type="application/atom+xml" rel="alternate" />
    <link href="ci?alt=application%2Fjson" type="application/json" rel="alternate" />
    <link href="ci?alt=text%2Fhtml" type="text/html" rel="alternate" />
    <link href="ci?alt=application%2Fopensearchdescription%2Bxml"
      type="application/opensearchdescription+xml" rel="search" />
    <generator uri="/customers/{customerId}/alerts/ci" version="8.0.0.0">HP BAC Alerts
      Engine</generator>
  - <entry>
      <id>5704A4105F42CEAAE0403B10CA3D7F54</id>
      <title type="text" xml:lang="en">QACustCIAlert1(better)3 Default
        Client_QA_COAL_BPM_1</title>
      <category label="Minor" scheme="urn:hp:taxonomy:bac:alerts:ci_alerts:severity" term="10" />
    - <author>
        <name>HP BAC Alerts Engine</name>
      </author>
      <published>2008-09-16T17:09:57+03:00</published>
    - <content type="application/xml">
      - <alert xmlns="http://hp.com/2008/1/alert">
          <instance_id>5704A4105F42CEAAE0403B10CA3D7F54</instance_id>
          <creation_time>2008-09-16T17:09:57+0300</creation_time>
          <kpi_name>Performance</kpi_name>
          <ci_id>a6912224862b7f15fc208132cf1aa6d6</ci_id>
          <severity>10</severity>
          <name>QACustCIAlert1(better)3 Default Client_QA_COAL_BPM_1</name>
          <user_description>FIST Massive CI Alert Creation</user_description>
          <actual_description>CI Performance Status changed from Critical to
            Minor</actual_description>
          <condition_configuration>Status improved</condition_configuration>
        </alert>
      </content>
      <summary type="text" xml:lang="en">CI Performance Status changed from Critical to
        Minor</summary>
    </entry>
  - <entry>
```

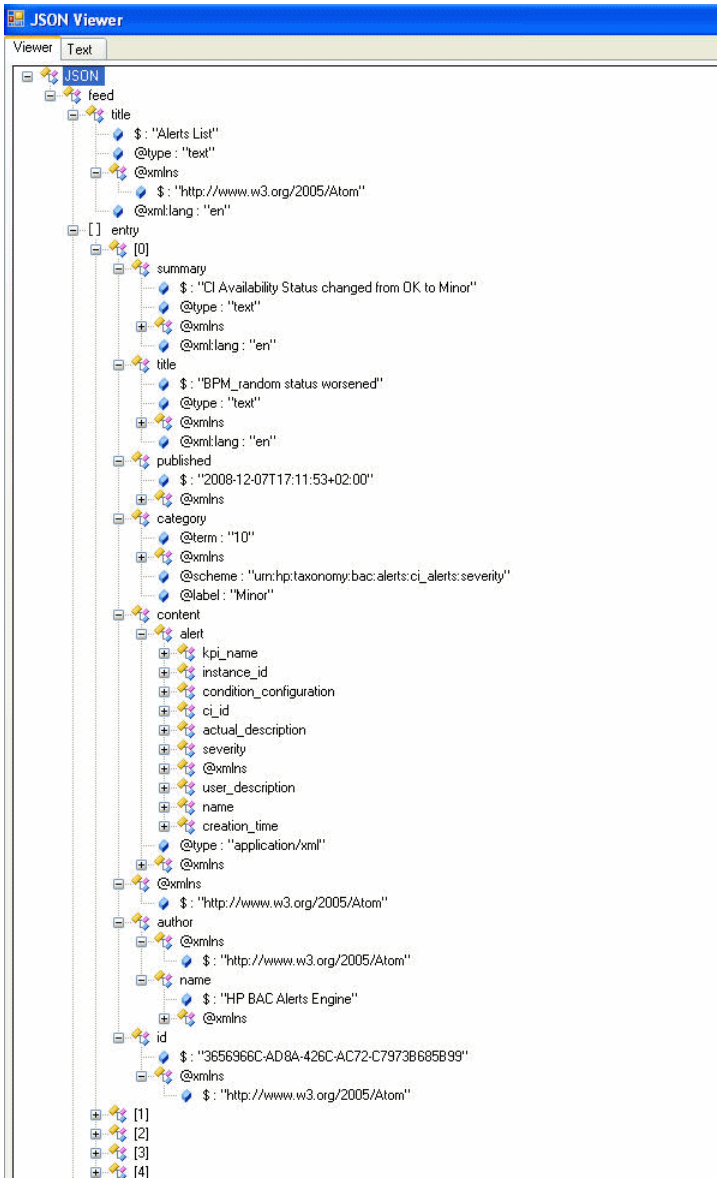
The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<**entry**>	The report includes an <entry> section for each CI selected in the CI Alert Retrieval Service invocation. **Note:** The <entry> sections are ordered by the alert time of occurrence This section includes the following information: ➤ <**id**> displays the ID of the alert instance. ➤ <**title**> displays the alert's name. ➤ <**category**> lists the severity of the alert. For details, see "Severity and Business Availability Center Status" on page 99. ➤ <**scheme**> displays the set of severities that the alert instance may have. ➤ <**author**> displays the name of the Alerts Engine. ➤ <**published**> displays the time when the alert was triggered in Business Availability Center. ➤ <**content**> displays information about the alert. For details about the displayed information, see "Content Description" on page 110. ➤ <**summary**> provides a summary of the condition that occurred and caused the CI Status alert to be triggered.

GUI Element (A-Z)	Description
<first section>	This section includes general information about the invocation: ➤ **<id>** is the id of the report. ➤ **<title>** is always Alerts List. ➤ **Next link** is returned if during the query time period, more alerts exist than the maximum alerts allowed in the response (500). The field is used as a link for paging to the next 500 alerts. ➤ **<generator>** displays the URI and the version and name of the Alerts Engine. ➤ **<updated>** returns the index of the last alert included in the feed (the time when the most recent alert was retrieved from Business Availability Center by HP Service Manager). The next invocation starts retrieving alert information from the time specified in the Updated field. If the invocation is empty, the **<updated>** field returns the value of the **from-time** field. ➤ **<links>.** This section includes the following links: ➤ **rel="self"** provides a link to the OpenSearch description document. ➤ **rel="alternate"** provides a link to the current report in XML, HTML, or JSON format. ➤ **rel="search"** provides a link to the OpenSearch description document.

Report Content in JSON Format

The following is an example of the CI Alert Retrieval Service Invocation in XML format.



The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
"**entry**"	The report includes an "entry" section for each CI selected in the CI Alert Retrieval Service invocation. **Note:** The "entry" sections are ordered by the alert time of occurrence This section includes the following information: ➤ "**id**" displays the ID of the alert instance. ➤ "**title**" displays the alert name. ➤ "**category**" displays the alert severity. ➤ "**author**" is always HP BAC Alerts Engine. ➤ "**published**" displays the time when the alert was triggered in Business Availability Center. ➤ **content** displays information about the alert. For details about the displayed information, see “Content Description” on page 110. ➤ "**summary**" provides a summary of the condition that occurred and caused the CI Status alert to be triggered.

GUI Element (A-Z)	Description
<**first section**>	This section includes general information about the invocation: ➤ "**id**" is the permanent URI where the feed can be read. ➤ "**title**" is always Alerts List. ➤ "**next**" is returned if during the query time period, more alerts exist than the maximum alerts allowed in the response (500). The field is used as a link for paging to the next 500 alerts. ➤ "**generator**" is the version of the Alerts Engine. ➤ "**updated**" returns the index of the last alert included in the field (the time when the most recent alert was retrieved from Business Availability Center by HP Service Manager). The next invocation starts retrieving alert information from the time specified in the Updated field. If the invocation is empty, the "**updated**" field returns the value of the "**from-time**" field. ➤ "**links**". This section includes the following links: ➤ "**rel**":"**self**" provides a link to the OpenSearch description document. ➤ "**rel**":"**alternate**" provides a link to the current report in XML, or HTML format. ➤ "**rel**":"**next**" provides a link to the next page. ➤ "**rel**":"**search**" provides a link to the OpenSearch description document.

Content Description

The alert details section or tag includes the following information:

Element Name (A - Z)	Description
actual_ description	Displays the condition that caused the alert to be triggered. **Example:** Application X status has changed to **Critical** from **Minor**
ci_id	The ID of the CI whose status change triggered the alert. **Example: a6912224862b7f15fc208132cf1aa6d6**
ci_type	The name of the Business Availability Center CI type. HP Service Manager should map it to the appropriate HP Service Manager CI types. For details, see "Mapping of Business Availability Center CI Types to HP Service Manager CI Types" on page 59. **Note:** This is displayed if you selected **extended-info=true**. **Example:** Host, tx_from_location
condition_ configuration	The alert triggering condition that was configured by the user. **Example:** Send alert if CI status worsens
creation_time	The time when the alert was triggered. Depending on the mode you selected, the time when the alert was triggered might be outside of the time range specified in the invocation. **Example:** 2008-09-14T1709:57+03:00
instance_id	The internal ID number of the alert.
kpi_name	The name of the KPI that caused the status change for the CI for which the alert was created. **Example:** Performance
name	The name of the alert as configured by the user.

Element Name (A - Z)	Description
ci_name	The name of the CI whose status change triggered the alert. **Note:** This is displayed if you selected **extended_info=true**. **Example:** Login application
severity	For details about the severities, see "Severity and Business Availability Center Status" on page 99.
user_ description	The description of the alert as it was configured by the Business Availability Center user. **Example:** My alert - restart server when alert occurs.

5

Open Incidents Reference

This chapter provides reference information about the opening of incidents in HP Service Manager, using the CI Alert Retrieval Service, when CI Status alerts are triggered in HP Business Availability Center 8.0.

For details about how to open incidents in HP Service Manager, see "Opening Incidents in HP Service Manager" on page 50.

This chapter includes:

Reference

Business Availability Center Alert/HP Service Manager Incident Correlation Rules

In the Business Availability Center Alert Feed process work flow, rules are used to search, create, update and close incidents.

The rules are configured in the Business Availability Center Alert Integration Configuration page. To access the page, make sure you have installed the out-of-box unload file in the HP Service Manager navigator, and select **System Administration** > **Base System Configuration** > **BAC Alert Integration Configuration**. In the table below, the columns describe the rules:

Configuration Name	Category	Description
Incident.correlation.rule	Rules	The value of this rule is a SQL clause Expression. This configuration is the condition for searching for the incident in HP Service Manager database. **Configurationvalue:** bac.ci.id = "$external.ci_id$" and product.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved"
v1.incident.correlation.rule	Rules	The value of this rule is a SQL clause Expression. This configuration is the condition for searching for the incident in HP Service Manager database. **Configurationvalue:** logical.name = "$external.ci_name$" and problem.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved"

Configuration Name	Category	Description
incident.create.rules	Rules	The value of this rule is a javascript Expression. The numbers (such as 10,20) are the severity value in Business Availability Center Alert, which is mapped in value mapping. $external.severity$ is the reference variable for the severity value This rule means that if the value of the severity equals 0 or 5 or 10 or 15, the rule passes. **Configurationvalue:** $external.severity$ ==0 || $external.severity$ ==5 || $external.severity$ ==10 || $external.severity$ ==15
Incident.create.action	Action	HP Service Manager action. Add a new incident which is translated from Business Availability Center Alert. **Configurationvalue:** addsave
incident.update.rules	Rules	The value of this rule is a javascript Expression. This rule means that if the value of the severity does **not** equal 20, the rule passes. **Configurationvalue:** $external.severity$ ==0 || $external.severity$ ==5 || $external.severity$ ==10 || $external.severity$ ==15
Incident.update.action	Action	HP Service Manager action. Update the existed incident in HP Service Manager via the new related data in Business Availability Center Alert. **Configurationvalue:** save
incident.close.rules	Rules	The value of this rule is a javascript Expression. This rule means that if the value of the severity equals 20, the rule passes. **Configurationvalue:** $external.severity$ ==20
Incident.close.action	Action	HP Service Manager action. Close the existed incident in HP Service Manager via the new related data in Business Availability Center Alert. **Configurationvalue:** close

Where:

- **Configuration Name** provides the internal name of the rule.
- **Category** has two values: Rules and Action. The value of the configuration with the Rules category is the real constraint. The value of the configuration with the Action category is the action (the operation that is performed when the retrieved Alert matches the corresponding rule).
- **Configuration Value** describes the rule condition. If the condition is fulfilled the rule is considered to have **passed**. The rule is considered to have **failed**, if the condition is not fulfilled.
- **Description** describes the rule. Each create, update, or close rule has a corresponding Action configuration. When a rule is considered passed, the corresponding action is performed.

Note: All the variables between dollar ($) signs represent fields in Business Availability Center CI Status alerts. The other variables represent fields in HP Service Manager incidents.

Parameters Setting in the sm.ini File

The table lists the parameters that can be used for SSL. For details, see "Configure the Security – Optional" on page 78.

Parameters	Comments
-ssl: 1	0 = Does not require SSL for SOAP connections, 1=Require SSL for SOAP connections (OPTION)
-sslConnector: 1	0 = Does not load SSL connector, 1 = Load SSL connector. Default is 0 (OPTION)
-ssl_reqClientAuth: n	0 = Does not require client authentication, 1=Do client authentication, 2=Do client authentication and the client has to be a trusted client. (OPTION)
-keystoreFile	Server keystore (OPTION)

Parameters	Comments
-keystorePass	Pass phrase for server keystore. Default value is "changeit" (OPTION)
-truststoreFile	The TrustStore file to use to validate client certificates. Default to the cacerts in the RUN\jre\security directory. (OPTION)
-truststorePass	The pass phrase for the TrustStore file. Default value is "changeit" (OPTION)
-ssl_trustedClientsJKS	A keystore file. This file contains a list of certificates that server trusts (OPTION)
-ssl_trustedClientsPwd	Pass phrase for the trusted client keystore file. (OPTION)

Business Availability Center Setting Parameters

The default settings used in the integration are as follows:

Settings and Details	Default value
Max time to retrieve data from the history The maximum period of time used to retrieve data from the history. **Note:** The maximum period of time is used only when you use a **serial** mode. There is no limit for **regular** mode. The default value can be modified by the HP Software Support.	1 week

Settings and Details	Default value
Max number of rows returned in response The maximum number of rows returned in the Service Invocation results. **Note:** If more than 500 alerts are returned, the following line is added at the end of the report: <link href="ci?alt=application%2Fatom%2Bxml&mode=serial&from-time=2008-08-14T14%3A27%3A52%2B0300&extended-info=false" rel="next/> You can use the link to access the rest of the alert details.	500
Enable legacy ServiceCenter integration	false

Mapping Details

This section describes the data included in the out-of-box unload file used for the customization.

This section includes the following topics:

Main Menu Folder

Option	Description
# Note: Enter a different number than the existing one. When you manually add this record to HP Service Manager, several records are already present.	Business Availability Center Alert Integration (Can be customized) **Group:** Base System Configuration (Can be customized) **Note:** Can be customized in other super menu **Parameter name:** name **Application:** menu.manager **Parameter value:** SMBAC Alert Integration **Condition:** index("SysAdmin", $lo.ucapex)>0

Detail Menu Items

Option	Application	Description
1	database	Business Availability Center Alert Integration Configuration (Can be customized) **Default value:** name **Additional information:** SMBACConfiguration **Condition:** index("SysAdmin", $lo.ucapex)>0
2	database	Business Availability Center Alert Integration Entity (Can be customized) **Default value:** name **Additional information:** SMBACEntityType **Condition:** index("SysAdmin", $lo.ucapex)>0

Option	Application	Description
3	database	Business Availability Center Alert Integration Field (Can be customized) **Default value:** name **Additional information:** SMBACField **Condition:** index("SysAdmin", $lo.ucapex)>0
4	database	Business Availability Center Alert Integration Field Mapping (Can be customized) **Default value:** name **Additional information:** SMBACMapping **Condition:** index("SysAdmin", $lo.ucapex)>0

Configuration

Field Name (A-Z)	Application	Description
Accept-Language	Header	Business Availability Center Request Language Setting (Can be customized) **Default value: en**
Bac.cialert.rest.url	Basic	REST WebService URL (CI Alert Retrieval Service API) (Can be customized) **Default value:** http://<hostname>/topaz/services/technical/customers/1/alerts/ci **Additional information:** Hostname should be changed to Business Availability Center Rest web service URL.
http.conn.timeout	General	Http Connection Timeout Setting (Can be customized) **Default value:** 30 (Can be customized)
http.rec.timeout	General	Http Receive Timeout Setting (Can be customized) **Default value:** 30 (Can be customized)
http.send.timeout	General	Http Send Timeout Setting (Can be customized) **Default value:** 30 (Can be customized)

Field Name (A-Z)	Application	Description
Incident.close.action	Action	Business Availability Center Incident Close Action (Can be customized) **Default value:** close
incident.close.rules	Rules	Business Availability Center Incident Close Rule Condition (Can be customized) **Default value:** $external.severity$ ==20 **Additional information: $external.severity$** is the value of the **severity** field in Business Availability Center Alert This expression follows the **JavaScript** grammar.
incident.corelation.rule	Rules	Incident correlation rule (Can be customized) **Default value:** bac.ci.id = "$external.ci_id$" and product.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved" **Additional information:** This expression follows the **SQL clause** grammar. This configuration is the condition for searching the incident in DB
Incident.create.action	Action	Business Availability Center Incident Creation Action (Can be customized) **Default value:** addsave
incident.create.rules	Rules	Business Availability Center Incident Creation Rule Condition (Can be customized) **Default value:** $external.severity$ ==0 || $external.severity$ ==5 || $external.severity$ ==10 || $external.severity$ ==15 **Additional information:** This expression follows the **JavaScript** grammar.
Incident.update.action	Action	Business Availability Center Incident Update Action (Can be customized) **Default value:** save

Field Name (A-Z)	Application	Description
incident.update.rules	Rules	Business Availability Center Incident Update Rule Condition (Can be customized) **Default value:** $external.severity$ ==0||&external.severity$==5\|\|$external.severity$ ==15 **Additional information:** This expression follows the **JavaScript** grammar.
json.feed.path	General	Business Availability Center Response Json Feed Path (Can be customized) **Default value:** content.alert
logging.level	General	HP Service Manager Business Availability Center Logging Level (Can be customized) **Default value:** INFO (Can be customized) **Additional information:** The candidate values are DEBUG,INFO,WARN,ERROR,OFF
mappingId	General	Business Availability Center-HP Service Manager Mapping ID (Can be customized) **Default value:** SMBACMapping (Can be customized) **Additional information:** It can be changed according to the mapping ID in FieldMapping table.
password	Header	Password (Can be customized) **Default value:** <Password> (Must be customized)
retry.times	General	Queue Retry Times (Can be customized) **Default value:** 2 (Can be customized)
updated.time	General	Business Availability Center CI Alert Update Time **Note:** Can be customized **Default value:** 2001-11-11T13:09:16+0800 (Can be customized) **Additional information:** It usually should not be updated by customer.

Field Name (A-Z)	Application	Description
user	Header	User Name (Can be customized) **Default value:** <user> (Must be customized) **Additional information:** The account of the REST Web Service. Set the checkbox **Is Password** to **true** for the Password configuration.
v1.incident. corelation.rule	Rules	Incident correlation rule when using the legacy URL (Can be customized) **Default value:** logical.name = "$external.ci_name$" and problem.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved" **Additional information:** This expression follows the **SQL clause** grammar. This configuration is the condition for searching the incident in DB (Only when using the legacy URL data)
version	General	Business Availability Center CI Alert and HP Service Manager Incident Submission Integration Version (Can be customized) **Default value:** 01.00.001 **Additional information:** The version of the current build

Field

Primary key indicates that the customization data is part of the key words needed to identify the alert. This setting is used to fields of the BAC CI Alert type.

Required means that the field must be populated in the Field Mapping. This setting is used to fields of the BAC CI Alert type.

ID (A-Z)	Entity Type	Description
bacalert. actual_description	BAC CI Alert	Actual Description (can be customized) **Field Name:** actual_description **Field Type:** string
bacalert.alert_name	BAC CI Alert	Alert name (can be customized) **Field Name:** name **Field Type:** string
bacalert.ci_id	BAC CI Alert	CI Alert ID (can be customized) **Note:** Primary Key **Field Name:** ci_id **Field Type:** string
bacalert.ci_name	BAC CI Alert	CI Alert Name (can be customized) **Field Name:** ci_name **Field Type:** string
bacalert.ci_type	BAC CI Alert	CI Alert Type (can be customized) **Field Name:** ci_type **Field Type:** string
bacalert.condition_ configuration	BAC CI Alert	Condition Configuration (can be customized) **Field Name:** condition_configuration **Field Type:** string
bacalert.creation_ time	BAC CI Alert	Creation Time (can be customized) **Field Name:** creation_time **Field Type:** string

ID (A-Z)	Entity Type	Description
bacalert.kpi_name	BAC CI Alert	KPI Name (can be customized) **Note:** Primary Key **Field Name:** kpi_name **Field Type:** string
bacalert.severity	BAC CI Alert	Severity (can be customized) **Field Name:** severity **Field Type:** string
bacalert.user_ description	BAC CI Alert	User Description (can be customized) **Field Name:** user_description **Field Type:** string
incident.action	SM Incident	Action (can be customized) **Field Name:** action **Field Type:** string
incident. assignment	SM Incident	Assignment (can be customized) **Field Name:** assignment **Field Type:** string
incident.bac.ci.id	SM Incident	Business Availability Center CI Alert ID (can be customized) **Note:** Primary Key **Field Name:** bac.ci.id **Field Type:** string
incident.brief. description	SM Incident	Brief Description (can be customized) **Field Name:** brief.description **Field Type:** string
incident.category	SM Incident	Category (can be customized) **Field Name:** category **Field Type:** string

ID (A-Z)	Entity Type	Description
incident.ciname	SM Incident	CI Name (can be customized) **Field Name:** logical.name **Field Type:** string
incident.citype	SM Incident	CI Alert Type (can be customized) **Field Name:** type **Field Type:** string
incident.contact.name	SM Incident	Contact Name (can be customized) **Field Name:** contact.name **Field Type:** string
incident.explanation	SM Incident	Explanation (can be customized) **Note:** Multivalue **Field Name:** explanation **Field Type:** string
incident.fix.type	SM Incident	Fix Type (can be customized) **Field Name:** fix.type **Field Type:** string
incident.initial.impact	SM Incident	Initial Impact (can be customized) **Field Name:** initial.impact **Field Type:** string
incident.opened.by	SM Incident	Opened by (can be customized) **Field Name:** opened.by **Field Type:** string
incident.problem.type	SM Incident	Problem type (can be customized) **Field Name:** problem.type **Field Type:** string

ID (A-Z)	Entity Type	Description
incident.product.type	SM Incident	HP Service Manager Incident Product Type (can be customized) **Note:** ➤ Primary Key ➤ Required **Field Name:** Product.type **Field Type:** string
incident.resolution	SM Incident	Resolution (can be customized) **Note:** Multivalue **Field Name:** resolution **Field Type:** string
incident.resolution.code	SM Incident	Resolution Code (can be customized) **Field Name:** resolution.code **Field Type:** string
incident.severity	SM Incident	Severity (can be customized) **Field Name:** severity **Field Type:** string
incident.site.category	SM Incident	Site Category (can be customized) **Field Name:** site.category **Field Type:** string
incident.subcategory	SM Incident	Sub Category (can be customized) **Field Name:** subcategory **Field Type:** string
incident.type	SM incident	Type (can be customized) **Field Name:** type **Field Type:** string

ID (A-Z)	Entity Type	Description
incident.update.action	SM Incident	Update Action (can be customized) **Field Name:** update.action **Field Type:** string
incident.vendor	SM Incident	Vendor (can be customized) **Field Name:** vendor **Field Type:** string

Entity

ID	Description	Business Availability Center Entity
SM Incident	Incident Entity in HP Service Manager Note: Can be customized.	
BAC CI Alert	CI Alert Entity in Business Availability Center Note: Can be customized.	Y

Field Mapping

External Field ID	Internal Field ID	Description
bacalert.ci_name	incident.ciname	Lookup CI in device table. If found, set "logical.name" field (that is SM CI name). If lookup fails, set it empty **Note:** Can be modified **Internal Field Callback:** lookupEmpty("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "logical.name")
bacalert.severity	incident.severity	Translate Business Availability Center alert severity to HP Service Manager Incident severity value **Note:** Can be modified **Value Mapping Group:** severityGroup **Internal Field Callback:** setValue("insert|update")
bacalert.kpi_name	incident.product.type	Lookup product type. Create new product type record if it fails. **Note:** Can be modified **Internal Field Callback:** lookupCreate("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"$incident.category$\" and subcategory =\"$incident.subcategory$\"", "product.type", ["product.type", "category", "subcategory"], ["$bacalert.kpi_name$","$incident.category$","$incident.subcategory$"])
	incident.problem.type	Lookup problem type. Create new problem type record if it fails. **Note:** Do not modify **Internal Field Callback:** lookupCreate("problemtype", "product.type=\"$bacalert.kpi_name$\" and problem.type=\"$bacalert.kpi_name$\" and limited.given.level2 =\"$incident.subcategory$\"", "problem.type", ["product.type", "problem.type", "limited.given.level2"], ["$bacalert.kpi_name$","$bacalert.kpi_name$","$incident.subcategory$"])

External Field ID	Internal Field ID	Description
bacalert.alert_ name	incident.brief. description	Combine "name" and "actual_description" fields from Business Availability Center Alert **Note:** Can be modified **Internal Field Callback:** combine(["bacalert.alert_name", "bacalert.actual_description"], false, " : ")
	incident.action Note: Do not modify	Combine "name" and "actual_description" fields from Business Availability Center Alert **Note:** Do not modify **Internal Field Callback:** combine(["bacalert.creation_time", "bacalert.alert_name", "bacalert.actual_description", "bacalert.user_description", "bacalert.condition_configuration"], true, "\n") **Note:** Do not modify
bacalert.ci_id Note: Do not modify	incident.bac.ci.id Note: Do not modify	Customized by user.
	incident.category	Customized by user.
	incident.subcateg ory	Customized by user.
	incident. resolution	In 'close' action, set value with BAC Alert "actual_description" field. **Note:** Can be modified **Internal Field Callback:** setValue("close", "$bacalert.actual_description$") **Note:** Do not modify
	incident.resoluti on.code	In 'close' action, set default value **Note:** Can be modified **Internal Field Callback:** setValue("close", "User Closure")

External Field ID	Internal Field ID	Description
	incident.fix.type	In 'close' action, set default value **Note:** Can be modified **Internal Field Callback:** setValue("close","permanent")
	incident.contact.name	Lookup SM CI info. If not found, set default value **Note:** Can be modified **Internal Field Callback:** lookup("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "contact.name")
	incident.initial.impact	Lookup SM product type info. If not found, set default value **Note:** Can be modified **Internal Field Callback:** lookup("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"$incident.category$\" and subcategory =\"$incident.subcategory$\"", "severity")
bacalert.ci_type Note: Do not modify	incident.type Note: Do not modify	Lookup SM CI info. If not found, set value from Business Availability Center Alert field **Note:** Can be modified **Internal Field Callback:** lookup("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "type") **Value Mapping Group:** citypeGroup **Note:** Do not modify
	incident.vendor	Lookup HP Service Manager CI info. If not found, leave it empty **Note:** Can be modified **Internal Field Callback:** lookup("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "vendor")

External Field ID	Internal Field ID	Description
	incident.site. category	Lookup HP Service Manager CI info. If not found, set default value **Note:** Can be modified **Internal Field Callback:** lookup("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "site.category")
	incident.opened. by	Customized by user.
	incident. assignment	Lookup HP Service Manager product type info. If not found, set default value **Note:** Can be modified **Internal Field Callback:** lookup("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"$incident.category$\" and subcategory =\"$incident.subcategory$\"", "assignment")
	incident.closing. comments Note: Do not modify	**Internal Field Callback:** setValue("close", "Creation time: $bacalert.creation_time$\nAlert Name: $bacalert.alert_name$\nActual Description: $bacalert.actual_description$\nUser Description: $bacalert.user_description$\nCondition Configuration: $bacalert.condition_configuration$") **Note:** Do not modify

Value Mapping

Value Mapping Group	External Value	Internal Value
severityGroup	0	1
	5	2
	10	3
	15	4

Value Mapping Group	External Value	Internal Value
citypeGroup	business_service_for_catalog	bizservice
	logical_application	application
	host	computer
	nt	computer
	unix	computer

Callback Functions

This section describes the functions that are invoked to assign values to the fields in HP Service Manager.

This section includes the following topics:

Lookup Function

Method Name:	Lookup		
Description:	Searches the table specified by the first parameter of the function using the search condition. If a matching condition is found, is uses the value of the field. If the search sails, it uses the predefined default values.		
Input Parameters:	**Type**	**Name**	**Description**
	String	filename	File name to query, for example "device"
	String	query	Search condition
	String	fieldname	The field to retrieve value.

Return:	None
Example:	lookup ("device", "ucmdb.id = \"$ bacalert.ci_id \"$ || logical.name=\"$bacalert.ci_name$\"", "contact.name")
	If "bacalert.ci_id" is "1111111", and "bacalert.ci_name" is "bpm3", the lookup function uses the following query [ucmdb.id = "1111111" || logical.name = "bpm3"] to search the device table. The query [ucmdb.id = "1111111"] is run first. If the table includes this value, the condition [logical.name = "bpm3"] is ignored. If the table does not include this value, the function uses the following query [logical.name = "bpm3"]. If the table includes this value, "contact.name" field is given the value of the current field in incident. If the table does not include this value, "contact.name" is assigned the default value.

LookupCreate Function

Method Name:	LookupCreate		
Description:	Searches the database table using the search condition behaving like the Lookup function. If it does not find a matching record, a new item is created.		
Input Parameters:	**Type**	**Name**	**Description**
	String	filename	File name to query, for example "device"
	String	query	Search condition
	String	fieldname	The field to retrieve value.
	Array	fieldArray	If lookup fails, this parameter is used to create a new item. This array contains the fields to be set value when creating new instance.
	Array	valueArray	If lookup fails, this parameter is used to create a new item. This array contains value when creating new instance.

Return:	None
Example:	lookupCreate ("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"shared infrastructure\" and subcategory =\"enterprise\"", "product.type", ["product.type", "category", "subcategory"], ["$bacalert.kpi_name$","shared infrastructure","enterprise"])
	If "bacalert.kpi_name" is "Performance", this function uses the [product.type="Performance" category="shared infrastructure" subcategory ="enterprise"] query to search in the producttype table. If a corresponding record is found, it sets the value of "product.type" field to current field in the incident. If the search fails, it creates a new product type following the rule below. Value for field "product.type" in incident is "Performance"; Value for this "category" in incident is "shared infrastructure"; Value for field "subcategory" in incident is "enterprise".

LookupEmpty Function

Method Name:	LookupEmpty		
Description:	Searches the device table using the search condition behaving like the Lookup function. If it finds a matching record in the device table, the field is to set to an empty value whether the “default value” has been defined or not.		
Input Parameters:	**Type**	**Name**	**Description**
	String	filename	File name to query, for example "device"
	String	query	Search condition
	String	fieldname	The field to retrieve value.
Return:	None		
Example:	lookupEmpty ("device", "logical.name=\"$bacalert.ci_name$\"", "logical.name")		
	If "bacalert.ci_name" is "bpm3", this function uses the [logical.name = "bpm3"] query to search the device table. If a matching record is found, the value of "logical.name" is changed to the current field in the incident. If the seach fails, the value of "logical.name" is set to an empty value independently of the default value or of the value passed from Business Availability Center.		

setValue Function

Method Name:	setValue		
Description:	The function inserts, updates, or close using the specified value. If you do not specify a value, the default value is used.		
Input Parameters:	**Type**	**Name**	**Description**
	String	action	Action type ("insert"/"update"/"close"), it may be a combination of the types. For example: "insert|update"
	String	Value	Value to be used. If this parameter is missing, the value from Business Availability Center or default value is used.
Return:	None		
Example:	Example 1: setValue ("close", "$bacalert.actual_description$") Example 2: setValue("close|update", "description");		
	1. If "bacalert.actual_description" is "brief description"; the function is setValue ("close", "brief description") 2. Only when the action is insert or update, the value from external field (Business Availability Center) or the default value is used.		

combine Function

Method Name:	combine		
Description:	This function combines the fields in the input parameters into the HP Service Manager field.		
Input Parameters:	**Type**	**Name**	**Description**
	Array	fieldArray	Fields to combine
	boolean	hasTitle	Whether contain title for each field. The title is the description for each field.
	String	splitStr	The space mark
Return:	String, the combined string with the parameters.		

Example:	Combine (["bacalert.alert_name", "bacalert.actual_description"], false, "| ")
	If "bacalert.alert_name" is "**alert name**", and "bacalert.actual_description" is "**Alert Name**" (where description is one of the properties of the Alert Name field and the value of the "bacalert.actual_description" property is "**brief description**"), the result of this function is: **alert name| brief description** If the parameter **hasTitle** is TRUE, the result is: **Alert Name: alert name| Actual Description: brief description**

6

Open Incidents in HP Service Manager Using the Legacy URL

This chapter provides information on opening incidents in HP Service Manager using the legacy URL when CI Status alerts are triggered in HP Business Availability Center 8.0.

Note: HP Business Availability Center integrates with both HP ServiceCenter and HP Service Manager though only HP Service Manager is mentioned in this chapter. For details about the supported versions, see "Opening Incidents in HP Service Manager" on page 50.

This chapter includes:

Concepts

Tasks

Incidents Opened in HP Service Manager by CI Status Alerts Using the Legacy URL

You can automatically open an incident in HP Service Manager when a CI Status alert is triggered.

Data about the alert is passed to HP Service Manager and used to open incidents identified by the CI Name. Those parameters are among the parameters passed to HP Service Manager by the alert. An incident previously opened is updated with new alert data when a CI Status is triggered with the same identifying information.

The incident is opened in HP Service Manager using a URL that is sent to HP Service Manager from Business Availability Center.

The URL has the following format:
<protocol_type>://<ServiceCenter_host_name>:<port>/<directory_path>?ciname=<<CI_name>>&alertname=<<alert_name>>&triggertime=<<trigger_time>>&currstatus=<<current_status>>&prevstatus=<<Previous Severity Description>>&kpiname=<<KPI_name>>&kpivalue=<<KPI_value>>

You must specify some of the parameters and optionally modify the defaults of other parameters. The alert-related parameters (**CI_name**, **alert_name**, **trigger_time**, **current_status**, **previous_status, KPI_name**, and **KPI_value)** are provided by the alert.

In HP Service Manager, you can keep track of the system status and handling. You can also validate and monitor the alert.

For details on how to automatically create an incident in HP Service Manager, see “Open an Incident in HP Service Manager Using the Legacy URL” on page 141.

Open an Incident in HP Service Manager Using the Legacy URL

To automatically open an incident in HP Service Manager using the legacy URL, when a CI Status is triggered in Business Availability Center, follow the steps described in this section.

For details about the mechanism used to open an incident in HP Service Manager when a CI Status alert is triggered, see "Incidents Opened in HP Service Manager by CI Status Alerts Using the Legacy URL" on page 140.

This task includes the following steps:

1 Specify the Name of the HP Service Manager Host

To specify the name of the host where HP Service Manager is located (**ServiceCenter host name** parameter), select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and enter the name of the host in the **ServiceCenter host name** entry in the Integration with other applications - ServiceCenter Integrations table.

2 Specify the Protocol to be Used For the Interface

To specify the protocol to be used for the interface between the Alerts application and the HP Service Manager application, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and enter the protocol (either **http** or **https**) in the **Protocol type** entry in the Integration with other applications - ServiceCenter Integrations table.

3 Specify the Hidden Parameters – Optional

You can change the hidden parameters to match the new information, if, for example, HP Service Manager changes the path to their directories or the port dedicated to listening to Business Availability Center alerts.

Optionally, you can also add parameters to the URL.

To change the hidden parameters or to add parameters to the URL, contact HP Software Support.

4 Add the Open ticket in ServiceCenter Option in the CI Status Alert Wizard

To add the **Open ticket in ServiceCenter** option in the CI Status Alert wizard, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and locate the **Enable alerts to ServiceCenter** entry in the Integration with other applications - ServiceCenter - Alert Integration table. Specify **true** to add the **Open ticket in ServiceCenter** option to the CI Status Alert wizard or **false** to remove the option.

5 Enable the Legacy URL to Open Incidents in HP Service Manager

To enable the legacy URL to open incidents in HP Service Manager, you must set the **Enable legacy integration with Service Manager** parameter to **true** and the **Enable url action for opening incident in Service Manager** parameter to **true**.

To set the parameters to **true**, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and in the Integrations with other applications - Alerts-Service Manager Integration table, locate:

- the **Enable legacy integration with Service Manager** entry, and change the value to **true**.
- the **Enable url action for opening incident in Service Manager** entry, and change the value to **true**.

6 Define CI Status Alerts

Define CI status alerts. For details, see "Create a CI Status Alert Scheme and Attach it to a CI" on page 65.

7 Enable the Open ticket in ServiceCenter Option in the CI Status Alert Wizard

While defining the CI Status alerts, select the **Open ticket in ServiceCenter** option in the CI Status Alert wizard to automatically sent CI Status to ServiceCenter when the CI Status alert is triggered.

For details about the option for the CI Status alert, see "Actions Page" on page 98.

8 Result

When a CI Status alert is triggered in Business Availability Center, a corresponding incident is opened in HP Service Manager. For details, see "Incidents Opened in HP Service Manager by CI Status Alerts Using the Legacy URL" on page 140.

Part III

Problem Isolation

7

Problem Isolation and HP Service Manager Integration

This chapter includes the main concepts, tasks, and reference information for the integration of Problem Isolation and HP Service Manager.

This chapter includes:

Concepts

Tasks

Problem Isolation and HP Service Manager Integration

You can integrate Problem Isolation with HP Service Manager to link isolation data (from Problem Isolation) with incident or problem data (from HP Service Manager), to create a complete problem management lifecycle. To integrate the two applications, you must configure the connectivity settings between them. For details on how to perform this task, see "Configure Problem Isolation and HP Service Manager Integration" on page 150. For an overview of the integration between Business Availability Center and HP Service Manager, see "HP ServiceCenter and HP Service Manager Integration Overview" in *Solutions and Integrations*.

Note: You can also integrate Problem Isolation with HP ServiceCenter. All references to HP Service Manager in this section and in the relevant user interface pages are also applicable to HP ServiceCenter.

When Problem Isolation and HP Service Manager are integrated, you can do the following:

- When isolating a problematic CI in Problem Isolation, link the isolation details to an existing HP Service Manager incident or problem. For details on the user interface, see "Isolation History Page" on page 85.
- When isolating a problematic CI in Problem Isolation, create a new HP Service Manager incident or problem and link the isolation details to it. For details on the user interface, see "Isolation History Page" on page 85.
- In Problem Isolation, upload the Problem Snapshot report, which contains data about suspect CIs, on-demand monitor results, changes for a problematic CI, and HP Operations Orchestration run books invoked on suspect CIs, to an HP Service Manager incident or problem. For details on the user interface, see "Problem Snapshot Report" on page 129.
- View basic information from an HP Service Manager incident or problem in a problematic CI's isolation properties. For details on the user interface, see "Properties Pane" on page 89.

➤ From an HP Service Manager incident or problem, isolate a CI in Problem Isolation. For details on the user interface, see "Problem Isolation Entry Page for HP Service Manager" on page 122.

Note:

➤ For details on working in HP Service Manager, see the HP Service Manager documentation.

➤ You can collect performance and availability data from an existing HP ServiceCenter Server and view the data in HP Business Availability Center applications. For details on this topic, see "HP ServiceCenter and HP Service Manager Integration Overview" in *Solutions and Integrations*.

Configure Problem Isolation and HP Service Manager Integration

This task describes how to configure the integration between Problem Isolation and HP Service Manager. For an overview of the integration between Business Availability Center and HP Service Manager, see "HP ServiceCenter and HP Service Manager Integration Overview" in *Solutions and Integrations*.

This task includes the following steps:

1 Configure URLs for the Integration in HP Service Manager

This step is performed for both the integration of Business Availability Center with HP Service Manager and Problem Isolation with HP Service Manager. For details, see "Configure URLs for the Integration" in *Solutions and Integrations*.

2 Configure the Symphony Adapter for HP Service Manager

This step is performed for both the integration of Business Availability Center with HP Service Manager and Problem Isolation with HP Service Manager. For details, see "Configure the Symphony Adapter for HP Service Manager" in *Solutions and Integrations*.

3 Modify the application-context.xml File

This step is performed for both the integration of Business Availability Center with HP Service Manager and Problem Isolation with HP Service Manager. For details, see "Modify the application-context.xml File" in *Solutions and Integrations*.

4 Configure Connection Settings in Business Availability Center

To configure the connection settings from Problem Isolation to HP Service Manager, in Business Availability Center select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integrations with other applications**, and modify the values of the following entries in the **Problem Isolation-ServiceCenter Integration** table:

- **HP ServiceCenter UI endpoint URL.** The URL used to access the HP Service Manager Web server from Problem Isolation. Enter the URL in the format: http://<fully qualified server name>:<port>/SymphonyAdapter/ui.
- **HP ServiceCenter Web services endpoint URL.** The URL used to access the HP Service Manager Web services from Problem Isolation. Enter the URL in the format: http://<fully qualified server name>:<port>/SymphonyAdapter/inbound/ws.
- **HP ServiceCenter Web services timeout (milliseconds).** The connection timeout for HP Service Manager Web services.

5 Load the Integration Tailoring Material

HP Service Manager uses a proprietary binary file format known as **unload files** to contain packages of scripts, forms, file records, and other materials. By convention, these files have a file type of **.unl** on Windows platforms.

a Copy the UNL file required for integration.

- For HP ServiceCenter 6.2.1 and above, copy the file located at: **<ServiceCenter_installation_DVD>\BACUnload\BAC_PI_62_v(X).unl** to an accessible network location.
- For HP Service Manager 7.0 and above, unzip the following file: **<Service_Manager_installation_DVD>\AppUnloads\7.02unloads.zip** and copy the file is **BAC_PI_70_v(X).unl** to an accessible network location.

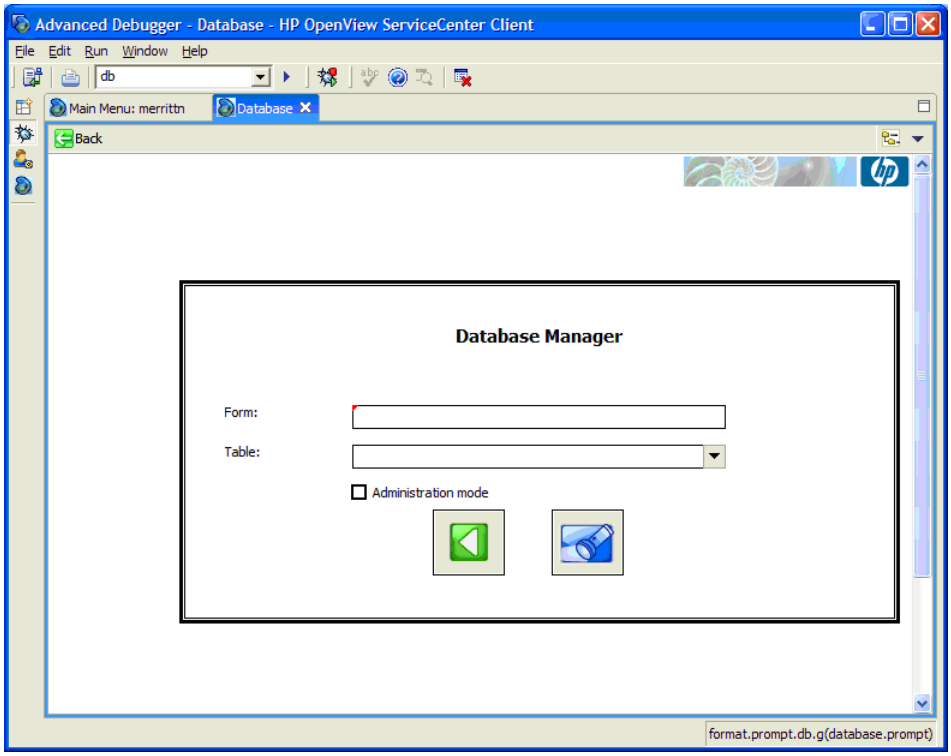
  Note: This step is not needed for HP Service Manager 7.01 and later.

b In the Windows client, select:

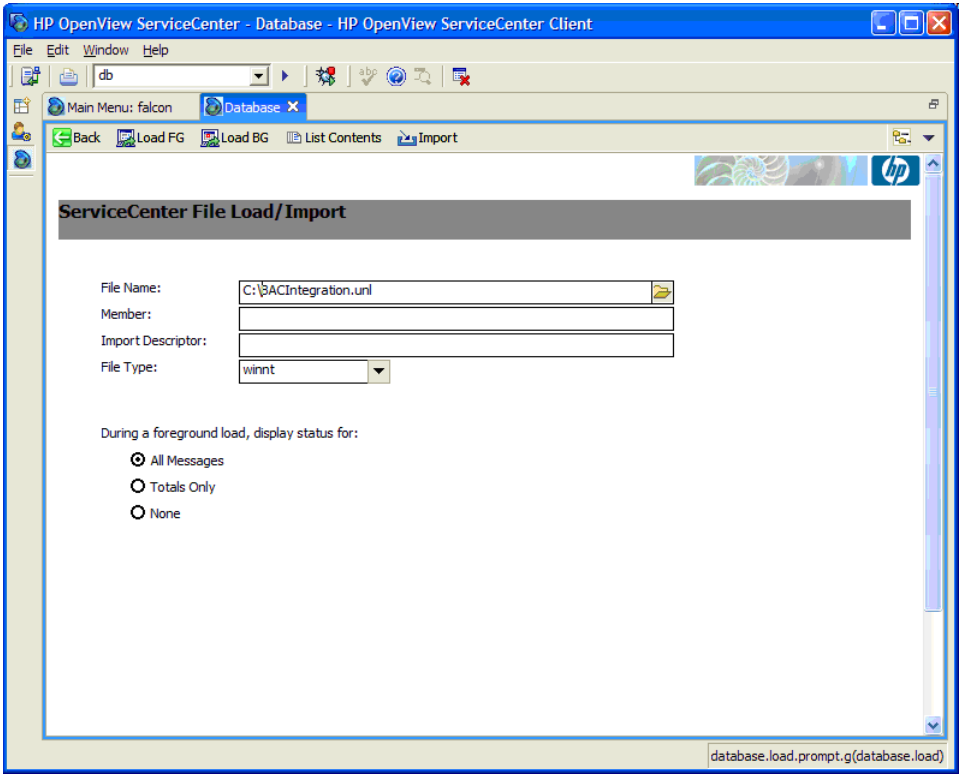
- For HP ServiceCenter 6.2.1 and above: **Start** > **Programs** > **Service Center 6.2**, and log in as a user with Administrator privileges, such as **falcon** (no password).
- For HP Service Manager 7.0 and above: **Start** > **Programs** > **Service Manager 7.0**, and log in as a user with Administrator privileges, such as **falcon** (no password).

c Locate the command line text widget in the menu bar at the top of the client display, to the right of the Printer icon.

d Type **db** and press enter to start the Database Manager application.



e Right-click anywhere on the white background, and select **Import / Load** from the context menu that displays to start the ServiceCenter File Load/Import application.



f Click the manila folder icon at the end of the **File Name** box and navigate to the **BAC_PI_62_v(X).unl** or **BAC_PI_70_v(X).unl** file you saved previously, select it, and click **Open**. The screen shown above refreshes and displays with the path to the selected file.

g Click the **Load FG** button on the toolbar to load the file.

h Log out of the client.

6 Change the Default HP Service Manager Entity – Optional

The configured default entity determines the default title for displaying incident or problem details in the Properties page, as well as the default action when you click the **Associate** or **New** buttons on the page. For details on the Properties page, see "Problem Isolation Properties Page" on page 125.

To change the default HP Service Manager entity:

To modify the default HP Service Manager entity, in Business Availability Center select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Default ServiceCenter entity** entry in the **ServiceCenter** table. Modify the value to Incident or Problem.

7 Federate HP Business Availability Center and HP Service Manager Data

Business Availability Center supports the integration of Problem Isolation using the federation adapter, with HP ServiceCenter 6.2.x and HP Service Manager 7.02.

Use the HP ServiceCenter/Service Manager Adapter to federate Universal CMDB data with HP Service Manager CMDB data. For details on this topic, see "The HP ServiceCenter/Service Manager Adapter" in *Model Management*.

8

The HP ServiceCenter/Service Manager Adapter

This chapter provides information on the HP ServiceCenter/Service Manager Adapter, version 1.0. The Adapter is compatible with HP Business Availability Center, version 7.0 or later, HP ServiceCenter, version 6.2, and HP Service Manager, version 7.0 (following changes to the WSDL configuration).

Note: This Adapter is a specific configuration of the ServiceDesk Adapter.

This chapter includes:

Concepts

Tasks

Adapter Usage

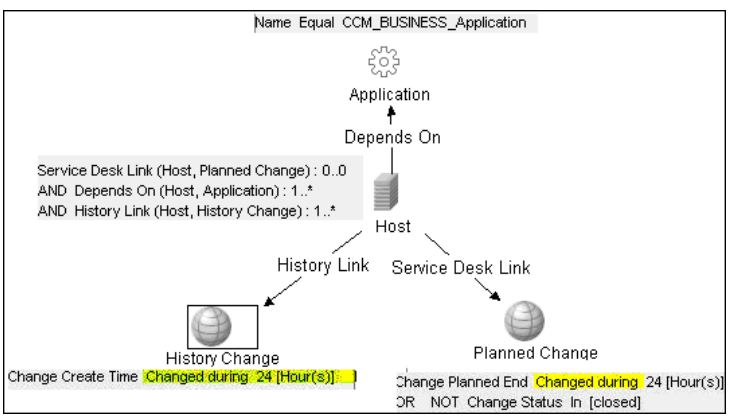
The ServiceCenter/Service Manager Adapter supports the retrieval of data from HP ServiceCenter and HP Service Manager. This adapter connects to, and receives data from, ServiceCenter/Service Manager using the Web Service API. Every request to ServiceCenter/Service Manager to calculate a federated query is made through this adapter.

The Adapter supports three external CI types: Incident, Problem, and Planned Change. The adapter retrieves the CIs of these types from ServiceCenter/Service Manager with the required layout and by a given filter (using reconciliation and/or a CI filter). Each of these CITs can be related to one of the following UCMDB internal CITs: Host, Business Service, Application. Each UCMDB internal CIT includes a reconciliation rule in the ServiceCenter/Service Manager configuration that can be changed dynamically (for details, see "Reconciliation Data Configuration" on page 164). Note that there are no internal relationships between Adapter-supported CITs.

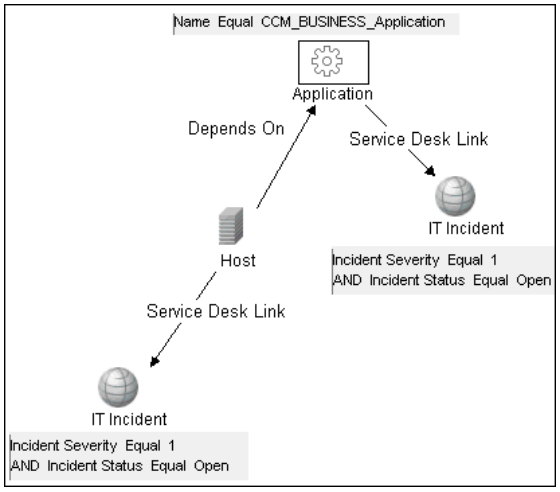
The modeling of the supported CITs and virtual relationships is supplied with the Adapter. You can add attributes to a CIT (for details, see "Add an Attribute to the ServiceCenter/Service Manager CIT" on page 175).

The following use cases (that include TQL examples) describe how the Adapter can be employed:

1 A user needs to display all unplanned changes to all hosts running a specific application during the last 24 hours:



2 A user needs to see all open critical incidents on an application and its hosts:



The Adapter Configuration File

The Adapter configuration file **serviceDeskConfiguration.xml** is located in the following directory:

<HP Business Availability Center root directory>\fcmdb\CodeBase \ServiceDeskAdapter

This file contains three parts:

1 The first part, which is defined by the ucmdbClassConfigurations element, contains the external CIT configuration that the Adapter supports. For details, see "External CITs Configuration" on page 160.

2 The second part, defined by the reconciliationClassConfigurations element, contains reconciliation data information for appropriate UCMDB CITs. For details, see "Reconciliation Data Configuration" on page 164.

3 The third part, defined by the globalConnectorConfig element, includes the global configuration for a specific connector implementation. For details, see "Global Configuration" on page 168.

Important: The adapter is delivered without a default configuration file. Before defining a data store, you must prepare the appropriate file, according to the version of ServiceCenter/Service Manager you are working with:

➤ Locate the **...\fcmdb\CodeBase\ServiceDeskAdapter** folder.

This folder contains three configuration files:
serviceDeskConfiguration.xml.6.xx for ServiceCenter version 6.xx
serviceDeskConfiguration.xml.7.0x for Service Manager version 7.0x
serviceDeskConfiguration.xml.7.1x for Service Manager version 7.1x

➤ Delete the suffix of the appropriate configuration file. For example, if you are working with Service Manager 7.0x, locate the **serviceDeskConfiguration.xml.7.0x** file and delete **.7.0x**, so that the new name of the file is **serviceDeskConfiguration.xml**.

External CITs Configuration

Each CIT that is supported by the Adapter is defined in the first section of the Adapter configuration file.

This section, ucmdbClassConfiguration, represents the only supported CIT configuration. This element contains the CIT name as defined in the UCMDB class model (the ucmdbClassName attribute), mapping for all its attributes (the attributeMappings element), and a private configuration for a specific connector implementation (the classConnectorConfiguration element):

➤ The ucmdbClassName attribute defines the UCMDB class model name.

➤ The attributeMappings element contains attributeMapping elements.

The attributeMapping element defines the mapping between the UCMDB model attribute name (the ucmdbAttributeName attribute) to an appropriate ServiceCenter/Service Manager attribute name (the serviceDeskAttributeName attribute).

For example:

```
<attributeMapping ucmdbAttributeName="problem_brief_description"
serviceDeskAttributeName="brief.description"/>
```

This element can optionally contain the following converter attributes:

- The converterClassName attribute. This is the converter class name that converts the UCMDB attribute value to the ServiceDesk attribute value.
- The reversedConverterClassName attribute. This is the converter class name that converts the ServiceDesk attribute value to the UCMDB attribute value.

- The classConnectorConfiguration element contains the configuration for the specific connector implementation for the current external CIT. Wrap this configuration in CDATA if it contains special XML characters (for example, & replacing &).

  The useful fields of the Service Manager classConnectorConfiguration element are as follows:

  - The **device_key_property_names** element contains the fields names in the WSDL information of the current object that can contain the device ID (for example, ConfigurationItem). Each field should be added as a device_key_property_name element.
  - The **id_property_name** element contains the field name in the WSDL information that contains the ID of the current object.

The following example shows the ucmdbClassConfiguration section of the serviceDeskConfiguration.xml file. The section includes the ucmdbClassName element for the Incident CIT with a ServiceCenter connector implementation:

```
 <ucmdbClassConfiguration ucmdbClassName="it_incident">
          <attributeMappings>
             <attributeMapping ucmdbAttributeName="incident_id"
serviceDeskAttributeName="IncidentID"/>
             <attributeMapping ucmdbAttributeName="incident_brief_description"
serviceDeskAttributeName="BriefDescription"/>
             <attributeMapping ucmdbAttributeName="incident_category"
serviceDeskAttributeName="Category"/>
             <attributeMapping ucmdbAttributeName="incident_severity"
serviceDeskAttributeName="Severity"/>
             <attributeMapping ucmdbAttributeName="incident_open_time"
serviceDeskAttributeName="OpenTime"/>
             <attributeMapping ucmdbAttributeName="incident_update_time"
serviceDeskAttributeName="UpdatedTime"/>
             <attributeMapping ucmdbAttributeName="incident_close_time"
serviceDeskAttributeName="ClosedTime"/>
             <attributeMapping ucmdbAttributeName="incident_status"
serviceDeskAttributeName="IMTicketStatus"/>
          </attributeMappings>
<classConnectorConfiguration>
             <![CDATA[ <class_configuration
connector_class_name="com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.servi
ceCenterConnector.impl.SimpleServiceCenterObjectConnector">
<device_key_property_names>
<device_key_property_name>ConfigurationItem</device_key_property_name>
         </device_key_property_names>
         <id_property_name>IncidentID</id_property_name>
         <keys_action_info>
           <request_name>RetrieveIncidentKeysListRequest</request_name>
           <response_name>RetrieveIncidentKeysListResponse</response_name>
</keys_action_info>
```

```
<properties_action_info>
        <request_name>RetrieveIncidentListRequest</request_name>
        <response_name>RetrieveIncidentListResponse</response_name>
      </properties_action_info>
    </class_configuration> ]]>
      </classConnectorConfiguration>
    </ucmdbClassConfiguration>
```

Adding an Attribute to a CIT

When adding an attribute to the UCMDB model for a Adapter-supported CIT:

1. In **serviceDeskConfiguration.xml**, add an attributeMapping element to the appropriate ucmdbClassConfiguration element.
2. Verify that ServiceCenter/Service Manager externalizes this attribute in its Web Service API.
3. Save **serviceDeskConfiguration.xml**.
4. Send a call to the JMX to reload the adapter: **FCmdb Config Services** > **loadOrReloadCodeBaseForAdapterId**, using the appropriate customer ID and the ServiceDeskAdapter adapter ID.

Reconciliation Data Configuration

Each UCMDB CIT that can be related to the adapter-supported CIT is defined in the second section of the Adapter configuration file.

This section, reconciliationClassConfigurations, represents the reconciliation data configuration for one UCMDB CIT. The element includes two attributes:

- The ucmdbClassName attribute. This is the CIT name as defined in the UCMDB class model.
- The concreteMappingImplementationClass attribute. This is the class name of the concrete implementation for the ConcreteMappingEngine interface. Use this attribute to map between instances of UCMDB CITs and external Adapter CITs. The default implementation that is used is:

```
com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.mapping.impl.OneNodeMappingEngine
```

An additional implementation exists that is used only for the host reconciliation CIT for reconciliation by the IP of the host:

```
com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.mapping.impl.
HostIpMappingEngine
```

The reconciliationClassConfiguration element can contain one of the following elements:

- The reconciliationById element. This element is used when the reconciliation is done by ID. In this case, the text value of this element is the ServiceDesk field name that contains the CMDB ID. For example:

```
<reconciliationById>SerialNumber</reconciliationById>
```

In this example, the ServiceDesk field SerialNumber contains the CMDB ID of the appropriate host.

- The reconciliationData element. Use this element if the reconciliation is done by comparing attributes. You can run reconciliation with one attribute or several attributes by using the logical operators OR and/or AND.

If you run reconciliation with one attribute, the reconciliationData child element should be a reconciliationAttribute element. The reconciliationAttribute element contains an appropriate UCMDB attribute name (the ucmdbAttributeName attribute) and an appropriate ServiceDesk attribute name (the serviceDeskAttributeName attribute). This element can also contain a ucmdbClassName attribute that defines the appropriate UCMDB CIT name. By default, the current reconciliation UCMDB CIT name is used.

You can also use the converterClassName and reversedConverterClassName attributes; they should contain the converter class name that converts the UCMDB attribute value to the ServiceDesk attribute value, or vice versa.

For example:

```
<reconciliationData>
            <reconciliationAttribute ucmdbAttributeName="host_hostname"
serviceDeskAttributeName="NetworkName"
converterClassName="com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.converter.PropertyValueConverterToUpperCase"/>
  </reconciliationData>
```

For reconciliation to run with two or more attributes, use a logical operator between reconciliation attributes.

The logical operator AND can contain several reconciliationAttribute elements (the minimum is 2). In this case the reconciliation rule contains an AND operator between attribute comparisons.

For example:

```
<reconciliationData>
<AND>
            <reconciliationAttribute ucmdbAttributeName="host_hostname"
serviceDeskAttributeName="NetworkName"
converterClassName="com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.converter.PropertyValueConverterToUpperCase"/>
             <reconciliationAttribute ucmdbClassName=”ip”
ucmdbAttributeName="ip_address" serviceDeskAttributeName="NetworkAddress" />

</AND>
  </reconciliationData>
```

In this example, the reconciliation rule follows this format: host.host_hostname= NetworkName and ip.ip_address= NetworkAddress.

The logical operator OR can contain several reconciliationAttribute and AND elements. In this case the reconciliation rule contains an OR operator between attributes and AND expressions. Since XML does not assure the order of elements, you should provide a priority attribute to each sub-element of OR element type. The comparison between OR expressions is calculated by these priorities.

For example:

```
<reconciliationData>
<OR>
            <reconciliationAttribute ucmdbAttributeName="host_dnsname"
serviceDeskAttributeName="NetworkDNSName" priority=”2” />
<AND priority=”1” >
          <reconciliationAttribute ucmdbAttributeName="host_hostname"
serviceDeskAttributeName="NetworkName"
converterClassName="com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.converter.PropertyValueConverterToUpperCase"/>
            <reconciliationAttribute ucmdbClassName=”ip”
ucmdbAttributeName="ip_address" serviceDeskAttributeName="NetworkAddress" />

</AND>
</OR
  </reconciliationData>
```

In this example the reconciliation rule follows this format: (host.host_dnsname= NetworkDNSName OR (host.host_hostname= NetworkName and ip.ip_address= NetworkAddress)). Since the AND element takes a priority attribute of value 1, the (host.host_hostname= NetworkName and ip.ip_address= NetworkAddress) condition is checked first. If the condition is satisfied, the reconciliation is run. If not, the .host_dnsname= NetworkDNSName condition is checked.

The additional sub-element of the reconciliationClassConfiguration element is classConnectorConfiguration. The classConnectorConfiguration element contains the configuration for a specific connector implementation for the current reconciliation CIT. This configuration should be wrapped by CDATA if it contains some special XML characters (for example, & replacing &).

Changing the Reconciliation Rule of a CIT

1 In **serviceDeskConfiguration.xml**, update the appropriate reconciliationData element with the new rule.

2 Call to the JMX to reload the adapter: **FCmdb Config Services** > **loadOrReloadCodeBaseForAdapterId**, using the appropriate customer ID and ServiceDeskAdapter adapter ID.

Reconciliation of a Host by ip_address or by host_name

To run reconciliation on a host by ip_address or host_name, place the following ReconciliationData element in the Adapter configuration file:

```
<reconciliationData>
    <OR>
        <reconciliationAttribute priority="1" ucmdbClassName="ip"
ucmdbAttributeName="ip_address" serviceDeskAttributeName="NetworkAddress"/>
        <reconciliationAttribute priority="2" ucmdbClassName="host"
ucmdbAttributeName="host_hostname" serviceDeskAttributeName="NetworkName"
converterClassName="com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.conver
ter.PropertyValueConverterToUpperCase"/>
    </OR>
</reconciliationData>
```

You should also change the value of the concreteMappingImplementationClass attribute of the reconciliationClassConfiguration element to:

```
="com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.mapping.impl.HostIpMappin
gEngine"
```

Global Configuration

The third section of the Adapter configuration file contains the global configuration for the specific connector implementation.

This configuration, globalConnectorConfig, should be wrapped by CDATA if it contains some special XML characters (for example, & replacing &).

The useful fields of the Service Manager globalConnectorConfig element are as follows:

1. The **date_pattern** element contains the date pattern that the Service Manager is working with.

   The default is MM/dd/yy HH:mm:ss.

   If the date pattern is wrong, an FTQL returns wrong date condition results.

2. The **time_zone** element defines the time zone of Service Manager. The default is the UCMDB server time zone.

   To check the Service Manager date pattern and time zone:

   a. **Service Manager version 7**: Access **Menu Navigation** > **System Administration** > **Base System Configuration** > **Miscellaneous** >**System Information Record**. Click the **Date Info** tab.

   b. **ServiceCenter version 6.1**: Access **Menu Navigation** > **Utilities** >**Administration** > **Information** >**System Information**. Click the **Date Info** tab.

3. The **max_query_length** element defines the maximal query length in a Service Manager Web service request. The default value is 1000000.

4. The **name_space_uri** element defines the name space URI to connect to the Service Manager Web service. The default value is http://servicecenter.peregrine.com/PWS.

5. The **web_service_suffix** element defines the Service Manager Web service center URI suffix. The default value is sc62server/ws. It is used when the URL is created.

Deploy the Adapter

This section describes a typical deployment of the adapter.

This section includes the following steps:

1 "Deploy the ServiceDesk Adapter" on page 169

   a "Extract the Adapter Implementation Files and Deploy the Package" on page 170

   b "Add a ServiceCenter/Service Manager External Data Source" on page 170

   c "Configure HP ServiceCenter 6.2" on page 170 (when connecting to HP ServiceCenter)

   d "Configure HP Service Manager 7.0" on page 173 (when connecting to HP Service Manager)

2 "Add an Attribute to the ServiceCenter/Service Manager CIT" on page 175

   a "Add an Attribute to the Business Availability Center Model" on page 178

   b "Export Attributes from HP ServiceCenter by Changing the Configuration" on page 179 (when connecting to HP ServiceCenter)

   c "Export Attributes from HP Service Manager by Changing the Configuration" on page 181 (when connecting to HP Service Manager)

   d "Modify the Adapter Configuration File" on page 183

   e "Load the Changes" on page 184

Deploy the ServiceDesk Adapter

This section explains where to place the files needed for deployment.

This section includes the following steps:

- "Extract the Adapter Implementation Files and Deploy the Package" on page 170
- "Add a ServiceCenter/Service Manager External Data Source" on page 170
- "Configure HP ServiceCenter 6.2" on page 170

➤ "Configure HP Service Manager 7.0" on page 173

1 Extract the Adapter Implementation Files and Deploy the Package

a Verify the location of the following folder and file:

➤ ServiceDeskAdapter

➤ serviceDeskAdapter.zip

b Move the **serviceDeskAdapter.zip** package to the following directory: **<HP Business Availability Center root directory>\mam_lib\packages**.

c Deploy the serviceDeskAdapter.zip package: Log in to Business Availability Center and access the Package Manager (**Admin** > **Universal CMDB** > **Settings** > **Package Manager**). Select the package and click the **Deploy** button.

For details on deploying packages, see "Deploy a Package" on page 665.

d Move the **ServiceDeskAdapter** folder to the following directory:

<HP Business Availability Center root directory>\fcmdb\CodeBase

2 Add a ServiceCenter/Service Manager External Data Source

In this step, you add an external data store.

a In Business Availability Center, access the Federated CMDB window: **Admin** > **Universal CMDB** > **Settings** > **Federated CMDB**.

b Click the button to add a data store. In the Data Store dialog box that opens, choose the **ServiceDeskAdapter** and fill in the mandatory fields.

For help with this dialog box, see "Data Stores Tab" on page 1021.

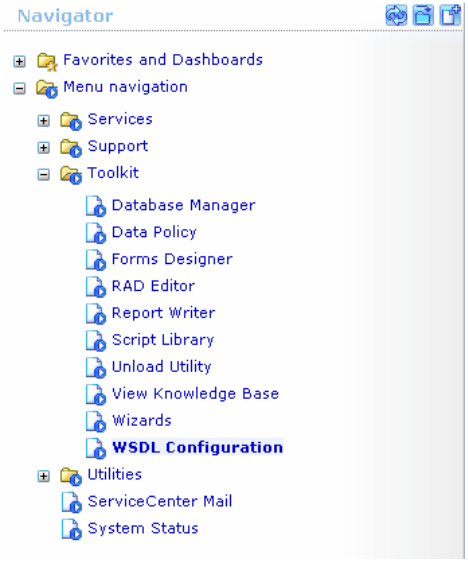
c Continue to "Configure HP ServiceCenter 6.2" on page 170 or "Configure HP Service Manager 7.0" on page 173.

3 Configure HP ServiceCenter 6.2

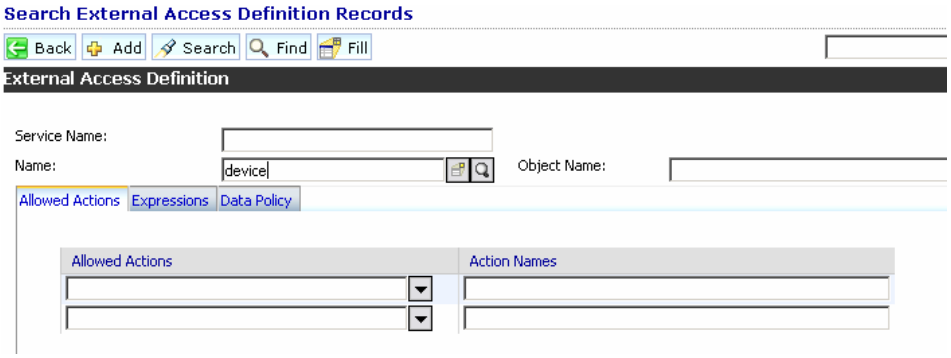
If you are connecting to HP ServiceCenter, perform the following procedure.

a Open HP ServiceCenter, then the ServiceCenter client.

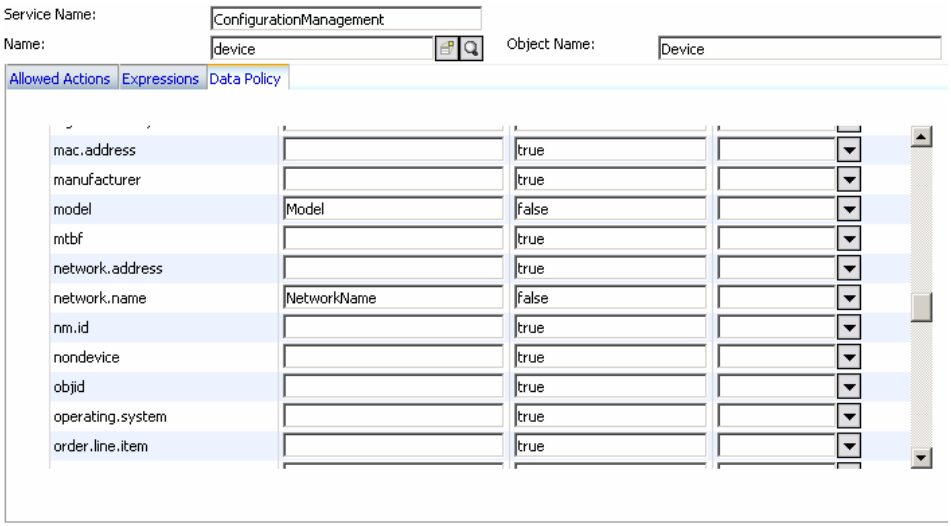
b Display **WSDL Configuration** in the Navigator (**Main Menu** > **Menu navigation** > **Toolkit**):



c In the Name field, enter **device** and press **Enter**:



d Select the **Data Policy** tab and ensure that the network.name attribute is not empty (its value should be **NetworkName**). Change the value to **false**. Save your changes.

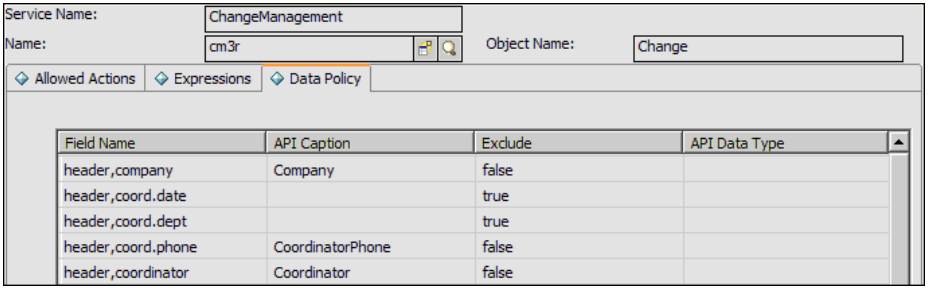


e After saving, click the **Cancel** button.

f In the Object Name field type **Change** and press **Enter**.

g Select the Data Policy tab and ensure that:

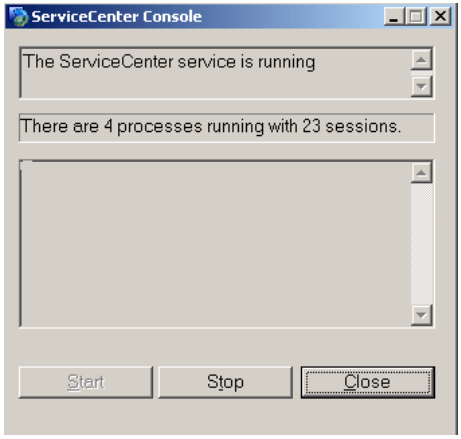
➤ The **header,coordinator** attribute is not empty (its value should be **Coordinator**). Change the value to **false**.



➤ The **header,orig.operator** attribute is not empty (its value should be **OpenedBy**). Change the value to **false**.

h Save the changes.

i Restart ServiceCenter: Select **Start** > **Programs** > **ServiceCenter 6.2** > **Server** > **Console** to open the ServiceCenter Console.



j Click **Stop** and then **Start**.

k Continue to "Add an Attribute to the Business Availability Center Model" on page 178.

4 Configure HP Service Manager 7.0

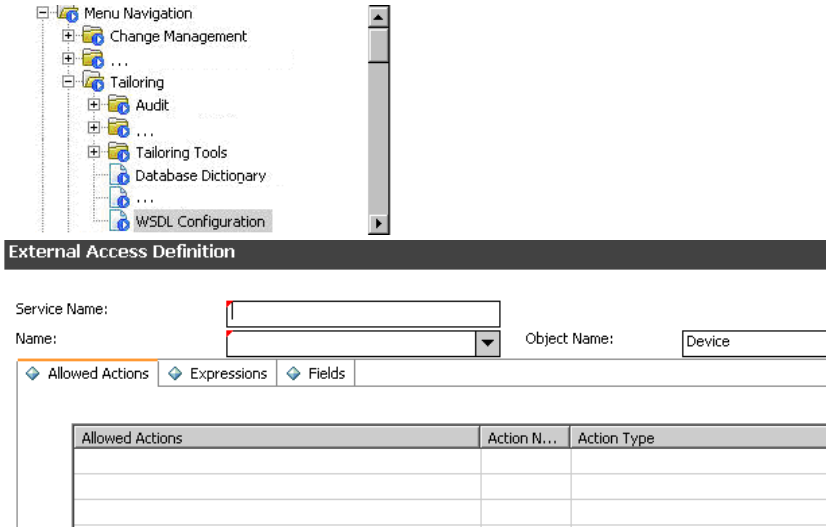
If you are connecting to HP Service Manager, perform the following procedure.

a Import the **SCR41399_SM70.unl** unload file. To do so, in Service Manager, click **Menu Navigation** > **Tailoring** > **Database Manager**.

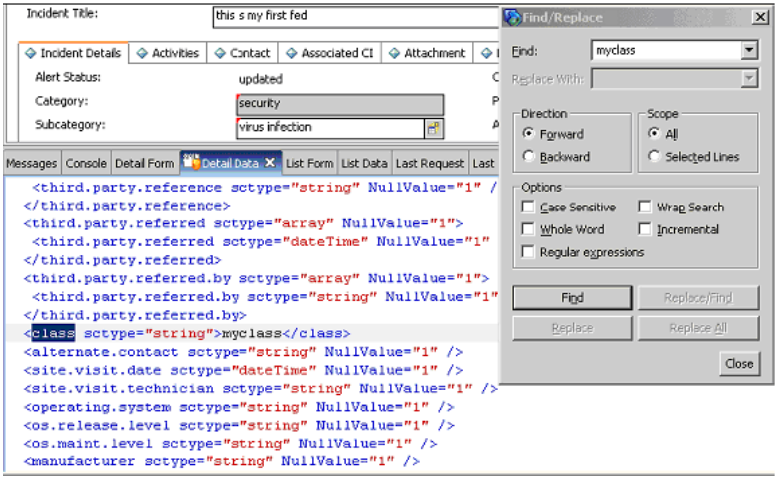
- ➤ Right-click the detail button and select **Import/Load**.
- ➤ In the HP Service Manager File Load/Import, click **Specify File** and locate the **SCR41399_SM70.unl** unload file on the Service Manager DVD. The file is loaded via the file browser.
- ➤ Enter the description in the **Import Description** box.
- ➤ Select **winnt** in the **File Type** list.
- ➤ Select a display option.
- ➤ Click **Load FG** to start loading.

b Open the HP Service Manager client.

c Display **WSDL Configuration** in the Navigator (**Main Menu** > **Menu navigation** > **Tailoring**) and in the Object Name field:



➤ Enter **Device** and press ENTER. Click the **Fields** tab and ensure that the network.name attribute appears in the **Field** list with NetworkName as its caption. If this attribute does not appear in the Field list, add it and save your changes.



➤ Enter **Change** and press ENTER. Click the **Fields** tab and ensure that the header,orig.operator attribute appears in the **Field** list with OpenedBy as its caption and the header,coordinator attribute appears in the **Field** list with Coordinator as its caption. If this attribute does not appear in the Field list, add it and save your changes.

➤ Enter **Problem** and press ENTER. Click the **Fields** tab and ensure that the status attribute appears in the **Field** list with Status as its caption and the affected.ci(ci.device.name) attribute appears in the **Field** list with CiDeviceName as its caption. If this attribute does not appear in the Field list, add it and save your changes.

d After saving, click the **Cancel** button.

e Continue to "Add an Attribute to the Business Availability Center Model" on page 178.

Add an Attribute to the ServiceCenter/Service Manager CIT

This section explains how to retrieve additional data from ServiceCenter/Service Manager by adding an attribute.

This section includes the following steps:

1 Replace the it_problem ucmdb Class Configuration

You must replace the **it_problem ucmdb** class configuration in the **serviceDeskConfiguration.xml** file as explained in this step.

a In the server where FCMDB service is running, open the **serviceDeskConfiguration.xml** file located in **HPBAC\fcmdb\CodeBase\ServiceDeskAdapter**.

b Replace the entire **it_problem ucmdb** class configuration with the following:

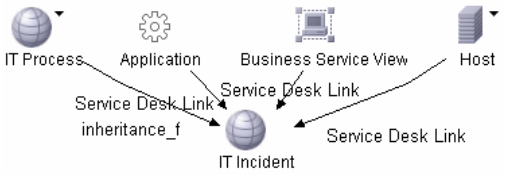
```
<ucmdbClassConfiguration ucmdbClassName="it_problem">
	<attributeMappings>
		<attributeMapping ucmdbAttributeName="problem_id"
serviceDeskAttributeName="ID"/>
		<attributeMapping ucmdbAttributeName="problem_brief_description"
serviceDeskAttributeName="BriefDescription"/>
		<attributeMapping ucmdbAttributeName="problem_status"
serviceDeskAttributeName="Status"/>
		<attributeMapping
ucmdbAttributeName="problem_expected_resolution_day"
serviceDeskAttributeName="ExpectedResolutionTime"/>
		<attributeMapping ucmdbAttributeName="problem_category"
serviceDeskAttributeName="Category"/>
		<attributeMapping ucmdbAttributeName="problem_impact"
serviceDeskAttributeName="InitialImpact"/>
		<attributeMapping ucmdbAttributeName="problem_urgency"
serviceDeskAttributeName="Severity"/>
		<attributeMapping ucmdbAttributeName="problem_priority"
serviceDeskAttributeName="PriorityCode"/>
		<attributeMapping ucmdbAttributeName="problem_assignment_group"
serviceDeskAttributeName="Assignment"/>
	</attributeMappings>
<classConnectorConfiguration><![CDATA[<class_configuration
connector_class_name="com.mercury.topaz.fcmdb.adapters.serviceDeskAdapter.servi
ceCenterConnector.impl.SimpleServiceCenterObjectConnector"  >
	<device_key_property_names>
		<device_key_property_name>CI</device_key_property_name>
		<device_key_property_name>CiDeviceName</device_key_property_name>
	</device_key_property_names>
	<id_property_name>ID</id_property_name>
	<keys_action_info>
		<request_name>RetrieveProblemKeysListRequest</request_name>
		<response_name>RetrieveProblemKeysListResponse</response_name>
	</keys_action_info>
	<properties_action_info>
		<request_name>RetrieveProblemListRequest</request_name>
		<response_name>RetrieveProblemListResponse</response_name>
	</properties_action_info>
</class_configuration>]]></classConnectorConfiguration>
</ucmdbClassConfiguration>
```

c Reload the **ServiceDeskAdpater** from **Admin** > **uCMDB** > **Settings** > **Federation**:

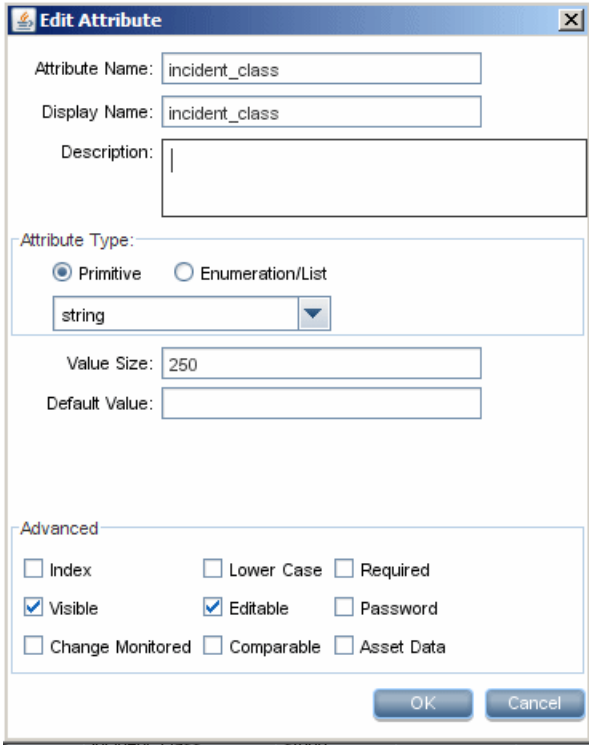
2 Add an Attribute to the Business Availability Center Model

To add an attribute to the model proceed as follows:

a Add the new attribute to Business Availability Center: Edit the Incident CIT: Select **Admin** > **Universal CMDB** > **Modeling** > **CI Type Manager**. In View Explorer, select **IT Process** > **IT Incident**.



b Select the Attribute tab and add the new attribute:



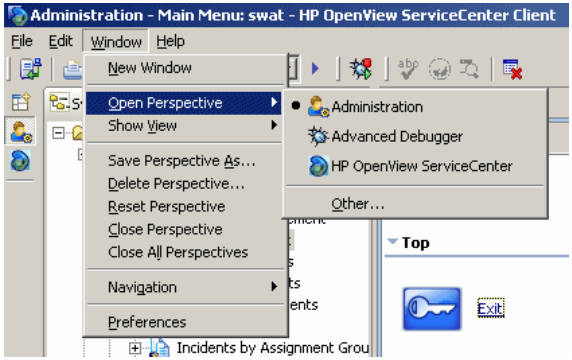
c Continue to “Export Attributes from HP ServiceCenter by Changing the Configuration” on page 179 or “Export Attributes from HP Service Manager by Changing the Configuration” on page 181.

3 Export Attributes from HP ServiceCenter by Changing the Configuration

If you are connecting to HP ServiceCenter, perform the following procedure.

a In HP ServiceCenter, open the ServiceCenter client.

b Select **Window** > **Open Perspective** > **Administration**:

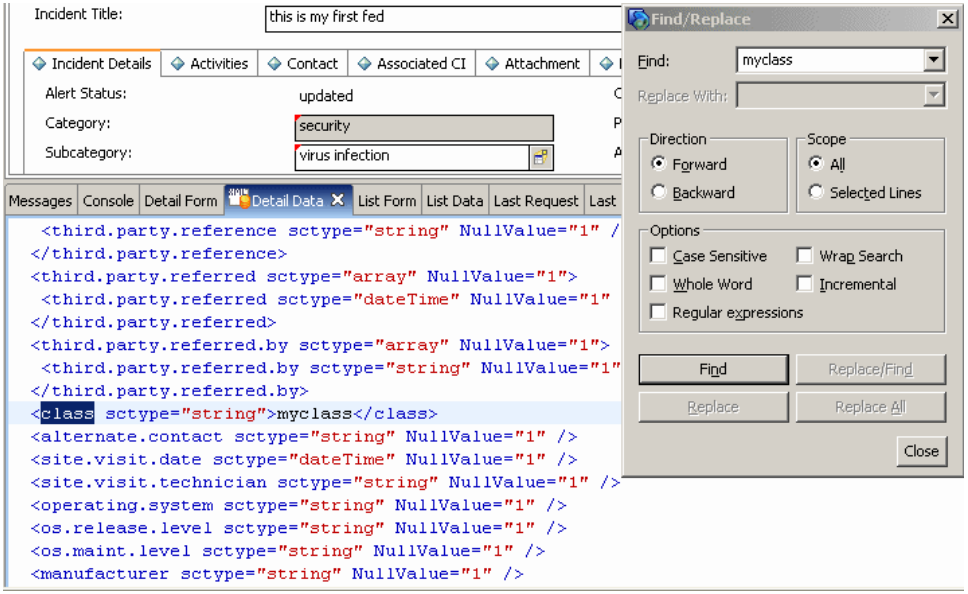


c Select **Incident Management** > **All Open Incidents**, and select one of the incidents you created.

Note: Verify that the value in the Class field is the one that you want to report to Business Availability Center.

---

d Search for the value you entered in the Class field (that is, **myclass**), in the XML file displayed below. This is the CI name in ServiceCenter.



e Display **WSDL Configuration** in the Navigator (**Main Menu** > **Menu navigation** > **Toolkit**). Locate the Object Name field, enter **Incident** and press **Enter**.

f Select the **Data Policy** tab. Enter a name for the CI mentioned in the XML file (that is, **class**). Change the value to **false**. Save your changes.

g Restart ServiceCenter: Select **Start** > **Programs** > **ServiceCenter 6.2** > **Server** > **Console** to open the ServiceCenter Console.

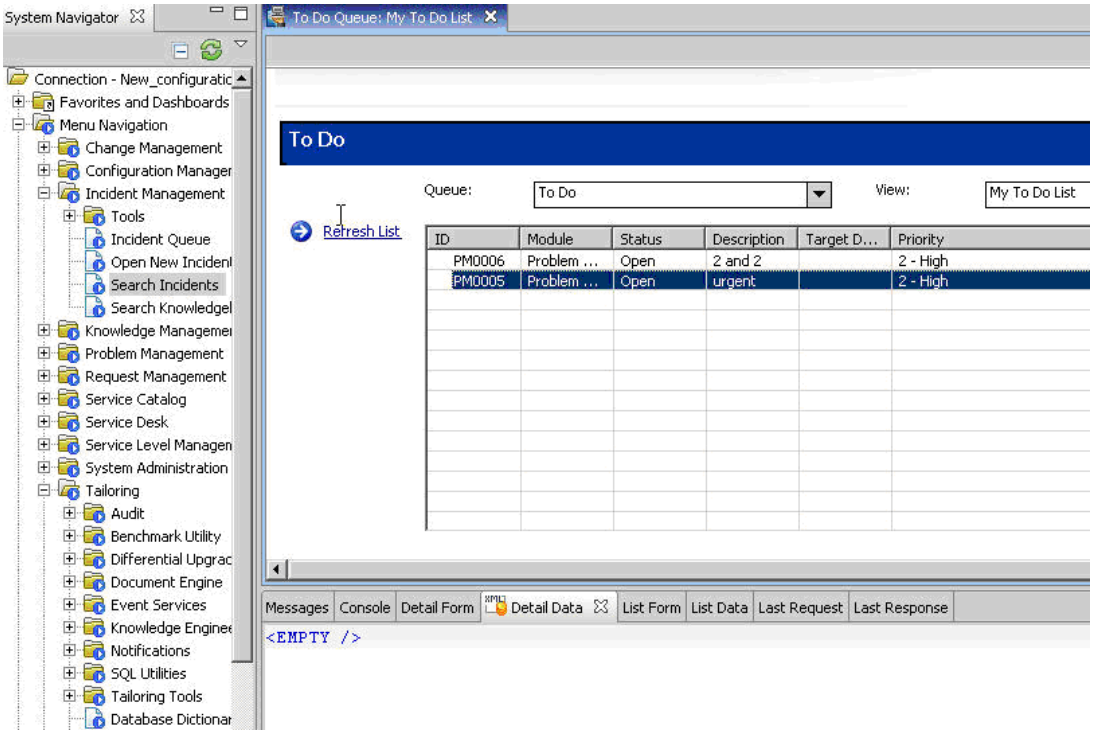
h Click **Stop** and then **Start**.

i Continue to “Modify the Adapter Configuration File” on page 183.

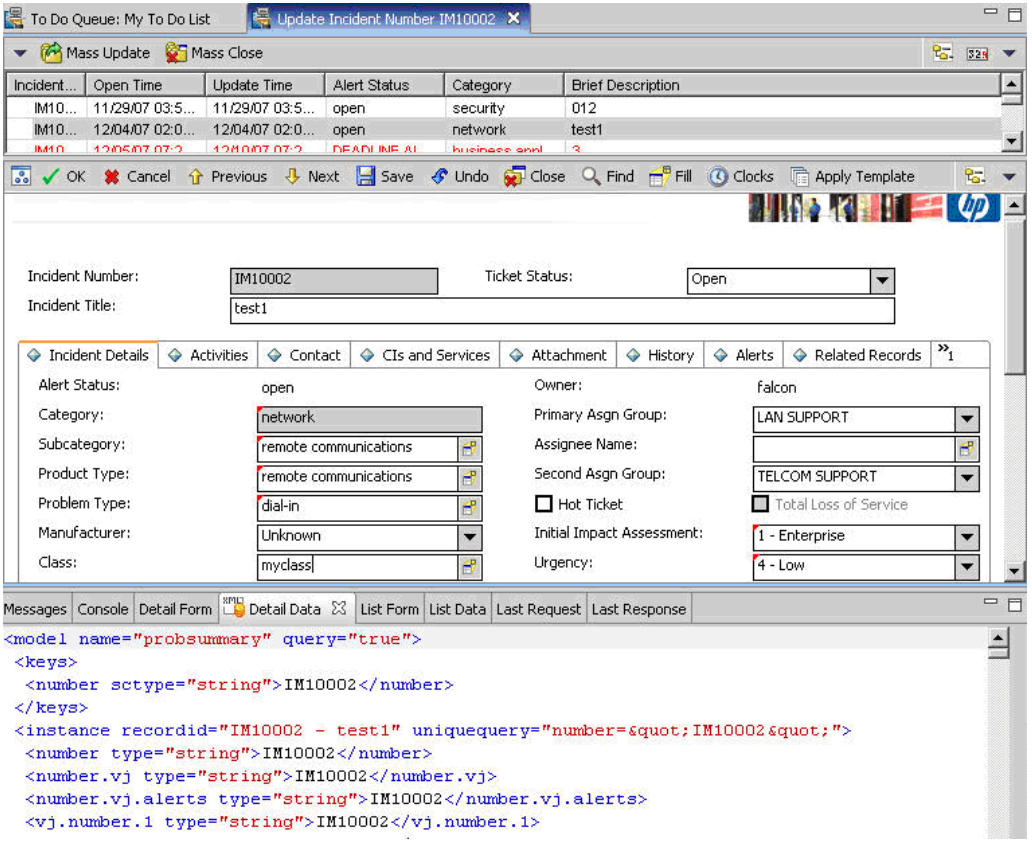
4 Export Attributes from HP Service Manager by Changing the Configuration

If you are connecting to HP Service Manager, perform the following procedure.

a In the HP Service Manager client, restore the bottom right pane by clicking the **Restore** button. Click the **Detail Data** tab.

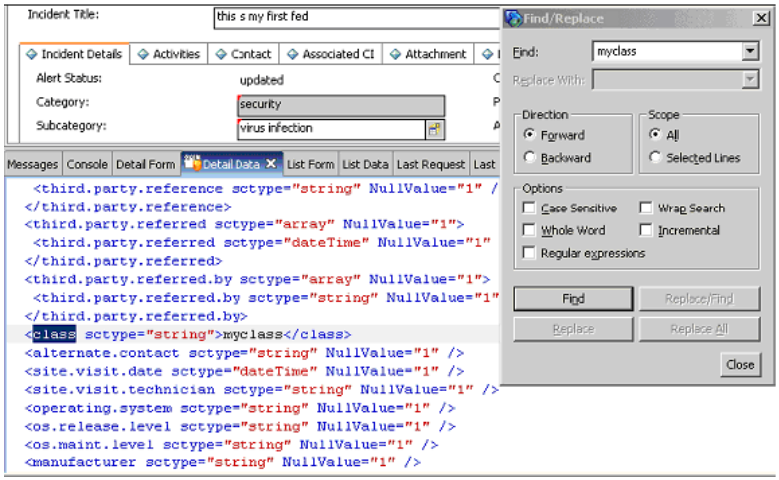


b Open one of the incidents you created: Select **Incident Management** > **Search Incidents**. Click the search button (you can filter the fields to limit the search).



Note: Verify that the value in the Class field is the one that you want to report to Business Availability Center.

c Search for the value you entered in the Class field (that is, **myclass**), in the XML file displayed below. This is the CI name in Service Manager.



d Display **WSDL Configuration** in the Navigator (**Main Menu** > **Menu Navigation** > **Tailoring**). Locate the Object Name field, enter **Incident** and press ENTER.

e Select the **Data Policy** tab.

f Select the **Fields** tab and ensure that the CI name mentioned in the XML file (that is, **class**) appears in the Field list with **ClassName** as its caption. If this attribute does not appear in the Field list, add it and save your changes.

g Restart the HP Service Manager 7.00 Server service.

h Continue to “Modify the Adapter Configuration File” on page 183.

5 Modify the Adapter Configuration File

Perform this procedure for all configurations.

a Edit the **ServiceDeskConfiguration.xml** file in

<HP Business Availability Center root directory>\fcmdb\CodeBase\ServiceDeskAdapter

b Add the new attribute line under the Incident area: Locate the following marker:

```
<ucmdbClassConfiguration ucmdbClassName="it_incident">
<attributeMappings>
```

c Add the following line:

```
<attributeMapping ucmdbAttributeName="incident_class"
ServiceDeskAttributeName="ClassName"/>
```

where:

- ucmdbAttributeName="incident_class" is the value defined in the CI Type Manager
- ServiceDeskAttributeName="ClassName" is the valued defined in ServiceCenter/Service Manager

d Continue to "Load the Changes" on page 184.

6 Load the Changes

Perform this procedure to load changes.

a Launch the Web browser and enter the following address:

```
http://<machine name or IP address>:8080/jmx-console/
```

where <machine name or IP address> is the machine on which Business Availability Center is installed.

Note: In the case of a distributed deployment, the machine name is the machine on which the Data Processing server is installed.

You may have to log in with the administrator's user name and password.

b Click the **Topaz** > **service=Fcmdb Config Services** link.

c In the JMX MBEAN View page, locate the following operation: **loadOrReloadCodeBaseForAdapterId()**.

d In the customerID field, enter **1**. In the AdapterId field, enter the name of the Adapter folder (ServiceDeskAdapter). Click **Invoke**.

Index

I

L

P

S

U