HP Business Service Management

for the Windows and Linux operating systems

Software Version: 9.10

Solutions and Integrations

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2005 - 2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

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

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

iPod is a trademark of Apple Computer, Inc.

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

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

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support web site at:

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

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

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

• Search for knowledge documents of interest

• Submit and track support cases and enhancement requests

• Download software patches

• Manage support contracts

• Look up HP support contacts

• Review information about available services

• Enter into discussions with other software customers

• Research and register for software training

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

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

To find more information about access levels, go to:

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

Table of Contents

Table of Contents

Welcome to This Guide

This guide describes the various solutions and integrations available for HP Business Service Management.

This chapter includes:

➤ How This Guide Is Organized on page 13

➤ Who Should Read This Guide on page 14

➤ How Do I Find the Information That I Need? on page 15

➤ Additional Online Resources on page 17

➤ Documentation Updates on page 18

How This Guide Is Organized

The guide contains the following parts:

Part I   Application Management for SAP

Describes how to install the Application Management for SAP application, the specific tasks involved in administering it, how the SAP discovery process discovers SAP-related CIs and general CIs (such as hosts) that are related to them, and provides information that can help troubleshoot the Application Management for SAP application.

Part II   Application Management for Siebel

Describes how to install the Application Management for Siebel application, the specific tasks involved in administering it, how the Siebel discovery process discovers Siebel-related CIs and general CIs that are related to them, and provides information that can help troubleshoot the Application Management for Siebel application.

Part III   Application Management for SOA

Describes the tasks to perform in BSM to monitor your Service-Oriented Architecture (SOA) enterprise environment.

Part IV   Integrations

Provides an overview of the integration of Business Service Management (BSM) with other HP products, other BSMs and third-party applications, and describes how to build new integrations or customize out-of-the-box integrations for EMS (Enterprise Management Systems) applications, how to integrate HP Operations Manager, HP Service Manager, Network Node Manager i, and NetScout nGenius data into BSM, how to set up an integration with HP Operations Orchestration (OO), enabling you to run OO run books on BSM CIs, and how to configure the integration between HP Diagnostics and BSM.

Who Should Read This Guide

This guide is intended for the following users of HP Business Service Management:

➤ HP Business Service Management administrators

➤ HP Business Service Management platform administrators

➤ HP Business Service Management application administrators

➤ HP Business Service Management data collector administrators

➤ HP Business Service Management end users

➤ HP Business Service Management integration developers

Readers of this guide should be knowledgeable about navigating and using enterprise applications, and be familiar with HP Business Service Management and enterprise monitoring and management concepts.

How Do I Find the Information That I Need?

This guide is part of the HP Business Service Management Documentation Library. This Documentation Library provides a single-point of access for all Business Service Management documentation.

You can access the Documentation Library by doing the following:

➤ In Business Service Management, select **Help** > **Documentation Library**.

➤ From a Business Service Management Gateway Server machine, select **Start** > **Programs** > **HP Business Service Management** > **Documentation**.

Topic Types

Within this guide, each subject area is organized into topics. A topic contains a distinct module of information for a subject. The topics are generally classified according to the type of information they contain.

This structure is designed to create easier access to specific information by dividing the documentation into the different types of information you may need at different times.

Three main topic types are in use: **Concepts**, **Tasks**, and **Reference**. The topic types are differentiated visually using icons.

Topic Type	Description	Usage
Concepts	Background, descriptive, or conceptual information.	Learn general information about what a feature does.
Tasks	**Instructional Tasks.** Step-by-step guidance to help you work with the application and accomplish your goals. Some task steps include examples, using sample data. Task steps can be with or without numbering: ➤ **Numbered steps.** Tasks that are performed by following each step in consecutive order. ➤ **Non-numbered steps.** A list of self-contained operations that you can perform in any order.	➤ Learn about the overall workflow of a task. ➤ Follow the steps listed in a numbered task to complete a task. ➤ Perform independent operations by completing steps in a non-numbered task.
	Use-case Scenario Tasks. Examples of how to perform a task for a specific situation.	Learn how a task could be performed in a realistic scenario.

Topic Type	Description	Usage
Reference	**General Reference**. Detailed lists and explanations of reference-oriented material.	Look up a specific piece of reference information relevant to a particular context.
	User Interface Reference. Specialized reference topics that describe a particular user interface in detail. Selecting **Help on this page** from the Help menu in the product generally opens the user interface topics.	Look up specific information about what to enter or how to use one or more specific user interface elements, such as a window, dialog box, or wizard.
Troubleshooting and Limitations	**Troubleshooting and Limitations**. Specialized reference topics that describe commonly encountered problems and their solutions, and list limitations of a feature or product area.	Increase your awareness of important issues before working with a feature, or if you encounter usability problems in the software.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

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 user ID, go to:

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

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

Part I

Application Management for SAP

1

Application Management for SAP Administration

This chapter includes:

Concepts

Tasks

Concepts

🔵 Application Management for SAP – Overview

Application Management for SAP enables you to gain visibility into your SAP systems and applications.

The SAP solution provides:

➤ A single operation console consolidating all SAP monitoring information.

➤ Automatic discovery and modeling of SAP-related elements, as well as their relations to other systems in the organization's IT.

➤ Change discovery and notification, for quicker problem resolution.

➤ Display of transport deployment impact, for move-to-production risk analysis.

➤ Proactive monitoring of end-user experience in SAP systems.

➤ A bridge between IT and line-of-business people using SAP Solution Manager business processes hierarchy monitoring.

➤ The ability to distinguish between SAP-specific problems and general ones.

➤ Examination, over time, of SAP CCMS monitoring data.

➤ Service Level Management of SAP systems service level commitments.

In addition, you can create SLAs centered around your SAP transaction CIs to gain visibility into performance or availability issues that affect these SLAs. For details on SLAs, see "Service Level Management - Overview" in *Using Service Level Management*.
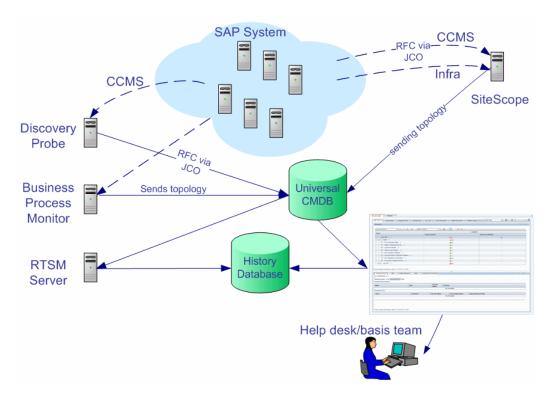
🔷 **Application Management for SAP License**

The Application Management for SAP license unlocks the following functionality in BSM:

➤ The SAP Systems pattern view, displaying a hierarchical view of SAP applications and infrastructure.

➤ Automatic linkage of SiteScope data to their respective SAP infrastructure.

➤ SAP-specific KPIs that enable differentiation between SAP-related issues and non-SAP ones.

➤ SAP Transport Changes and SAP Transaction Changes access from Service Health views for quick visualization of change impact. For details, see "SAP Transport Changes" and "SAP Transaction Changes" in *Using Service Health*.

➤ SAP-specific change reports, summarizing the impact transports have on transactions in the SAP system.

For details about the views and reports, see "How to Display SAP Information in BSM" on page 48.

🔷 Architecture

The following diagram illustrates the architecture of Application Management for SAP.

Most of the SAP CIs are created by automatic discovery. The configuration for these CIs is saved to the Run-time Service Model (RTSM). Some of the relationships to BPM and SiteScope CIs are created by automatic mechanisms unique to Application Management for SAP.

The architecture of Application Management for SAP includes the following components:

➤ The Data Flow Probe discovers SAP-related entities and the general entities (such as hosts) that are related to them using CCMS. The Data Flow Probe communicates with the RTSM using a Remote Function Call (RFC) with a Java Connector (JCo).

➤ The SiteScope SAP CCMS Solution Set communicates with the SAP system and retrieves CCMS monitoring data using a Remote Function Call (RFC) with a Java Connector (JCo).

➤ The BPM collects data on the performance and availability of BPM transactions carried out on the SAP system.

➤ The RTSM Server collects change information from the RTSM and stores it in the History database.

➤ The Service Health tabs and reports are used as the central console for viewing all of the data and performing analysis of the data. For details, see "Introducing Service Health" in *Using Service Health*.

For details about the SiteScope and BPM samples that include SAP data, see "Data Samples for SiteScope" and "Data Samples for Business Process Monitor" in *Reports*.

Collecting SAP System Information

The Automatic Discovery component discovers the actual SAP IT entities and stores them as CIs in the RTSM.

All configuration actions of SAP CIs are performed inside the RTSM Administration application. All SAP CIs appear in the SAP Systems view under the SAP Systems root CI.

All SAP system metrics are monitored by SiteScope monitors.

SAP business processes/transactions are simulated using BPM pre-recorded VuGen scripts. Each script includes one or more Business Transactions and is executed from a specific location. All BPM-related CIs are stored in the RTSM as non-SAP-related CIs with links to the appropriate SAP-related CIs.

Similar to other information, information about the SAP System is available in Service Health in all of the relevant tabs.

The SAP Systems views include information from the SAP IT entities, SAP system metrics monitored by SiteScope monitors, and information about the SAP business processes/transactions simulated by BPM scripts.

SAP Service

The SAP service is assigned to the Modeling Data Processing Server. It is a configuration service that enables BSM to work with data that is in SAP format.

For details on how to view a service status using the JMX Web console, see "High Availability for the Data Processing Server" in the *HP Business Service Management Deployment Guide* PDF.

The SAP Service is responsible for the following advantages:

➤ Intelligent relation of monitoring information.

➤ Loading occurs after the RTSM and Viewing System services are loaded.

➤ Check of the service activity in the JMX console. For details, see "How to Activate the SAP Service" on page 35.

➤ Automatic linkage of BPM scripts with standardized names. For details, see "Attach Business Transactions to a SAP Transaction Using the Naming Convention" on page 37.

➤ Creation of the Business Process container and connection of the appropriate Business Transactions to this container. A Business Transaction connected manually to the SAP transaction would also be connected to this container. For details, see "Attach Business Transactions to a SAP Transaction Without Following the Naming Conventions" on page 38.

Tasks

How to View SAP Information in Service Health

This section describes the processes to follow to display SAP information in Service Health.

This task includes the following steps:

➤ "Prerequisites" on page 27

➤ "Deploy Application Management for SAP" on page 28

➤ "Run the SAP discovery process" on page 28

➤ "Create Application CIs" on page 28

➤ "Create monitors" on page 28

➤ "Modify the SiteScope assignment" on page 29

➤ "Display SAP information in Service Health" on page 29

➤ "Add an application server to the SAP System" on page 29

1 Prerequisites

Ensure that the following software is installed before you install the SAP solution:

➤ **Data Flow Probe.** Used to perform the discovery of SAP topology in your organization. For details, see "SAP" in the *RTSM Data Flow Management Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.

➤ **SiteScope.** Used to integrate the SiteScope data collector into the Application Management for SAP solution. For details, see the *HP SiteScope Deployment Guide* PDF.

➤ **BPM.** Used to integrate the BPM data into the Application Management for SAP solution. For details, see "Introducing Business Process Monitor" in *the Business Process Monitor Administration* PDF.

Make sure that you also have a SAP license to view the SAP Systems view in HP Business Service Management.

Consult the relevant BSM_<version_number>_Release_Notes.pdf for details about the supported versions of SAP.

2 **Deploy Application Management for SAP**

For task details, see "How to Deploy Application Management for SAP" on page 31.

3 **Run the SAP discovery process**

You run the SAP discovery process to discover SAP elements and SAP topology. For task details, see "SAP" in the *RTSM Data Flow Management Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.

4 **Create Application CIs**

Use Applications CIs to simulate SAP users to obtain performance and availability information on the SAP transactions.

For concept details, see "How to Use Application, Business Transaction Flow, and Business Transaction CIs to Simulate SAP Users" on page 35.

5 **Create monitors**

You can create a SAP CCMS monitor and general SiteScope monitors to get the complete picture: Database Query Monitor, Ping Monitor, and so on. For task details, see "How to Create SiteScope Monitors" on page 34.

Note: The SAP CCMS Monitor is an optional SiteScope feature whose license is provided with the SAP solution.

---

6 **Modify the SiteScope assignment**

If required, you can modify the existing SiteScope assignments. For user interface details, see "Assignments Tab" in *Using Service Health*.

7 **Display SAP information in Service Health**

You can display SAP information in Service Health in different views and reports. For details, see "How to Display SAP Information in BSM" on page 48.

8 **Add an application server to the SAP System**

When you add a new application server to the SAP System, you must clear the **Report monitor and related CI topology** option, save the Monitor definition, and then select the option again and save the monitor definition, so the monitor recognizes the new application server. For details on creating a SAP CCMS Monitor, see "SAP CCMS Monitor Overview" in *Monitor Reference* in the SiteScope Help.

🔭 **How to Deploy the SAP CCMS Monitor**

The SAP CCMS monitor retrieves and reports data from SAP's centralized monitoring system CCMS. CCMS is used to monitor all servers, components and resources in the SAP R/3® System from one single centralized server, facilitating problem discovery and problem diagnosis. For concept details, see "SAP CCMS Monitor Overview" in *Monitor Reference* in the SiteScope Help.

Note: The SAP CCMS Monitor is an optional SiteScope feature whose license is provided with the SAP solution.

This task includes the following steps:

➤ "Deploy a CCMS monitor using the SiteScope CCMS Solution Template" on page 30

➤ "Attach SiteScope to BSM" on page 30

➤ "Check that the monitor is set to report all monitors and metrics" on page 30

1 Deploy a CCMS monitor using the SiteScope CCMS Solution Template

The **MonitorSetSSServer.mset** solution template is the most effective way to deploy a CCMS monitor.

To deploy a CCMS monitor using the SiteScope CCMS solution template, see "How to Deploy Monitors Using the Monitor Deployment Wizard" in in *Using System Availability Management* in the SiteScope Help and "SAP CCMS Monitor Overview" in *Monitor Reference* in the SiteScope Help.

2 Attach SiteScope to BSM

Make sure that SiteScope is attached to HP Business Service Management. For user interface details, see "New SiteScope Page" in *Using System Availability Management*.

3 Check that the monitor is set to report all monitors and metrics

To view SiteScope metrics, you must check that the monitor is set to report all monitors and metrics information:

a Select **Admin > System Availability Management**.

b Double-click the relevant SAP CCMS monitor under the appropriate group, select the **Properties** tab, and expand the **HP Integration Settings** area.

c Check that the **BSM Integration Data and Topology Setting** is set to **Enable reporting monitor status and metrics**.

⚓ How to Deploy Application Management for SAP

Deploying the SAP solution includes setting the appropriate licenses, connecting SAP Java Connector on the SiteScope machine, and setting the Data Flow Probe.

This task includes the following steps:

- ➤ "Set the license for the SAP solution" on page 31
- ➤ "Check that the jobs are deployed" on page 32
- ➤ "Set the SiteScope license" on page 32
- ➤ "Configure the SAP CCMS Monitoring Environment" on page 33
- ➤ "Restart the Data Flow Probe" on page 33

1 Set the license for the SAP solution

If the SAP solution license was set while installing BSM, the SAP jobs are automatically deployed and added to the RTSM.

To set the license for the SAP solution.

- **a** Log on to BSM.
- **b** Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**.
- **c** Click **Add license from file** to open the **Add license** page where you can search for the relevant **.dat** file and click **Add license**.
- **d** In the lower part of the License Management page, locate and click the link in the **Note: To activate licenses, go to Server Deployment page**.
- **e** In the Server Deployment page that opens, select the **SAP** (**Application Management for SAP**) option in the **Applications** column and click **Save**.

It is recommended to restart HP Business Service Management.

2 **Check that the jobs are deployed**

If the SAP solution license was set after installing HP Business Service Management, you must deploy the jobs manually or restart BSM so that the SAP jobs are deployed automatically (this is the recommended procedure).

The SAP-related jobs: **SAP.zip**, **SAP_discovery.zip**, and **SAP_monitoring.zip** are at the following location on the machine on which RTSM is installed: **<Discovery Probe root directory>\root\lib\packages**.

Select **Admin** > **RTSM Administration** > **Modeling** > **IT Universe Manager** and check that the SAP views are listed in the View list in Model Explorer.

For user interface details about Model Explorer, see "Working with the CI Selector" in *Modeling Guide*.

3 **Set the SiteScope license**

To set the SiteScope license appropriate for your system:

a Launch SiteScope by entering the following URL in a browser: **http://<SiS_machine_name>:8080**

b Choose **Preferences** > **General Preferences**.

c In the **Licenses** pane, click **Select**.

d In the dialog box that opens, select the relevant file and click **Open**.

e Click **Import**. The license is entered in the **License file** box.

f The relevant information is displayed in the **Installed Licenses** table.

Make sure to insert a license for: EMS monitors, SAP monitors, and the SAP R/3 solution template.

g Click **OK** to approve the changes.

For details, see "SiteScope Licenses" in the *HP SiteScope Deployment Guide* PDF.

4 Configure the SAP CCMS Monitoring Environment

Configure the SAP CCMS monitoring environment by downloading the SAP Java Connector, enabling the SAP CCMS monitor, and configuring the monitor's properties. For details, see "How to Configure the SAP CCMS Monitoring Environment" in *Monitor Reference* in the SiteScope Help.

5 Restart the Data Flow Probe

Perform the following steps:

a On the Data Flow Probe machine, access: **Start** > **Programs** > **HP UCMDB** > **Start Data Flow Probe (console)**

This starts the Data Flow Probe and opens a command console.

b Wait until the console displays the following line: **Finished startup sequence**

🔧 How to Create SiteScope Monitors

You create a SAP CCMS monitor and general SiteScope monitors to get the complete picture of your system.

This task includes the following steps:

➤ "Create a SAP CCMS monitor" on page 34

➤ "Create general monitors" on page 34

1 Create a SAP CCMS monitor

The SAP CCMS monitor retrieves and reports data using SAP centralized monitoring system CCMS. CCMS is used to monitor all servers, components, and resources in the SAP R/3® System from one single centralized server facilitating problem discovery and problem diagnosis.

For details on creating a SAP CCMS Monitor, see "SAP CCMS Monitor Overview" in *Monitor Reference* in the SiteScope Help.

SAP CCMS Monitor solution template is the most effective way to deploy a CCMS monitor. For task details, see "Deploy a CCMS monitor using the SiteScope CCMS Solution Template" on page 30.

2 Create general monitors

You create general SiteScope monitors to get the complete picture of your system. For example, you could use the Database Query monitor to monitor the availability and proper functioning of your database application, or the Ping monitor to discover if your network connection is congested.

For details, see "How to Deploy a Monitor" in *Using SiteScope* in the SiteScope help.

⚒ How to Activate the SAP Service

The SAP Service is activated by default. Check that it is activated and if necessary, activate it manually. For details, see "High Availability for the Data Processing Server" in the *HP Business Service Management Deployment Guide* PDF.

1 In the browser, enter (using JMX log on credentials):
http://<BSM server name>:8080/jmx-console/

2 Double-click **service=Verticals External Enrichment Service** listed under **Topaz**.

3 The JMX MBean View for Verticals External Enrichment Service opens.

4 Specify:

> ➤ **performLinkage.** The customer ID and the name of the relevant linkage to perform (**BPM_Auto/BPM_MANUAL/SiteScope manual**).

> ➤ **createTqlListeners.** Use for debugging.

> ➤ **Start.** Starts the service.

> ➤ **Stop**. Stops the service.

⚒ How to Use Application, Business Transaction Flow, and Business Transaction CIs to Simulate SAP Users

Use Application, Business Transaction Flow, and Business Transaction CIs to simulate SAP users and obtain performance and availability information on the SAP transactions.

You can view Business Transactions under the SAP view to enable you to analyze what happens in the SAP system.

This task includes the following steps:

➤ "Create Application, Business Transaction Flow, and Business Transaction CIs" on page 36

➤ "Select the appropriate protocol" on page 36

➤ "Select the appropriate run-time settings" on page 36

➤ "Edit the script" on page 36

➤ "Attach Business Transactions to SAP Application components" on page 37

1 Create Application, Business Transaction Flow, and Business Transaction CIs

You create the required Application, Business Transaction Flow, and Business Transaction CIs in End User Management. For task details, see "How to Set up Business Process Monitors" in *Using End User Management.*

2 Select the appropriate protocol

In HP Virtual User Generator (VuGen), SAP scripts are recorded using the SAPGUI protocol. You must select the SAPGUI protocol when you create a new script. For details, see the *HP Virtual User Generator User's Guide.*

3 Select the appropriate run-time settings

In VuGen, open the Run-Time settings window, and select the **SAPGUI:General** node. Select **Show SAP client during replay** and clear **Take Active screenshots during replay** to give more accurate user experience times. For details, see the *HP Virtual User Generator User's Guide.*

4 Edit the script

You can edit the script to make sure the password is recorded properly and to check and correct the script's connection parameters.

For details, see "Business Process Monitor Application Configuration Wizard" and "Business Transaction Flow Configuration Wizard" in *Using End User Management.*

5 Attach Business Transactions to SAP Application components

To display Performance and Availability information, Business Transactions must be attached to SAP transactions.

You can connect Business Transactions to a SAP transaction in two different ways:

Type of Connection	Description
Attach Business Transactions to a SAP Transaction Using the Naming Convention	Following the naming convention listed below, logically connects Business Transactions to a SAP transaction.
	Use the following format for the Business Transaction name: **<tran_name>_ _<sys_name>_ _<BPM_tran_name>**
	➤ **tran_name.** The name of the SAP transaction to which you want to attach the Business Transaction.
	➤ **sys_name.** The name of the SAP System on which the transaction is run (for example, MI7).
	➤ **BPM_tran_name.** The unique name of the Business Transaction.
	Any set of alphanumeric and mixed case characters is supported (special characters are not permitted). It is good practice to name the transaction so that the name indicates what occurs in that set of dialog steps.
	Note: You assign the appropriate name to a Business Transaction when you record it. For details, see the *HP Virtual User Generator User's Guide*.
	Example: The names of the Business Transactions assigned to the SAP transaction VA01 in the MI7 SAP System should start with: va01_ _mi7_
	In the SAP Systems View, a **Business Transactions** CI that is displayed under a specific SAP transaction is a container for all relevant transactions.
	It is important to split a SAP transaction into a few BPM transactions so that you are able to pinpoint the problem. For example, if each step of the SAP transaction is a separate BPM transaction, you can find the exact part of the SAP transaction where the problem occurs.

Type of Connection	Description
Attach Business Transactions to a SAP Transaction Without Following the Naming Conventions	If you do not want to follow the naming conventions for the Business Transactions, you must manually link a Business Transaction to a SAP transaction.
	1 Select **Admin > End User Management**, and build an application with BPM configuration.
	2 To manually connect Business Transactions with SAP transactions, select **Admin > RTSM Administration > Modeling > IT Universe Manager**, and select **SAP Systems View** in the **View** list. Right-click the SAP transaction that you want to monitor using the BPM application and select **Attach Related CI** to open the Insert Relationship dialog box. Select one of the monitor views (System Monitors view or End User Monitors view) in the **Views** list. Expand and select the Business Transaction to which you want to connect the SAP transaction, and select the **Monitored By for SAP** relationship type, as well as the **Allow CI Update** option.
	For user interface details, see "Insert Relationship Dialog Box" in the *Modeling Guide*.

🔍 **Troubleshooting and Limitations**

This section describes troubleshooting and limitations for Application Management for SAP.

This section includes the following topics:

➤ "The SAP KPI Status Remains Not Up to Date" on page 39

➤ "CCMS Does Not Manage to Monitor a SAP System" on page 40

➤ "The Performance and Availability KPIs Remain Uninitialized" on page 40

➤ "SAP BPM Scripts Do Not Execute" on page 41

➤ "Unable to Log On HP Business Service Management" on page 41

The SAP KPI Status Remains Not Up to Date

If the SAP KPI status remains **Not up to date** 💬 check the following solutions in the order listed below:

1 Synchronize SiteScope and BSM. In SiteScope, select **Integration Preferences** > **BSM Integration Preferences Dialog Box** > **BSM Preferences Available Operations**. For details, see "BSM Integration Preferences Dialog Box" in *Using SiteScope* in the SiteScope Help.

2 Check the following file to ensure that the samples arrive to the Business Logic Engine:
<HPBSM root directory on the Gateway Server> \log\marble_matcher\MarbleMatcher.log

3 Check that the samples arrive to the bus in the following file:
<HPBSM root directory on the Gateway Server> \log\wde\wdePublishedSamples.log

4 Check that the samples are sent in the following file:
<SiteScope root directory>\logs\topaz_all.log.1

5 If you see KPIs with the **Not up to date** status, check the threshold definition in System Availability Management.

6 Restart SiteScope, detach it, and re-attach it.

7 Check time synchronization between BSM and its management database.

CCMS Does Not Manage to Monitor a SAP System

If CCMS does not manage to monitor a SAP System, check the following solutions in the order listed below:

1 If you are able to connect to the SAP System using SAP Logon, run the **rz20** transaction.

2 Open **SAP CCMS Monitor Templates** > **Entire System**, and check if a tree is displayed.

➤ If there is no tree, there may be a problem with the job that is collecting CCMS information. Contact your SAP administrator.

➤ If there is a tree, check that the names of the application server and system match, in content and case, the ones used in SiteScope.

The Performance and Availability KPIs Remain Uninitialized

If the Performance and Availability KPIs remain uninitialized, check the following solutions in the order listed below:

1 Check that the samples arrive, in the file:
**<HPBSM root directory on the Gateway Server>
\log\marble_matcher\MarbleMatcher.log**

2 Try and run BPM as a specific user. For details, see "Set User Credentials" in the *Business Process Monitor Administration* PDF.

3 Check time synchronization between HP Business Service Management and its Management database.

4 Check the minute's synchronization between BPM and HP Business Service Management.

SAP BPM Scripts Do Not Execute

If the SAP BPM scripts do not execute, check the following solutions in the order listed below:

1 Verify that SAP Logon is installed on the BPM server.

2 Check that the SAP BPM scripts run in HP Virtual User Generator (VuGen) and check the script's connection parameters. For details, see "Edit the script" on page 36.

3 Register DLLs under **<Business_Process_Monitor_install_directory>\bin**, as follows:

➤ **regsvr32 SapGuiActiveScreen.dll**

➤ **regsvr32 SapGuiReplayEvents.dll**

➤ **regsvr32 ActiveScreen.dll**

Unable to Log On HP Business Service Management

If you are unable to log on HP Business Service Management, check the following solutions in the order listed below:

1 Check that the last line in the following file:
<HPBSM root directory on the Gateway Server>\log\jboss_boot.log
displays the following information: Jboss .... started in ...

2 If you are able to connect using port **8080** explicitly, give the **Read and Execute** permission to **Everyone** for the following DLLs in **<Windows installation directory>\System32**:

➤ **msvcr71.dll**

➤ **msvcp71.dll**

➤ **mfc71.dll**

➤ **atl71.dll**

3 If SiteScope is installed on the same machine as HP Business Service Management, check that HP Business Service Management is already running before you start SiteScope.

Tip: It is not recommended to install HP Business Service Management and SiteScope on the same machine.

An existing BPM machine can be leveraged for running SAP scripts as well.

2

Application Management for SAP Reports and Views

This chapter includes:

Concepts

Tasks

Reference

Concepts

🔷 SAP Systems View

After configuring Application Management for SAP, you can view SAP information in the SAP Systems view in Service Health. For user interface details, see "Service Health Workspace" in *Using Service Health*.

For details on configuring Application Management for SAP, see "How to View SAP Information in Service Health" on page 27.

The data displayed in the views is taken from the BPM and SiteScope samples. For details, see "Data Samples for Business Process Monitor" and "Data Samples for SiteScope" in *Reports*.
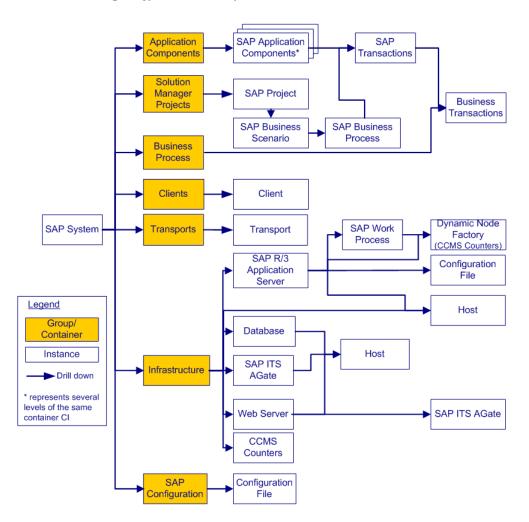
For additional information about views, see "View Topology" in *Using Service Health*.

The SAP Systems view in Model Explorer appears as follows:

To access SAP Systems TQL, select **Admin > RTSM Administration > Modeling > Modeling Studio > Application > SAP > SAP Systems**.

The following graphic shows the various layers and drilldowns available in the topology of the SAP Systems view.
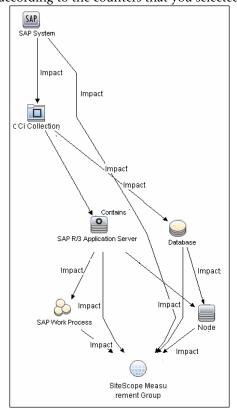
Topologies

In addition, the SAP Systems view includes the following topologies, which are created by specific SiteScope monitors:
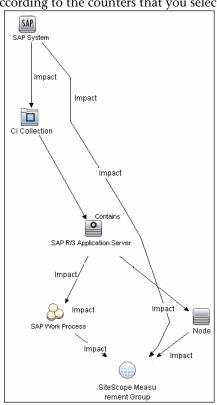
SAP CCMS topology discovered by SiteScope	SAP Work Processes topology discovered by SiteScope
SiteScope creates the following topology for the SiteScope SAP CCMS monitor. The CIs are created only for the monitored entities according to the counters that you selected.	SiteScope creates the following topology for the SiteScope SAP Work Processes monitor. The CIs are created only for the monitored entities according to the counters that you selected.

Limitation for the SAP CCMS topology: SiteScope does not have information about the machine on which the database is installed, therefore, in the SAP CCMS topology, it attaches the Database CI to the Node CI you specified in the Application Server field in the SiteScope monitor definition.

CCMS Counters

The CCMS Counters Dynamic Nodes collect the samples from SiteScope and display the metrics as the SAP General health indicator attached to the CIs representing the elements they are monitoring.

To view the SAP General health indicator details, select **Applications > Service Health**, click 360° View, open the SAP Systems view, select the relevant CI and click the **Health Indicator** tab in the lower pane of the 360° View. For details about the Health Indicator tab, see "Health Indicator Component User Interface" in *Using Service Health*.

Tasks

How to Display SAP Information in BSM

You can display SAP information in Service Health using one of the following capabilities.

This task includes the following steps:

➤ "View SAP data in Service Health" on page 48

➤ "View the CIs impacted by a root cause CI" on page 48

➤ "View changes made to SAP System CIs" on page 48

➤ "Display Configuration File information" on page 49

1 View SAP data in Service Health

You can view SAP information in the SAP Systems view in Service Health. For concept details, see "SAP Systems View" on page 44.

2 View the CIs impacted by a root cause CI

Select a CI, which is defined by an impact link as a root cause CI, to display all of the CIs that are affected by it. For user interface details, see "Show Impacting SAP Transport Transactions Report" on page 56.

3 View changes made to SAP System CIs

Changes made to the properties of all types of CIs are discovered by different types of discoveries. For details, see "Run the SAP discovery process" on page 28. Those changes are displayed in the Change report available as a right-click menu option for each one of the relevant CI types. For user interface details, see "CI Change Report Page" in *Reports*.

Some of the changes made to the SAP Transactions CIs are caused by the corresponding Transport CIs. Those specific changes are processed by impact links in discovery and are displayed in the SAP Transaction Changes report. The SAP Transaction Changes report displays and track changes made to a SAP Transaction CI when a transport was discovered. For user interface details, see "SAP Transaction Changes Report" on page 59.

4 **Display Configuration File information**

You can display additional information for the Configuration File CIs. For details, see "Configuration File Page" on page 55.

Reference

🔍 Default CIs in the SAP Systems View

The SAP System CIs are listed in the following table:

CI Type (A-Z)	Description
Application Gateway	An Internet Transaction Server (ITS) component.
	The CI establishes the connection to the R/3 System and performs the processing of tasks that are required to move data between R/3 applications and the Internet.
Business Transaction	These CIs are emulated SAP transactions executed on a Business Process Monitor machine. They are used to supply proactive monitoring of end user experience.
Business Transaction Flow	A logical container that contains all of the Business Transaction CIs attached to all of the SAP transactions.
CCMS Counters	These CIs are information elements, relevant to SAP, retrieved from SAP CCMS (Computer Center Management System).
Client	An organizational and legal CI in the SAP system. The main objective of the client is to keep the data isolated. The data in a client can only be visible within that client; it cannot be displayed or changed by another client. Each client on a system can represent a unique working environment.
Configuration File	The system/servers configuration parameters.
Contained Locations	These CIs are created as part of the Business Process Monitor hierarchy when working with the Transactions/locations option.

CI Type (A-Z)	Description
Database	A database management system holding the data tier, including all of the SAP elements: SAP transactions, programs, work processes, and so on. This is not a SAP-specific CI.
Monitor	SiteScope entities used to monitor the various CIs that exist in the RTSM. The monitors that are most likely to appear in the SAP view are host monitors: CPU, memory, disk space, and so on. These monitors appear in the SAP view only if they are manually attached to the Node CI.
Node	A Node CI represents the physical machine on which a server is installed. This is not a SAP-specific element.
R/3 Application Server	SAP R/3 Application Server is SAP's integrated software solution for client/server and distributed open systems. R/3 Application servers and databases are displayed under Nodes. You can also have several levels of hosts under the Nodes CI, SiteScope Monitor CIs, and CCMS Monitor CIs.
SAP Application Component	May include other SAP Application Components and some SAP transactions with some common denominator.
SAP Applications	A logical unit, grouping together Application Components.
SAP System	A logical unit, grouping together SAP-related CIs (and possibly other CIs as well) into one homogeneous SAP deployment.
SAP Transaction	Part of a business process defined in the SAP System. It consists of request-response couples called dialog steps. The end user uses SAP transactions to carry out actions on the SAP System.
Solution Manager Projects	Includes SAP Business Project CIs, SAP Scenario CIs, SAP Business Process CIs, and SAP Business Process Step CIs. Solution Manager Projects hierarchy is specified by the user in SAP Solution Manager.

CI Type (A-Z)	Description
Transports	Represents packaged change requests that include the changes that are to be deployed on the system.
Web Gateway	An Internet Transaction Server (ITS) component. A web server extension that establishes the connection between ITS and the Web server and forwards user requests to the Application Gateway.
Work Processes	A logical, single-instance representation of all of the work processes of the same type existing on the R/3 server. Several types of work processes are available: ➤ **Dialog Work Process.** Executes dialog programs (ABAP). ➤ **Update Work Process.** Responsible for asynchronous database changes (controlled by a COMMIT WORK statement in a dialog work process). ➤ **Update2 Work Process.** Used for statistical, non-critical updates (for example, result calculations). ➤ **Background Work Process.** Executes time-dependent or event-controlled background jobs. ➤ **Enqueue Work Process.** Executes locking operations (if SAP transactions have to synchronize themselves). ➤ **Spool Work Process.** Performs print formatting (to printer, file, or database).

⚛ SAP-Related KPIs

Different Key Performance Indicators (KPIs) are displayed depending on the selected CI. For details on the displayed KPIs, see "Default CIs in the SAP Systems View" on page 50.

The following table lists the SAP-related KPIs displayed in the Console tab:

UI Element (A-Z)	Description
SAP	The SAP KPI indicates problems related to the SAP infrastructure that are reported by CCMS.
Transactions	At the group level, displays the worst status of all of the child CIs. At the monitor level, displays the worst status of the **Performance** and **Availability** KPIs for the CI.

The other KPIs displayed in the views are not SAP-related. For more details on those KPIs, see "List of Service Health KPIs" in *Using Service Health*.

⚛ SAP-Related Menu Options

A list of all of the shortcut menu options available in the SAP Systems view is available in "Service Health Menu Options" in *Using Service Health*.

Different menu options are available depending on the type of CIs:

➤ **Show SAP Transport Impact.** For details, see "Show SAP Transport Impact" in *Using Service Health*.

➤ **Show Impacting SAP Transports.** For details, see "Show Impacting SAP Transports" in *Using Service Health*.

➤ **SAP Transport Changes.** For details, see "SAP Transport Changes" in *Using Service Health*.

➤ **SAP Transaction Changes.** For details, see "SAP Transaction Changes" in *Using Service Health*.

🔍 Application Management for SAP User Interface
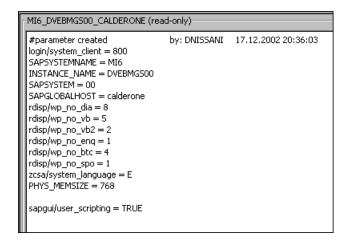
This section describes:

➤ Configuration File Page on page 55

➤ Show Impacting SAP Transport Transactions Report on page 56

➤ Show Impacting SAP Transports Report on page 57

➤ Show SAP Transport Impact Report on page 58

➤ SAP Transaction Changes Report on page 59

➤ SAP Transport Changes Report on page 61

🔩 Configuration File Page

This page displays the contents of the configuration file. Details on the SAP configuration file are provided in the SAP product documentation.

The following is an example of the Configuration File page.

```
┌─ MI6_DVEBMGS00_CALDERONE (read-only) ───────────────────┐
│                                                          │
│  #parameter created          by: DNISSANI   17.12.2002 20:36:03
│  login/system_client = 800                               │
│  SAPSYSTEMNAME = MI6                                      │
│  INSTANCE_NAME = DVEBMGS00                                │
│  SAPSYSTEM = 00                                           │
│  SAPGLOBALHOST = calderone                                │
│  rdisp/wp_no_dia = 8                                      │
│  rdisp/wp_no_vb = 5                                       │
│  rdisp/wp_no_vb2 = 2                                      │
│  rdisp/wp_no_enq = 1                                      │
│  rdisp/wp_no_btc = 4                                      │
│  rdisp/wp_no_spo = 1                                      │
│  zcsa/system_language = E                                │
│  PHYS_MEMSIZE = 768                                       │
│                                                          │
│  sapgui/user_scripting = TRUE                            │
│                                                          │
└──────────────────────────────────────────────────────────┘
```
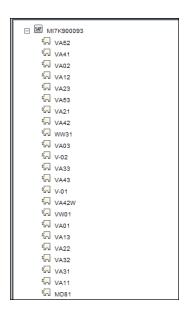
To access	Select **Admin** > **RTSM Administration** > **Modeling** > **IT Universe Manager**, select SAP Systems view, right-click Configuration File CI and invoke its properties, navigate to the **DocumentContent** property and invoke its value by pressing on the ellipsis button.

🔭 Show Impacting SAP Transport Transactions Report

This report enables you to display all SAP transactions that are affected by the selected transport.

The following is an example.

To access	In Service Health, access the **SAP Systems** view and click the gray arrow ▾ to the right of the CI, or right-click the appropriate CIs and select **Show Impacting SAP Transport Transactions**.
Important information	For details on impact rules, see "Impact Analysis Manager" in the *Modeling Guide*.
Relevant tasks	"How to Display SAP Information in BSM" on page 48

✎ Show Impacting SAP Transports Report

This report enables you to display all of the selected CIs and their child CIs that were impacted by any SAP Transport CIs.

The following is an example of the impacting SAP Transports report.

To access	In Service Health, access the **SAP Systems** view and click the gray arrow ▾ to the right of the CI, or right-click the appropriate CIs and select **Show Impacting SAP Transports**. For details about the appropriate CIs see **Important information**.
Important information	"How to Display SAP Information in BSM" on page 48
	This option is available for SAP-specific Transaction and group CIs.
	For Transaction CIs, it enables you to display the transports that are affecting the selected Transaction CI, with no historical limit to the information.
	Collection CIs represent the following CIs: SAP System and SAP Application Component.
	For details on impact rules, see "Impact Analysis Manager" in the *Modeling Guide*.
Relevant tasks	"How to Display SAP Information in BSM" on page 48

🔍 Show SAP Transport Impact Report

This report display all SAP transactions that are affected by the selected transport.

The following is an example of the SAP Transport Impact report.
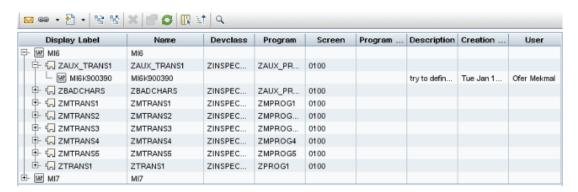
Description	In Service Health, access the **SAP Systems** view and click the gray arrow ▼ to the right of the CI, or right-click the appropriate CIs and select **Show SAP Transport Impact**.
Important Information	For details on correlation rules, see "Impact Analysis Manager" in *Modeling Guide*.
Included in Tasks	"How to Display SAP Information in BSM" on page 48

SAP Transaction Changes Report

This report enables you to display all the transactions and transport CIs that affect the selected SAP application.

The following is an example of the SAP Transaction Changes report.

Display Label	Name	Devclass	Program	Screen	Program ...	Description	Creation ...	User
MI6	MI6							
ZAUX_TRANS1	ZAUX_TRANS1	ZINSPEC...	ZAUX_PR...	0100				
MI6K900390	MI6K900390					try to defin...	Tue Jan 1...	Ofer Mekmal
ZBADCHARS	ZBADCHARS	ZINSPEC...	ZAUX_PR...	0100				
ZMTRANS1	ZMTRANS1	ZINSPEC...	ZMPROG1	0100				
ZMTRANS2	ZMTRANS2	ZINSPEC...	ZMPROG...	0100				
ZMTRANS3	ZMTRANS3	ZINSPEC...	ZMPROG...	0100				
ZMTRANS4	ZMTRANS4	ZINSPEC...	ZMPROG4	0100				
ZMTRANS5	ZMTRANS5	ZINSPEC...	ZMPROG5	0100				
ZTRANS1	ZTRANS1	ZINSPEC...	ZPROG1	0100				
MI7	MI7							

To access	In Service Health, access the **SAP Systems** view and click the gray arrow ▾ to the right of the CI, or right-click a SAP System CI or a SAP Transaction CI and select **Reports > SAP Transaction Changes report**.
Relevant tasks	"How to Display SAP Information in BSM" on page 48

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Common report settings>	See "Common Report and Page Elements" in *Reports*.
Creation Date	The date when the transport was created.
Description	The description of the transport.
Devclass	The development class that includes the transaction.

UI Element (A-Z)	Description
Display Label	The internal name of the CI, and the topology of Transaction and Transport CIs that affect the Application CI.
Name	The name of the CI corresponding to the Application, Transaction, or Transport CI.
Program	The name of the program that runs the transaction.
Program Version	The version of the program that runs the transaction.
Screen	The first screen that opens when you load the transaction.
User	The name of the user who created the transport.

SAP Transport Changes Report

This report enables you to display all the transport CIs that affect the selected SAP application.

The following is an example of the SAP Transaction Changes report.

Display Label	Name	User	Creatio...	Object ...	Object ...	Devclass	Program	Progra...	Screen
⊟ SAP MI7	MI7								
⊟ SAP MI7K900095	MI7K900095	Ofer Me...	Mon Jan ...						
⊟ SAP Include:ZXV...				ZXVVAU...	Include				
MD81	MD81					MDPB	SAPMV4...	127.1	0105
MD82	MD82					MDPB	SAPMV4...	127.1	0102
MD83	MD83					MDPB	SAPMV4...	127.1	0102
V-01	V-01					VA	SAPMV4...	127.1	0101
V-02	V-02					VA	SAPMV4...	127.1	0101
VA01	VA01					VA	SAPMV4...	127.1	0101
VA02	VA02					VA	SAPMV4...	127.1	0102
VA03	VA03					VA	SAPMV4...	127.1	0102
VA11	VA11					VA	SAPMV4...	127.1	0101
VA12	VA12					VA	SAPMV4...	127.1	0102
VA13	VA13					VA	SAPMV4...	127.1	0102
VA21	VA21					VA	SAPMV4...	127.1	0101
VA22	VA22					VA	SAPMV4...	127.1	0102
VA23	VA23					VA	SAPMV4...	127.1	0102
VA31	VA31					VA	SAPMV4...	127.1	0101
VA32	VA32					VA	SAPMV4...	127.1	0125
VA33	VA33					VA	SAPMV4...	127.1	0125
VA41	VA41					VA	SAPMV4...	127.1	0101
VA42	VA42					VA	SAPMV4...	127.1	0102
VA42W	VA42W					VA	SAPMV4...	127.1	0102
VA43	VA43					VA	SAPMV4...	127.1	0102
VA51	VA51					VA	SAPMV4...	127.1	0101
VA52	VA52					VA	SAPMV4...	127.1	0126
VA53	VA53					VA	SAPMV4...	127.1	0126
VRRE	VRRE					VA	SAPMV4...	127.1	0130
VW01	VW01					VAW	SAPMV4...	0.0	0100
WW31	WW31					BBPO	SAPMBB	0.0	1000

To access	In Service Health, access the **SAP Systems** view, and click the gray arrow ▼ to the right of the CI, or right-click a SAP System CI or a SAP Transport CI and select **Reports** > **SAP Transport Changes report**.
Relevant tasks	"How to Display SAP Information in BSM" on page 48

User interface elements are described below (unlabeled elements are shown in angle brackets):

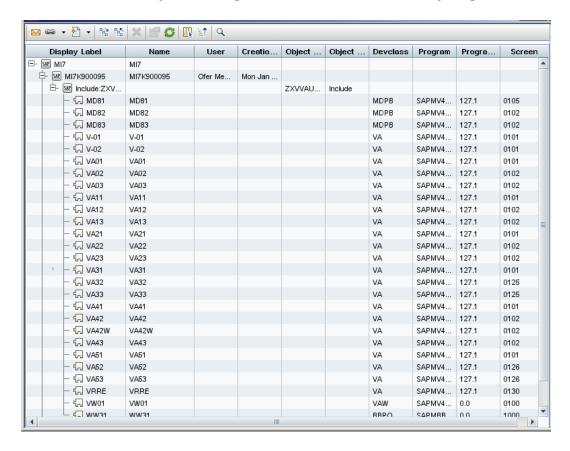| UI Element (A-Z)	Description
<Common report settings>	See "Common Report and Page Elements" in *Reports*.
Creation Date	The date when the transport was created.
Description	The description of the transport.
Devclass	The development class that includes the transaction.
Display Label	The internal name of the CI, and the topology of Transaction and Transport CIs that affect the Application CI.
Name	The name of the transport that has changed.
Object Name	The change that was made.
Object Type	The object that changed.
Program	The name of the program that runs the transaction.
Program Version	The version of the program that runs the transaction.
Screen	The first screen that opens when you load the transaction.
User	The name of the user who created the transport.

Part II

Application Management for Siebel

3

Application Management for Siebel Administration

This chapter includes:

Concepts

Tasks

Reference

Concepts

🔵 Application Management for Siebel – Overview

Application Management for Siebel, integrating SiteScope, BPM, and RTSM, enables you to gain visibility into your mission-critical Siebel applications.

The Siebel solution provides:

➤ A single operation console consolidating all Siebel monitoring information.

➤ Automatic discovery and modeling of Siebel-related elements, as well as their relationships to other systems in the organization's Information Technology (IT) department.

➤ Change discovery and notification for quicker problem resolution.

➤ Proactive monitoring of end-user experience in Siebel enterprises.

➤ The ability to distinguish between Siebel-specific problems and general ones.

➤ Management of Siebel-related service level commitments.

Note: You must have an Application Management for Siebel license to view the Siebel Enterprises view in HP Business Service Management (BSM).

Application Management for Siebel consolidates Siebel components and business processes in the Siebel Enterprises view to gain real-time visibility over the entire Siebel infrastructure from a business perspective.

Application Management for Siebel also monitors, reports, and issues alerts on the performance and functionality of the Siebel eBusiness applications and servers that include your Siebel Enterprise business process infrastructure.

Using Application Management for Siebel, your IT operation can analyze how each link in the Siebel Enterprise chain is impacting the user experience of customers, partners, suppliers, and employees. This enables your IT team to more accurately assess the resulting impact on business performance. It also enables the IT team, Siebel application support team, and Siebel Expert Services to take any steps that might be necessary to maximize availability, performance, and service levels to provide quality of service for all Siebel applications and end users.

The Siebel Enterprises view is available in the Service Health. For details, see "View Configuration File CI details" on page 141.

Right-click the CIs in the Siebel Enterprises view to access additional information and diagnostics tools. For details on the shortcut menu, see "Shortcut Menu Options" on page 144. For details on the diagnostics tools, see "Diagnostics Tools" on page 128.

In addition, you can create SLAs centered around your Application Management for Siebel Siebel Application CIs to gain visibility into performance or availability issues that impact these SLAs. For details on SLAs, see "Service Level Management - Overview" in *Using Service Level Management*.

Application Management for Siebel License
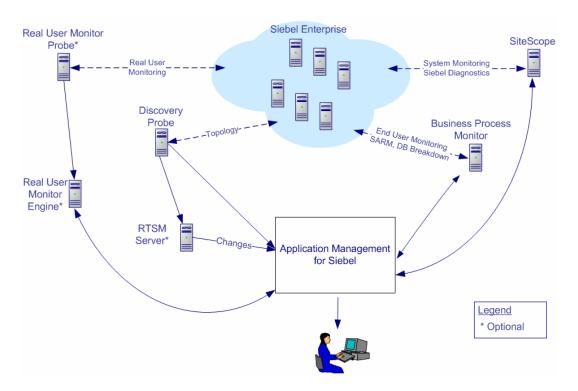
The Application Management for Siebel license unlocks the following functionality in BSM:

➤ The Siebel Enterprises pattern view, displaying a hierarchical view of Siebel applications and infrastructure.

➤ Automatic linkage of BPM transactions to the Siebel transactions they are monitoring.

➤ Automatic linkage of SiteScope measurements to their respective Siebel infrastructure.

➤ Siebel-specific KPIs that enable differentiation between Siebel-related issues and non-Siebel ones.

➤ Siebel diagnostics – SARM, Database Breakdown, Tasks, Processes – for in-depth, in-context data on the Siebel environment.

Architecture

For details about the architecture of Application Management for Siebel, see:

Most of the Siebel CIs are created by automatic discovery. The configuration for these CIs is saved into the Run-time Service Model (RTSM). Some of the relationships to BPM and SiteScope CIs are created by automatic mechanisms specific to the Application Management for Siebel.

The architecture of the Application Management for Siebel solution includes the following components:
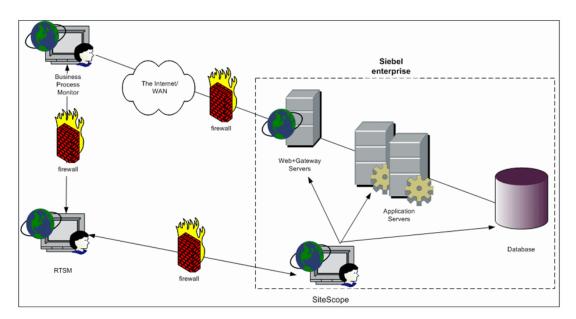
➤ The Data Flow Probe discovers Siebel-related CIs and other CIs (such as hosts) that are related to them.

➤ The Real User Monitor Probe monitors real user traffic and sends the data to the Real User Monitor engine, that processes and stores it.

➤ SiteScope communicates with the Siebel Enterprise system and retrieves system monitoring information using the srvrmgr CLI tool. It is also used as a middleware for all of the Siebel diagnostics tools. Middleware is software that runs in the middle tier of a Three Tier system of User Interface (Front End or Client), Application Server, and Database Server (Backend) and an additional tier that analyzes the output of the program.

➤ Business Process Monitor collects data on the performance and availability of the Siebel Enterprise by running transactions that correspond to Business Transaction Flows. It is also used for Database Breakdown, and can be leveraged in SARM; for example, user sessions can be correlated to the corresponding BPM transactions.

➤ Service Health tabs and reports are used as the central console for viewing all of the data and performing analysis of the data. For concept details, see "Service Health Overview" in *Using Service Health*.

Working with Firewalls

To work with firewalls, you must install a firewall with a Virtual Private Network (VPN) between:

➤ HP Business Service Management and the BPM to view Siebel Application Response Measurement (SARM) - user trace breakdown, database breakdown information, or both.

➤ HP Business Service Management and SiteScope to view all diagnostics information.

The following diagram illustrates a possible deployment involving firewalls:

Siebel Monitors

The following SiteScope monitors are used to monitor Siebel.

➤ **Siebel Application Server.** Uses Siebel Server Manager client to monitor all aspects of Siebel application servers. For details on the monitor, see "Siebel Application Server Monitor Overview" in *Monitor Reference* in the SiteScope Help.

➤ **Siebel Web Server.** Watches Siebel server log on session statistics and gauges the performance of Siebel Server Object Managers and database. For details on the monitor, see "Siebel Web Server Monitor Overview" in *Monitor Reference* in the SiteScope Help.

➤ **Siebel Log Monitor.** Monitors the Siebel log files by searching for entries containing a specific event type or subtype. For details on the monitor, see "Siebel Log File Monitor Overview" in *Monitor Reference* in the SiteScope Help.

These monitors must be deployed. For details, see "How to Deploy the SiteScope Siebel Monitors" on page 86.

The Siebel Service

The Siebel Service is a configuration service that provides the following advantages:

➤ Automatic linkage of SiteScope measurements to the relevant CIs based on the measurement name.

➤ Creation of a Business Process and Locations containers and connection of the Business Transaction Flows monitoring Siebel, and their respective locations, to these containers.

For details on how to view a service status with the JMX Web console, see "High Availability for the Data Processing Server" in the *HP Business Service Management Deployment Guide* PDF.

The Siebel Service must be activated. For details, see "Activate the Siebel Service" on page 76.

Tasks

🔧 How to Deploy Application Management for Siebel

This section describes the processes to follow to view Siebel data in Service Health, and gives examples.

This task includes the following steps:

1 Prerequisites

Consult the relevant BSM_<version_number>_Release_Notes.pdf for details about the supported versions of Siebel.

Ensure that the following software is installed before you install Application Management for Siebel:

Software	Comments
SiteScope	Used to integrate the SiteScope data collector into the Application Management for Siebel solution. For details, see the *HP SiteScope Deployment Guide* PDF. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the SiteScope product. **Note:** ➤ SiteScope monitors are not tested for SiteScope UNIX installation. ➤ If the SiteScope machine is located outside the HP Business Service Management LAN, you must configure the Virtual Private Network (VPN) to enable SiteScope to communicate with the HP Business Service Management Gateway Server.
Siebel	Install the applications you want to integrate into HP Business Service Management. For details, see the Siebel documentation. For details about the environments that support Siebel see the BSM_<version_number>_Release_Notes.pdf.
Siebel Server Manager	Install the Siebel Server Manager version that is appropriate for the Siebel version you have installed.
Siebel Application Response Measurement (SARM)	Install the version of the Siebel Application Response Measurement Analyzer (SARM) package that is appropriate for the Siebel version you have installed. If you are working with SARM in Siebel version 7.8, use SARM Analyzer for Siebel version 7.7.
Data Flow Probe	Used to perform the discovery of Siebel topology in your organization. For details, see "Siebel Discovery" in the *RTSM Data Flow Management Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.

Software	Comments
Business Process Monitor	Used to integrate the BPM data collector into the Application Management for Siebel. For task details, see "Business Process Monitor Administration" in *Using End User Management*.
Real User Monitor - Optional	Used to integrate the Real User Monitor Probe to monitor real user traffic and to send it to the RUM engine, that processes and stores it. For task details, see "Real User Monitor Administration" in *Using End User Management*.

2 Check the Siebel license in BSM

Check that the appropriate Siebel licenses are set in HP Business Service Management:

➤ The license for running the Application Management for Siebel.

➤ The license to enable the necessary amount of Business Transaction Flows to run.

➤ The SiteScope license.

To check that the licenses are set properly or to update the licenses, select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**.

3 Check the Siebel license in SiteScope

Check that the license that enables the definition of SiteScope Siebel monitors and deployment of Siebel solution templates is set properly in SiteScope. For concept details, see "Siebel Solution Templates" in *Using SiteScope* in the SiteScope help.

4 Deploy the Siebel Monitoring package

Deploy the Siebel Monitoring package. For details, see "Deploy a Package" in the *RTSM Administration Guide*.

5 Copy the srvrmgr tool to the Data Flow Probe server
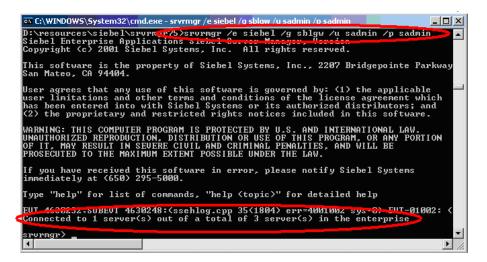
The srvrmgr tool is used to extract data about the enterprise's structure from Siebel.

Note: If you are working with different versions of Siebel in your organization, make sure you use a srvrmgr with a version that is appropriate for the Siebel server.

To copy the srvrmgr tool to the Data Flow Probe server, proceed as follows:

a Copy the srvrmgr Command Line Interface (CLI) tool from the Siebel server to any folder on the Data Flow Probe server. It is recommended to run the Siebel connection test to validate the srvrmgr installation.

b To run the connection test, open the command line on the Data Flow Probe server and change directory to the location of the **srvrmgr.exe** file. Run from the command line:
>**srvrmgr /e [site_name] /g [gateway_host] /u [username] /p [password]**

If the connection is established successfully, the srvrmgr prompt and the status message about the number of connected servers, are displayed as follows:

 6 Copy SARM Analyzer and srvrmgr tool to the SiteScope server

On SiteScope, the srvrmgr tool is launched by the Siebel Application Server monitor and is used to get the metrics.

SARM Analyzer is used for analyzing SARM data, so that it can be displayed in Application Management for Siebel's SARM - User Trace Breakdown tab.

For task details, see "Copy the srvrmgr Tool and the SARM Analyzer Tool to the SiteScope Server – Details" on page 78.

 7 Run the Siebel discovery process

You run the Siebel discovery process to discover Siebel elements and Siebel topology. For concept details, see "Discover Siebel Topology" in the *RTSM Data Flow Management Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.

 8 Configure specific Siebel CIs manually

When you run the Siebel discovery, the process creates CIs for the discovered components in the RTSM. In addition to the CI's properties that are automatically defined by the discovery process, you must manually define some properties so the Monitor Deployment Wizard and the Siebel diagnostics tools can run correctly. For details, see "Siebel CIs Properties" on page 96.

 9 Activate the Siebel Service

The Siebel Service is a configuration service for automatic linkage. The Siebel service is automatically activated when you have entered the appropriate license for HP Business Service Management for Siebel solution. The Siebel Service starts working after CIs are received. For additional information about the Siebel Service, see "The Siebel Service" on page 71.

For details on how to view a service status with the JMX Web console, see "High Availability for the Data Processing Server" in the *HP Business Service Management Deployment Guide* PDF.

Check that the Siebel Service is activated (it is activated only if you have a license). If necessary, activate it manually.

For details on how to view a service status with the JMX Web console, see "High Availability for the Data Processing Server" in the *HP Business Service Management Deployment Guide* PDF.

Tip: If you enter a new license in an old HP Business Service Management installation, you may need to restart the RTSM server to activate the service.

To check if the Siebel Service is active:

a In the browser, enter, using JMX log on credentials:
  **http://<BSM server name>
  :8080/jmx-console/**

b Double-click **service=hac-manager** listed under **Topaz**.

c In the JMX MBean View for hac-manager that opens, click the **Invoke** button corresponding to the **listAllAssignments** parameter.

10 Modify SiteScope KPI assignment group - optional

If required, you can modify the existing SiteScope KPI assignments. For user interface details, see "Assignments Tab" in *Using Service Health*.

11 Configure Application Management for Siebel applications

To monitor your Siebel eBusiness applications and servers using Application Management for Siebel, you must first set up the Siebel monitoring environment. For task details, see "How to Configure Application Management for Siebel" on page 81.

12 **Check that the deployment was successful**

To check that the deployment was successful:

a Run the predefined tests that check that the Application Management for Siebel deployment was successful. For user interface details, see "Siebel Deployment Validator Page" on page 98.

b Fix the problems discovered by failed tests, and rerun the failed tests. For a description of the existing tests and their parameters, see "List of Predefined Tests for Siebel Deployment Validator" on page 100.

c To change the default parameters, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Applications**.

➤ Select **Siebel**.

➤ In the Siebel - Siebel Deployment Validator table, locate **Deployment Validator tests definitions**. Modify the parameter values in the XML file.

13 **Display Siebel information in Service Health**

Application Management for Siebel is ready. After all these steps are completed, you can view Siebel data in the Service Health, use diagnostic tools, and so on. For task details, see "How to Display Siebel Information in BSM" on page 139.

🔧 **Copy the srvrmgr Tool and the SARM Analyzer Tool to the SiteScope Server – Details**

Note: If you are working with different versions of Siebel in your organization, make sure you use a srvrmgr and a SARM Analyzer with a version that is appropriate for the SiteScope server. For details, see "Shortcut Menu Options" on page 144.

This task is part of a higher level task. For details, see "How to Deploy Application Management for Siebel" on page 72. This section provides details on the processes used to copy the srvrmgr tool and the SARM Analyzer tool to the SiteScope server.

This task includes the following steps:

➤ "Copy the srvrmgr tool to the SiteScope server" on page 79

➤ "Copy the SARM Analyzer tool to the SiteScope server" on page 80

➤ "Perform the remote connection from SiteScope to Siebel" on page 80

➤ "Run the SiteScope service with a domain user" on page 81

1 Copy the srvrmgr tool to the SiteScope server

This section describes how to copy the srvrmgr tool to the SiteScope server.
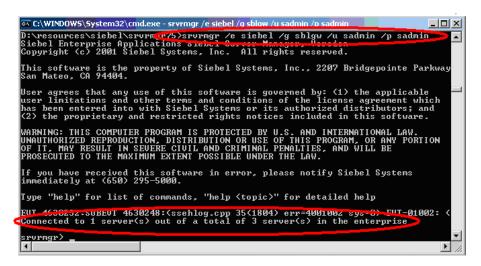
a Copy the srvrmgr Command Line Interface (CLI) tool from the Siebel server to any folder on the SiteScope server.

Tip: It is recommended to run the Siebel connection test to validate the srvrmgr installation.

---

b To run a connection test, open the command line on the SiteScope server and change directory to the location of the **srvrmgr.exe** file.

c Run from the command line:
>**srvrmgr /e [site_name] /g [gateway_host] /u [username] /p [password]**

Note: For the connection to work properly you must check that the user and password you are using have the correct permission for a remote connection. For details, see "Perform the remote connection from SiteScope to Siebel" on page 80.

If the connection is established successfully, you should see the srvrmgr prompt and the status message about the number of connected servers, as follows:

2 Copy the SARM Analyzer tool to the SiteScope server

To copy the SARM Analyzer tool to the SiteScope server, copy the SARM Analyzer tool from the Siebel server to a folder on the SiteScope server.

Tip: If your site includes a large number of Web servers, it is better to use multiple SiteScopes to distribute the work done by the SARM Analyzer tool between these SiteScopes; you can copy SARM Analyzer to each SiteScope.

---

3 Perform the remote connection from SiteScope to Siebel

All Siebel servers (Windows and UNIX) must be defined as remote servers on the SiteScope server. For details, see the "New/Edit Microsoft Windows Remote Server Dialog Box" or "New/Edit UNIX Remote Server Dialog Box" in *Using SiteScope* in the SiteScope help.

4 Run the SiteScope service with a domain user

SiteScope should run under a domain user who has permissions to run server manager and SARMAnalyzer and also has read access to the log folders on the Siebel servers (Web servers and application servers).

⚒ How to Configure Application Management for Siebel

This section describes the detailed steps used to configure the Siebel monitoring environment.

This task includes the following steps:

➤ "Create Business Transaction Flows that emulate Siebel application users" on page 81

➤ "Deploy SiteScope monitors for the Siebel templates using the Monitor Deployment wizard" on page 82

➤ "Configure specific CIs manually" on page 82

➤ "Go through the Diagnostics checklist" on page 82

1 Create Business Transaction Flows that emulate Siebel application users

You can use Siebel transactions to simulate Siebel users and obtain performance and availability information on the Siebel application. You use Business Transaction Flows to group several transactions.

For information about creating Business Transaction Flows, see "How to Use a Business Transaction Flows to Simulate Siebel Users – Details" on page 89.

2 Deploy SiteScope monitors for the Siebel templates using the Monitor Deployment wizard

You can use SiteScope monitors to monitor Siebel. For more information about the monitors, see "Siebel Monitors" on page 70.

For details on deploying the SiteScope Siebel monitors, see "How to Deploy the SiteScope Siebel Monitors" on page 86.

3 Configure specific CIs manually

When you run the Siebel discovery, the process creates CIs for the discovered components in the RTSM. In addition to the CI's properties that are automatically defined by the discovery process, you must manually define some properties so the Monitor Deployment Wizard and the Siebel diagnostics tools can run correctly. For details on the properties you must enter manually, see "Default CITs in the Siebel View" on page 144.

You manually define properties in IT Universe Manager. For details on defining properties for a CI, see "Configuration Item Properties Dialog Box" in *RTSM Administration Guide*.

Note: In addition, you must check that the connection parameters used to connect to SiteScope monitors are the parameters that exist in the various relevant CIs (Enterprise, Application Server, and so forth). For details, see "Troubleshooting Diagnostics Tools" on page 106.

---

4 Go through the Diagnostics checklist

Check that the Diagnostics-related settings are correctly set up to ensure that Diagnostics work properly.

For task details, see "How to Verify Diagnostics-Related Settings" on page 83.

🔨 How to Verify Diagnostics-Related Settings

This section provides details on the Diagnostics-related settings that ensure that Diagnostics work properly.

This task includes the following steps:

➤ "Check the Diagnostics-related settings for Siebel" on page 83

➤ "Check the Diagnostics-related settings for SiteScope" on page 84

➤ "Diagnostics-related settings for BSM" on page 84

1 Check the Diagnostics-related settings for Siebel

Check that:

➤ The SiteScope user has at least read-only access to the log directories of all Web and Application Servers.

➤ The SiteScope user has administrative privileges on all Siebel servers or, if this is not possible, give the permissions specified at the Microsoft Help and Support site (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q300702).

➤ You have defined a special Siebel user to be used by a Business Transaction Flow. This user should be used only for that purpose.

➤ **Siebel Breakdown** is enabled for the script that monitors the Siebel application. For details, see "How to Set up Business Process Monitors" in *Using End User Management*.

➤ **Siebel Server Manager and SARM Analyzer.** Check that:

➤ The **srvrmgr** package and **SARM Analyzer** package are installed on a SiteScope machine (they are needed for running the Diagnostics tools). You copy Siebel Server Manager and the SARM Analyzer to a SiteScope machine (preferably) or, if this is not possible, to another machine where it can be executed by a SiteScope user. For details, see "Copy the srvrmgr Tool and the SARM Analyzer Tool to the SiteScope Server – Details" on page 78.

➤ The SiteScope user on Siebel Server Manager has execution permissions when both SiteScope and Siebel are running on UNIX.

2 Check the Diagnostics-related settings for SiteScope

Check that:

➤ SiteScope service is running under a domain account (not a local system). This domain account (SiteScope user) must have the permissions specified in "Check the Diagnostics-related settings for Siebel" on page 83.

➤ Each Siebel Web and Application Server is defined as Remote NT or Remote UNIX appropriately. Remote UNIX machines must be defined using the Telnet protocol. Additionally, in the **initialize shell environment** field, enter **stty cols 1024; stty tabs; $SHELL**.

➤ SiteScope has access permissions to the Siebel machines. Check that the account SiteScope Service is running in Services (in Windows NT) or in the process (on UNIX).

➤ The **log** and **SARM log** folders on Siebel Web Server and Application Server are accessible from the SiteScope machine.

➤ SiteScope is attached to the Gateway Server.

➤ SiteScope has an additional license for Siebel Monitors.

3 Diagnostics-related settings for BSM

Check that:

➤ All the Application Management for Siebel configuration parameters of the Enterprise, and Siebel Servers are spelled correctly, the appropriate case is used, and there are no blank spaces at the end of the parameter string.

➤ There is no inconsistency in the treatment of the SiteScope host name between the SiteScope profile and System Availability Management (either defined with domain or as an IP address). Also, check that SiteScope can communicate with the Siebel server.

Diagnostics cannot access a SiteScope located in an outer LAN. The solution is to define SiteScope in System Availability Management using the host name provided by the SiteScope server. If the SiteScope server cannot be accessed using such a host name from the Gateway Server the host name must be defined in the hosts file in the operating system of all the Gateway Servers (for Windows NT, the location is: **C:\WINNT\system32\drivers\etc\hosts**; for some UNIX environments, the location is: **/etc/hosts**; in other UNIX environments it is in the **.rhosts** file).

➤ The SiteScope you are using for diagnostics is attached (click **Admin** > **System Availability Management** in HP Business Service Management).

➤ You are using a dedicated SiteScope for diagnostics purposes, when working with medium to large Siebel deployments.

➤ The time zone and time definitions of the SiteScope server used for diagnostic purposes (on which SARM Analyzer and srvrmgr are installed) are synchronized with the Siebel server time zone and time definition.

➤ You have network access (without firewalls or through VPN) to the BPM servers (port **2696**) you are going to use for diagnostics purposes.

➤ For each BPM server used for Diagnostics, you can open the **http:// <BPM_server>:2696/** page from the Gateway Server.

➤ All paths you set in Application Management for Siebel configuration are relative to SiteScope; for example: if they are local on SiteScope (Server Manager, SARM analyzer) use the local path, otherwise use the complete network path.

➤ You have a license for Siebel on the Gateway Server (select **Admin** > **Platform** > **Setup and Maintenance** > **License Management** to verify this).

➤ SiteScope data arrives to HP Business Service Management.

Consult the **dispatcher.txt** log file with the appropriate log level to check that information. You can update the log level of the dispatcher log on the first line of the
<HPBSM root directory on the Gateway Server>
\conf\core\DataService\DataService_logs.ini\dispatcher_log.cfg file. Change the value of **LogLevel** to **debug5**. This causes the samples from SiteScope to appear in the **dispatcher.txt** file.

For details on SiteScope samples, see "Data Samples for SiteScope" in *Reports*.

Tip: It is recommended to increase the log level only for a short period, so HP Business Service Management performance is not impacted.

➤ The user of your Siebel Application in Application Management for Siebel Configuration has appropriate permissions in the Siebel Site and the password is correct.

⚓ How to Deploy the SiteScope Siebel Monitors

This section provides the detailed steps to use to deploy SiteScope Siebel monitors.

You can deploy the Siebel monitors using the Monitor Deployment Wizard or the Siebel solution templates.

Both techniques leverage the concept of solution sets. Solution sets automate the creation of the monitors that should be used, and include built-in threshold information. Essentially, they encompass monitoring best practices.

The task includes the following steps:
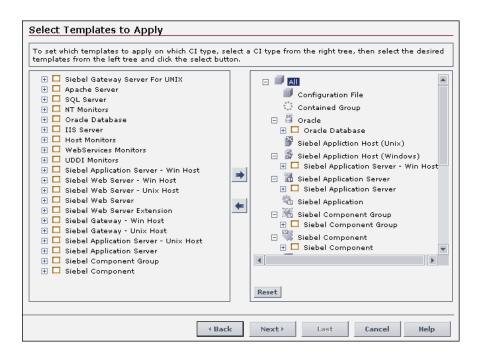
➤ "Use the Monitor Deployment wizard" on page 87

➤ "Using the Siebel solution templates" on page 88

Use the Monitor Deployment wizard

Use the Monitor Deployment Wizard to deploy Siebel monitors. For user interface details, see "Monitor Deployment Wizard" in *Using System Availability Management.*

In the Monitor Deployment wizard, in the left pane of the Select Configuration Items to Monitor page, select the **Siebel Enterprises** view. Select the CIs you would like monitored and move them to the right pane. In the Select Templates to Apply page, the left pane lists all the available templates in the wizard. The names of the Siebel-specific templates start with Siebel. The child objects are the monitors that are deployed by the template. The right pane lists the CI Types of all the CIs selected in the previous page.

If the wizard can match templates to the selected CI Types, the CI Type is listed with the applicable template as a child object:

Note: When deploying monitors on Siebel objects, the CI Types appearing in the right pane may be Siebel CI Types.

Using the Siebel solution templates

To create a SiteScope monitor that can monitor a Siebel Enterprise, you can run dedicated solution templates. Two kinds of solution templates are available for each solution (one for UNIX and one for Windows):

Solution Templates For Unix	Solution Templates For Windows	Description
Siebel Appl Server for UNIX	Siebel Appl Server For Windows	Deploy a set of monitors that test both Siebel-specific and general statistics on the Siebel Application servers.
Siebel Gateway Server For UNIX	Siebel Gateway Server For Windows	Deploy a set of monitors that test machine and OS-oriented statistics of Siebel Gateway servers.
Siebel Web Server For UNIX	Siebel Web Server For Windows	Deploy a set of monitors that test both Siebel-specific and general statistics on Siebel Web servers installed.

For details on running the solution template, see "Siebel Solution Templates" in *Using SiteScope* in the SiteScope documentation library. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the SiteScope product.

🔧 How to Use a Business Transaction Flows to Simulate Siebel Users – Details

This task is part of a higher level task. For details, see "How to Deploy Application Management for Siebel" on page 72.

This task provides details on how to use Business Transaction Flows to simulate Siebel users and obtain performance and availability information on the Siebel application.

You can use Business Transaction Flows to group several transactions.

This task includes the following steps:

➤ "Prerequisites" on page 89

➤ "Select the appropriate protocol" on page 90

➤ "Create Business Transaction Flows" on page 90

➤ "Deploy the SiteScope Siebel monitors" on page 90

➤ "View SARM Data in Business Transaction Flows" on page 91

1 Prerequisites

In the HP HP Virtual User Generator (VuGen), check that:

➤ When recording scripts on VuGen for Siebel, you only use the Siebel-Web protocol. For details see *HP Virtual User Generator User's Guide*.

➤ You record scripts with a special user created for monitoring/diagnostics purposes on Siebel.

➤ You set a think time separator of 10 seconds for the script transactions used for Siebel diagnostics. The VuGen script includes discrete transactions (transactions that do not include **lr_think_time()** within them) and that it uses the **lr_think_time(…)** functions to separate between the VuGen transactions.

➤ The script must not be too long (recommended no more than five transactions per script) since the Diagnostics tools need to run the whole script every time you want to analyze a specific transaction. For example, if a problematic transaction is located close to the end of the script, you would have to run all the previous transactions to reach the problematic one. If you need to record more transactions, record an additional script.

➤ Optionally, the Run-Time Settings should be configured for setting appropriate values: **Think-Time-Replay policy**, **Timeout values**, **logging options**, **Proxy**, **Browser Emulation**, and so on.

You can only use Vugen scripts with Siebel applications.

2 **Select the appropriate protocol**

You must select the Siebel-Web protocol when you create a new script, because, in HP HP Virtual User Generator (VuGen), Siebel scripts are recorded using the Siebel-Web protocol. For details, see *HP Virtual User Generator User's Guide*.

To select the appropriate protocol:

a In VuGen, select **New** to open the New Virtual User page.

b Select **New Single Protocol Script**.

c Select the **Siebel-Web** protocol.

3 **Create Business Transaction Flows**

You can create Business Transaction Flows in End User Management. For concept details, see "Monitoring Essential Transactions" in *Using End User Management*.
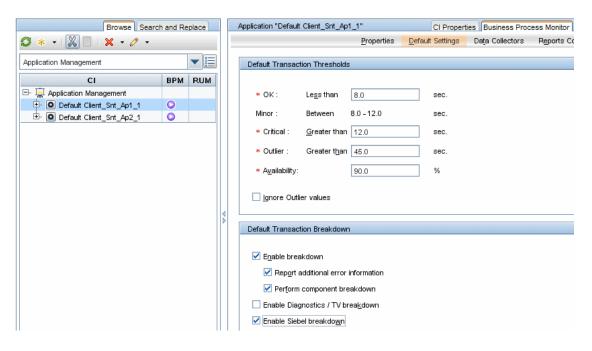
4 **Deploy the SiteScope Siebel monitors**

Deploy the SiteScope Siebel monitors. You can deploy the Siebel monitors using the Monitor Deployment Wizard or the Siebel solution templates. For task details, see "How to Deploy the SiteScope Siebel Monitors" on page 86.

5 **View SARM Data in Business Transaction Flows**

To view Siebel Application Response Measurement (SARM) data in Business Transaction Flows in the Application Management for Siebel SARM - User Trace Breakdown diagnostics tool, you must select the **Enable Siebel Breakdown** property for each Siebel transaction monitor in the Business Transaction Flows. When you do not select the property, the Transactions tab is empty.

To see SARM data under Business Transaction Flows, select **Admin > End User Management > Monitoring**, right-click the CI, click the **Business Process Monitor** tab, and in the Default Settings tab, in the Default Transaction Breakdown area, select the **Enable Siebel Breakdown** parameter. .

🔧 How to Customize Application Management for Siebel

You can customize Application Management for Siebel using the capabilities listed in this section.

The task includes the following topics:

➤ "Save the generated XML files after generating the SARM report" on page 92

➤ "Specify the default SiteScope monitors" on page 93

➤ "Specify the SiteScope monitor used to execute Siebel diagnostics tools" on page 93

➤ "Change the default timeout for the execution of a SiteScope monitor" on page 94

➤ "Increase the default timeout for either a SARM task or a SARM Analyzer execution" on page 95

1 Save the generated XML files after generating the SARM report

After the generation of the SARM report, the generated XML files are automatically deleted from the SiteScope and HP Business Service Management.

To prevent the deletion and save the generated XML files after generating the SARM report, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Applications**.

➤ Select **Siebel**.

➤ In the **Siebel - Siebel SARM Breakdown** area, locate:

> ➤ **Remove SARM results temporary directory from BAC.** If you give this parameter the value **false**, then the XML files are saved in the **<HPBSM root directory on the Gateway Server>\ AppServer\webapps\site.war\Imgs\chartTemp\offline** directory.

> ➤ **Remove SARM results temporary directory from SiteScope.** If you give this parameter the value **false**, then the XML files are saved in the **<SiteScope installation directory>\cache\tempbyage\ <TimeStamp>_SIEBEL_SARM\<web_server>_<App_server>** directory.

2 Specify the default SiteScope monitors

Specify the default SiteScope monitors with which you want to work.

To specify the default SiteScope monitors, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Applications**.

➤ Select **Siebel**.

➤ In the **Siebel - Siebel SARM Breakdown** area, locate **Default SiteScopes for SARM diagnostics**. Modify the value by entering one of the following:

> ➤ The SiteScope monitor names separated by semicolons (for example: rca3;rca4)

> ➤ **ALL** to use all attached SiteScope monitors

3 Specify the SiteScope monitor used to execute Siebel diagnostics tools

Specify the default SiteScope agent used to execute Siebel diagnostics tools when using the shortcut menus options listed in the **Go to Siebel SARM** or **Go to Siebel Database Breakdown** shortcut menu. For details, see "Service Health Menu Options" in *Using Service Health*.

To specify the default SiteScope monitors, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Applications**.

➤ Select **Siebel**.

➤ In the **Siebel - General Settings** table, locate **Default SiteScope for Diagnostic drilldown from Service Health**. Enter the name of the default SiteScope that is being used from Service Health to execute diagnostic tools.

4 Change the default timeout for the execution of a SiteScope monitor

If the **Siebel.ejb.log**, located on the Gateway server, indicates that an execution of a SiteScope monitor timed-out, change the default timeout for the execution of this monitor.

To change the default timeout for the execution of a SiteScope Monitor, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Foundations**.

➤ Select **Verticals**.

➤ In the Vertical - SiteScope Remote Control Settings table, locate **SiteScope monitor timeout in seconds**. Modify the parameters's value. The parameter indicates the default timeout for the execution of a SiteScope monitor.

5 Increase the default timeout for either a SARM task or a SARM Analyzer execution

If the **<SiteScope root directory>\tools\sarmDiagnostics\logSiteScope \sarmanalyzer.log** indicates that a SARM task or SARMAnalyzer execution has been timed-out, increase the default timeout for either a SARM task or a SARM analyzer execution.

To increase the default timeout for either a SARM task or a SARM analyzer execution, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Applications**.

➤ Select **Siebel**.

➤ In the Siebel - Siebel SARM Breakdown table, locate:

➤ **SARM task timeout in seconds.** Change the default timeout for the execution of a SARM task (analyzing Web Server file, analyzing Application Server files, and so on) as required.

➤ **SarmAnalyzer command timeout in seconds.** Change the default timeout for the execution of **sarmanalyzer.exe** (used to generate CSV or XML files) as required.

Reference

🔍 Siebel CIs Properties

The following properties remain empty and must be entered manually.

CI Type	Properties	Description
Siebel Enterprise	Admin user name	The name of the user used to log on Server Manager.
	Admin password	The password of the user used to log on Server Manager.
	SARM Script Path	The path to the location of the Siebel Application Response Measurement (SARM) Analyzer package on the SiteScope server. The path is relative to the SiteScope server.
	Server Manager Script Path	The path to the location of Server Manager package on the SiteScope server. The path is relative to the SiteScope server. For details, see "Copy the SARM Analyzer tool to the SiteScope server" on page 80.
Siebel Application	Emulated Transaction User Name	The name of the user used in the script that analyzes the application. It is the default user name that appears when configuring the Database Breakdown tool.
Siebel Web Server Extension	SARM Log Folder	The log folder to which SARM log files are written on the Web Server Extension's machine. The path is relative to the SiteScope server. The folder should be shared. The format should be: **<siebel_web_server_extension_name>\<log_directory>**

CI Type	Properties	Description
Siebel Application Server	SARM Log Folder	The log folder to which SARM files are written on the Application Server machine. The path is relative to the SiteScope server. The folder should be shared. The format should be: **<siebel_app_server_name>**\ **<sarm_log_directory>**
	Log Folder	The log folder to which Siebel general log files are written on the Application Server machine. The path is relative to the SiteScope server. The folder should be shared. The format should be: **<siebel_app_server_name>**\ **<log_directory>**

🔍 **Application Management for Siebel Administration User Interface**

This section describes:

➤ Siebel Deployment Validator Page on page 98

➤ Siebel Deployment Validator Test Summary Dialog Box on page 101

🔧 Siebel Deployment Validator Page

This page enables you to execute all or part of the predefined tests that detect known problems that can occur while deploying Application Management for Siebel.

To access	Select **Admin** > **Application Management for Siebel Administration.**
Relevant tasks	"How to Deploy Application Management for Siebel" on page 72
See also	"List of Predefined Tests for Siebel Deployment Validator" on page 100

User interface elements are described below:

UI Element (A-Z)	Description
▷	**Run Selected Tests.** Runs the selected test.
☐	**Stop.** Stops the selected test.
🖳	**Test Summary.** Opens the Siebel Deployment Validator Test Summary dialog box. For details, see "Siebel Deployment Validator Test Summary Dialog Box" on page 101.
☑ ☒	**Show Passed/Hide Passed.** Displays/hides the tests that ran successfully.
Running 1 of 1 Failed 0	Displays the test execution progress: ➤ How many tests are running ➤ How many tests failed ➤ How many tests ended
Category	The application related to the test: BSM, BPM, or Siebel.
Description	The test description.
Execution Time	The time and date when the test was last run.

UI Element (A-Z)	Description
Status	The status of the test. ⚙ Waiting ▶ Running ✓ Passed ✗ Failed
Test Name	The name of the test. Predefined tests enable you to detect known problems that may occur during HP Business Availability for Siebel Applications deployment. For a list of available tests and their description, see "List of Predefined Tests for Siebel Deployment Validator" on page 100. A combination of parameter's values is used to create the appropriate test. The values can be: ➤ **@ALL@.** The test checks all the appropriate items represented by the parameter (for example, the Siebel Enterprises View Test checks that the Siebel Enterprises view contains all the appropriate CIs for all Siebel Enterprises sites). ➤ **@ANY@.** The test checks at least one appropriate item represented by the parameter (for example, the SiteScope Connection Test checks that at least one SiteScope working with the Windows operating system is attached to BSM). ➤ **@\<value>@.** Some of the parameters can only be set to @ALL@ or to some specific value. For example, the BPM Script Execution Test parameters creates the following test: run at least one of the BPMScripts (BPMScripts = @ANY@) connected to the Siebel Enterprise CI (Enterprises = @siebel@) on all the locations available (Locations = @ALL@).

🔍 List of Predefined Tests for Siebel Deployment Validator

The predefined tests are listed below.

Test Name (A - Z)	Checks That:	Category	Parameters
Siebel Application Server Settings Test	The **Log folder** and **SARM log folder** are defined for the Siebel Application Server, and are accessible.	BSM	➤ Enterprises = @ALL@ ➤ AppServers = @ALL@ ➤ SiteScopes = @ALL@
Siebel Application Structure Test	At least one Siebel Application is linked to the selected Siebel Enterprise CI that has, at least, one child BPM Transaction CI.	BSM	Enterprises = @ALL@
Siebel Enterprise SARM Analyzer Setting Test	The sarmAnalyzer path is defined and the folder is accessible from the Siebel Enterprise application.	BSM	➤ Enterprises = @ALL@ ➤ SiteScopes = @ALL@
Siebel Enterprise Srvrmgr Settings Test	The **Admin user name**, **Admin password** and **srvrmgr path** are defined for the Siebel Enterprise, and the srvrmgr can be launched.	BSM	➤ Enterprises = @ALL@ ➤ SiteScopes = @ALL@
Siebel Enterprises View Test	The Siebel Enterprises view contains Siebel Enterprises CIs with child Siebel Application Server, Siebel Web Server Extension, and Siebel Gateway CIs.	BSM	Enterprises = @ALL@
Siebel Package Deployment Test	The Siebel_monitoring.zip package is deployed on HP Universal CMDB. If the test fails, see "Siebel Enterprises View Is Not Found" on page 105.	BSM	None

Test Name (A - Z)	Checks That:	Category	Parameters
Siebel Tasks List Command Test	Checks the **list tasks** command of the Siebel server manager. If the test fails, see "Errors That Occur when Building the Siebel Enterprises View" on page 103.	Siebel	➤ Enterprises = @ALL@ ➤ SiteScopes = @ALL@
Siebel Web Server Extension Settings Test	The SARM log folder is defined for the Siebel Web Server Extension and is accessible.	BSM	➤ Enterprises = @ALL@ ➤ WSE = @ALL@ ➤ SiteScopes = @ALL@
SiteScope Connection Test	The SiteScope working with the Windows operating system is attached to BSM. If the test fails, see "Errors That Occur when Building the Siebel Enterprises View" on page 103.	BSM	SiteScopes = @ANY@

🔍 Siebel Deployment Validator Test Summary Dialog Box

This dialog box displays the results of the Siebel Deployment Validator test run.

To access	Select **Admin** > **Application Management for Siebel Administration**, select a Deployment Validator test, and click the **Test Summary** 🔡 button.

User interface elements are described below:

UI Element (A-Z)	Description
Category	The application related to the test: BAC, BPM, or Siebel.
Description	The test description.
Error details	The error message that explains why the test failed.

UI Element (A-Z)	Description
Last execution date	Date when the test was last run.
Last time test passed	Date when the test was last run successfully.
Status	The status of the test.
Test Name	The name of the test.
Test Parameters	Click to open the area. The area lists the parameters used to run the test and their values and indicates where in the Infrastructure Settings you can modify the test parameters, add new tests, or delete existing tests.

🔍 Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Application Management for Siebel.

This section includes the following topics:

➤ "Troubleshooting Errors in Logs" on page 103

➤ "Troubleshooting Siebel Enterprises View" on page 105

➤ "Troubleshooting Diagnostics Tools" on page 106

➤ "Troubleshooting SARM-Related Issues" on page 106

➤ "Troubleshooting Database Breakdown" on page 121

➤ "Troubleshooting Processes" on page 124

➤ "Troubleshooting Tasks" on page 125

🔍 **Troubleshooting Errors in Logs**

Logs are available to help you debug problems with Siebel views and problems that occur when using the Siebel diagnostics tools.

This section includes the following items:

➤ "Errors That Occur when Building the Siebel Enterprises View"

➤ "Errors That Occur when Running One of the Diagnostics Tools"

Errors That Occur when Building the Siebel Enterprises View

When this type of error occurs, run the following tests to pinpoint the problem:

➤ **SiteScope Connection Test**

➤ **BPM Adapter Mode Test**

➤ **Siebel Task List Command Test**

➤ **BPM Transaction Execution Test**

For details on the tests, see "List of Predefined Tests for Siebel Deployment Validator" on page 100.

You can also check the **Siebel.ejb.log** file (on the RTSM server). It includes information about whether all the automatic links between the BPM or SiteScope and the Siebel CIs worked correctly or not. For details on the automatic links, see "How to Use a Business Transaction Flows to Simulate Siebel Users – Details" on page 89.

To debug the log:

1 Open the **<HPBSM root directory on the Data_processing Server>\conf\ core\Tools\log4j\EJB\topaz.properties** file

2 In the line that follows, change **${loglevel}** to debug. The lines should be as follows: **log4j.category.com.mercury.topaz. vertical=debug, vertical.appender log4j.category.com. mercury.am.bac.vertical.rules=debug, vertical.appender**

3 Open the error log, located on the RTSM server at the following location: **<HPBSM root directory on the Data_processing Server>\log \EJBContainer\Siebel.ejb.log**

4 Locate the **#define appender for vertical module** line.

5 You can now analyze the log information.

6 After you complete the debugging tasks, make sure to change **debug** back to **${loglevel}** in the lines that follows **#define appender for vertical module**. The lines should be as follows:
log4j.category.com.mercury.topaz.vertical=${loglevel}, vertical. appenderlog4j.category.com.mercury.am.bac.vertical.rules=${loglevel}, vertical.appender

Errors That Occur when Running One of the Diagnostics Tools

The **Siebel.ejb.log** file (on the Gateway server) includes detailed information about the operations that take place in the Siebel Diagnostics tools.

For details on the Siebel Diagnostics tools, see "Diagnostics Tools" on page 128.

To debug the log:

1 Open the
<HPBSM root directory on the Data_processing Server>\conf\ core\Tools\log4j\EJB\topaz.properties file

2 In the line that follows, change **${loglevel}** to debug. The line should be as follows:
log4j.category.com.mercury.topaz.siebel=debug, siebel.appender

3 Open the error log, located on the Gateway server at the following location:
<HPBSM root directory on the Data_processing Server>\ log\EJBContainer\Siebel.ejb.log

4 Locate the **#define appender for siebel** line.

5 You can now analyze the log information.

6 After you have completed the debugging tasks, make sure to change **debug** back to **${loglevel}** in the line that follows **#define appender for siebel**. The line should be as follows:
log4j.category.com.mercury.topaz.siebel=${loglevel}, siebel.appender

🔍 Troubleshooting Siebel Enterprises View

This section describes issues related to the Siebel Enterprises View and how to solve these problems.

This section includes the following items:

➤ "Siebel Enterprises View Is Not Found"

➤ "Session Data Is Not Available"

➤ "Task Data Is Not Available"

Siebel Enterprises View Is Not Found

If the "Siebel Enterprises" view is not found, or if the **Siebel Package Deployment Test** fails, check that the Siebel Monitoring package appears in the Package Manager. For details, see "Package Administration Overview" in the *RTSM Administration Guide*.

For details on the **Siebel Package Deployment Test**, see "List of Predefined Tests for Siebel Deployment Validator" on page 100.

Session Data Is Not Available

If, in the view, the **Siebel Sessions** KPI is empty, it might be because the **No. of Running Sessions** measurement is not monitored for an application server/component in the relevant Siebel Application Server monitor.

Task Data Is Not Available

If, in the view, the **Siebel Error** KPI is empty, it might be because the **No. of Tasks in Error** measurement is not monitored for an application server/component in the relevant Siebel Application Server monitor.

🔍 Troubleshooting Diagnostics Tools

This section describes issues related to the Diagnostics tools and how to solve these problems.

Connection parameters do not match

When one of the diagnostics tools is activated, a temporary SiteScope monitor is created, run, and then erased. The connection parameters used are the parameters that exist in the various relevant CIs (Enterprise, Application Server, and so on).

You must check that the connection parameters (user name, password, enterprise name, and gateway name) used in the CIs conform to the parameters used in the permanent SiteScope monitors monitoring the Siebel Enterprise. (If the connection parameters do not match, then most diagnostics features do not work.) For example, the same user name and password needs to be used in the Siebel Enterprise configuration and in the permanent monitors defined in SiteScope.

If a problem occurs, check the SiteScope error log (in SiteScope under the logs directory) and the Siebel log and check the list of parameters used to access SiteScope and Siebel. For details on the Siebel log, see "Errors That Occur when Running One of the Diagnostics Tools" on page 104.

🔍 Troubleshooting SARM-Related Issues

This section describes issues related to Siebel Application Response Measurement (SARM) and how to solve these problems.

This section includes the following items:

➤ "All the log data is written to a few large log files instead of separate log files per task" on page 107

➤ "SARM does not work" on page 108

➤ "SARM Analyzer fails to run" on page 111

➤ "SARM configuration is not correct" on page 112

➤ "Error message after running SARM Diagnostics" on page 112

All the log data is written to a few large log files instead of separate log files per task

The Siebel logging mechanism for an application is sometimes configured in such way that all log data is written to a few large log files instead of creating a separate log file per task. Large log files are a problem because parsing takes a long time.

To solve the problem, two solutions are available:

➤ The Siebel administrator should configure the relevant parameters so that each task writes to a separate log data file.

➤ The Siebel administrator should provide:

  ➤ A script to be used before running the diagnostic tools. That script should set the logging mechanism to log each task into a separate file. This is required when you want to use the Database Breakdown reports and may also be relevant when the Siebel Log Monitor is configured. Consult Siebel documentation for more detailed instructions.

  ➤ A script to be used after running the diagnostics tool. That script should switch the log level back to its initial state.

SARM does not work

Check all steps of the following checklist:

1 The SARM Analyzer path that you defined for the Siebel Enterprise is accessible through SiteScope, by running the **Siebel Enterprise SARM Analyzer Setting Test**. For details, see "Siebel Deployment Validator Page" on page 98.

2 At least one Web Server, one Application Server, and one Gateway Server have been discovered during the discovery process, by running the **Siebel Enterprises View Test**. For details, see "Siebel Deployment Validator Page" on page 98.

3 The SARM log folder defined for the Web Server is accessible through SiteScope, by running the **Siebel Web Server Extension Setting Test**. For details, see "Siebel Deployment Validator Page" on page 98.

4 The SARM log folder defined for the Application Server is accessible through SiteScope, by running the **Siebel Application Server Setting Test**. For details, see "Siebel Deployment Validator Page" on page 98.

5 SiteScope is running with a user on the SiteScope machine:

➤ In the SiteScope machine, open **Services**.

➤ Right-click the SiteScope service to open its properties.

➤ Click the **Log On** tab.

➤ Check that **This Account** is checked.

➤ Check that the user name and password are correct.

6 The **<SiteScope_root_directory>\tools\sarmdiagnostics** directory exists on the SiteScope server (used when running the SARM Analyzer tool).

7 Siebel Server Manager properties are defined properly for the Siebel Enterprise, in IT universe (select **Admin** > **RTSM Administration** > **Modeling** > **IT Universe Manager**) in HP Business Service Management (for more information, see "Troubleshooting Diagnostics Tools" on page 106).

8 SiteScope is attached.

If you checked the entire list and SARM still does not work, check the following options:

➤ "SARM does not generate properly" on page 109

➤ "SARM Analyzer might have failed" on page 110

SARM does not generate properly

If the **No Relevant Sessions** error message is issued when you know that you should have data, SARM might not generate properly.

To identify the problem:

1 Open one the XML files located in the relevant SiteScope in the following directory: **<SiteScope installation directory>\cache\tempbyage \<TimeStamp>_SIEBEL_SARM\ <web_server>_<App_server>**
If there are no XML files in that directory follow the next procedure.

2 Select any of the last requests in the XML file:

➤ If the request does not include a **<SiebsrvrDetails>** section with a **<Group>** node under it, then Siebel is not generating the SARM data properly.

➤ If the request does include a **<SiebsrvrDetails>** section with a **<Group>** node under it, then follow the procedures below. For details, see below or "SARM Analyzer fails to run" on page 111.

To solve the problem:

1 The generated XML files are being deleted from the SiteScope and HP Business Service Management after the generation of the SARM report. To see them you should first select the appropriate settings to save these files and not delete them. For details, see "Save the generated XML files after generating the SARM report" on page 92.

2 Delete all the SARM files from the Application Server and from the Web server.

If this does not help, restart the Siebel machine.

SARM Analyzer might have failed

If the **No Relevant Sessions** error message is issued when you know that you should have data, SARM Analyzer might have failed

or

It takes at least five minutes for the message: No relevant session were found is used

If the **No Relevant Sessions** error message is issued when you know that you should have data, SARM Analyzer might have failed because the requests counter was reset to **0** in the middle of the session without any logical reason. Another indication is that it takes at least five minutes for this error to appear, because the execution of the batch files in SiteScope times out.

To identify the problem:

SARM Analyzer has failed if any one of the following situations occurs:

➤ A message (**No relevant sessions were found**) is issued, indicating that there are no sessions when you know there should be sessions.

➤ The timestamp of the **crash<nnn>** file in the SARM Analyzer folder corresponds to the time when you ran the User Session Trace. This indication almost always occurs.

➤ An error message is issued in the SiteScope machine. This indication is rare.

To solve the problem:

➤ Connect to the Siebel Web server, and delete (locally) the last SARM binary file from the Web server log folder.

➤ If this does not help and the problem occurs again, restart the Siebel machine.

SARM Analyzer fails to run

When you run the SARM Analyzer from a remote machine (not locally on the SiteScope machine), the SARM Analyzer fails to run.

To identify the problem:

SARM Analyzer failed to run if any one of the following situations occurs:

➤ A message (**No relevant sessions were found**) is issued, indicating that there are no sessions when you know there should be sessions.

➤ One of the following errors was added to the SiteScope **sarmAnalyzer.log** log on
<SiteScope installation directory>
 \Tools\sarmDiagnostics\log\sarmAnalyzer.log during the execution of the SARM diagnostics:

   ➤ **Failed to analyze app server SARM files**

   ➤ **SarmAnalyzer failed**

   ➤ **Error running command: <command_name>**

Tip: The problem occurs because of a different domain or because of permissions issues.

To solve the problem:

Check that SiteScope can communicate with the Siebel server.

SARM configuration is not correct

SARM configuration is not correct, if SARM is configured to store data for a long period of time (several days), or if processing takes too long.

To identify the problem:

SARM is configured to store data for a long period of time (several days), or if processing takes too long.

To solve the problem:

Configure SARM correctly.

Error message after running SARM Diagnostics

After running SARM Diagnostics, the following error message: **A Sitescope server failed to access a Siebel SARM folder or file. Make sure all SiteScope servers have the proper permissions.** is displayed.

To identify the problem:

The user name used to log to the SiteScope Service does not have the appropriate permissions to access the SARM folder on the Web or application server.

To solve the problem:

1 Go through steps 3 to 8 of the SARM Does Not Work procedure above. For details, see "SARM does not work" on page 108.

2 Log on to one of the SiteScope machines with the SiteScope username and password, and try to access the SARM folders defined in BSM.

Error message after running SARM Diagnostics

After running SARM Diagnostics, the following error message: **The operation completed with several errors. Please check the logs for more information.** is displayed.

This error can be caused by a number of reasons, including unexpected SARMAnalyzer output, network issues, or Server manager errors.

To solve the problem:

To check the errors that occurred, go through the following log files and search for error messages logged around the time you invoked User Session Breakdown:

➤ On the HP Business Service Management Gateway server: **<HPBSM root directory on the Data_processing Server>/log/ EJBContainer/siebel.ejb.log**

➤ On the SiteScope machine: **<SiteScope root directory>/tools/sarmDiagnostics/log/sarmAnalyzer.log**

Timed-out execution of a SARM task or SARMAnalyzer execution

If the sarmAnalyzer.log (SiteScope) indicates that a SARM task or SARMAnalyzer execution has been timed-out, increase the default timeout for either a SARM task or a SARM analyzer execution. For details, see "Increase the default timeout for either a SARM task or a SARM Analyzer execution" on page 95.

If the **Siebel.ejb.log** (on the Gateway Server) indicates that an execution of a SiteScope monitor got timed-out, change the default timeout for the execution of this monitor. For details, see "Increase the default timeout for either a SARM task or a SARM Analyzer execution" on page 95.

Error message after running SARM Diagnostics

The message **No working SiteScope server could be found to process SARM data.** is issued when running SARM Diagnostics.

To identify the problem:

If the message **No working SiteScope server could be found to process SARM data.** is issued when running SARM Diagnostics, proceed as explained in this section.

To solve the problem:

1 Open the **Advanced Options** section of the User Trace Breakdown page in HP Business Service Management. For details, see "Siebel Views" on page 132.

2 Verify that the SiteScope servers that are selected in **Using SiteScope:** list are the servers you want to use for SARM diagnostics.

3 Go through steps 5 to 8 of the SARM Does Not Work procedure for these servers. For details, see "SARM does not work" on page 108.

4 If this does not help, restart the SiteScope servers.

SARM on the Windows NT platform - When working with the SARM tool in Siebel 7.8, use SARM Analyzer for Siebel version 7.7.

SARM on the UNIX platform - When working with the SARM tool on a UNIX platform, check that the following requirements are met:

➤ **Siebel 7.7 and 7.8**

   ➤ When working with the SARM tool in Siebel 7.8, use SARM Analyzer for Siebel version 7.7.

   ➤ The SARM feature is supported only if SiteScope is installed on a Windows NT platform.

   ➤ A connection must exist between SiteScope and the Siebel machine. The SiteScope user must have permission to read from the relevant directories (it means that the user has to be declared as a mounting point machine user and as a UNIX user).

➤ **Siebel 7.5.3**

Note: The SARM user trace breakdown diagnostic tool is not recommended for use on Siebel 7.5.3 running on UNIX. It only works for full UNIX environments (in Siebel 7.7 you can work with mixed environments). This is a limitation from Siebel. For example, in Siebel 7.5.3, the SARMAnalyzer tool cannot work on files from different environments; therefore, if you use SARMAnalyzer for the Windows NT platform you must work only with the Windows NT environment.

➤ The SiteScope user has execution permissions for the server manager and the SARM Analyzer.

➤ A mount point must exist between the SiteScope machine and the Siebel machine.

➤ The SiteScope user must have permissions to read from the relevant directories on the Siebel machine.

➤ Make the following changes to the **start-monitor** and **start-service** scripts located in the **<SiteScope>/classes** directory: insert all the variables that are related to **LD_LIBRARY_PATH** from the **siebenv.sh** file (generally located in the **siebsrvr** directory), and set them to be accurate (insert all the definitions from the **siebenv.sh** file). This definition is needed to run **srvrmgr** and **SARMAnalyzer** on the SiteScope machine with mount. It is recommended to copy the **srvrmgr** and **SARMAnalyzer** directories to SiteScope for better performance.

Enable SARM for Siebel

You can control Siebel Application Response Monitoring (SARM) using Siebel server parameters and environment variables.

To enable SARM, you must enable specific SARM parameters for the Web server using environment variables and for the Siebel Server using Server Manager or the Siebel Server Manager Graphical User Interface. When a component starts up in the Siebel Enterprise, it checks the status of the SARM parameters.

Note: SARM is disabled by default.

You can enable SARM for the Web server only at the Web server level, and for the application server either at the Application Server level, or at the component level:

To enable SARM for Siebel at the Web server level:

1 Update the values of the appropriate environment variables parameters listed in the table. For details, see "SARM Parameters" on page 120.

2 Check whether the settings for the **SarmMaxMemory** and **SarmMaxFileSize** parameters are appropriate since these parameters determine how soon SARM flushes its data to a disk, and how large the SARM files can be. For details on the recommendations for these parameters settings, see "Calculating the SarmMaxFileSize Parameter" on page 118.

3 Restart the Siebel server for the new values to take effect.

To enable SARM for Siebel at the Application level from the environment variables

1 Update the values of the appropriate environment variables parameters listed in the table above.

2 Check whether the settings for the **SarmMaxMemory** and **SarmMaxFileSize** parameters are appropriate since these parameters determine how soon SARM flushes its data to a disk, and how large the SARM files can be. For details on the recommendations for these parameters settings, see "Calculating the SarmMaxFileSize Parameter" on page 118.

3 Restart the Siebel server for the new values to take effect.

Note: The Application Server Parameters can be updated from either the environment variables or from the Siebel Server user interface (follow the procedure below). If the parameters are defined both in the user interface and the environment variables, the environment variables override the user interface definitions.

To enable SARM for Siebel at the Application Server level from the Siebel Server user interface:

1 In Siebel Server Manager Graphical User Interface, select **Site Map > Server Administration** > **Servers** > **Server Parameters**.

2 In the Server Parameters List Applet, query for SARM.

3 Update the values of the appropriate parameters listed in the table above.

4 Check whether the settings for the **SarmMaxMemory** and **SarmMaxFileSize** parameters are appropriate since these parameters determine how soon SARM flushes its data to a disk, and how large the SARM files can be. For details on the recommendations for these parameters settings, see "Calculating the SarmMaxFileSize Parameter" on page 118.

Note: The Application Server Parameters can be updated from either the environment variables (follow the procedure above) or from the Siebel Server user interface (follow the procedure below). If the parameters are defined both in the user interface and the environment variables, the environment variables override the user interface definitions.

To enable SARM for Siebel at the component level:

1 In Siebel Server Manager Graphical User Interface, select **Site Map > Server Administration** > **Servers** > **Component Parameters**.

2 In the Component Parameters List Applet, query for SARM.

3 Update the values of the appropriate parameters listed in the table above.

4 Check whether the settings for the **SarmMaxMemory** and **SarmMaxFileSize** parameters are appropriate since these parameters determine how soon SARM flushes its data to a disk, and how large the SARM files can be. For details on the recommendations for these parameters settings, see "Calculating the SarmMaxFileSize Parameter" on page 118.

Calculating the SarmMaxFileSize Parameter

The **SarmMaxFileSize** parameter settings recommended for working with SARM depend on the Siebel version. For details on where to set the parameter, see Siebel documentation.

➤ **Siebel 7.5.3**

The amount of data that is written per second can be calculated in the following way: **37kb/<nbr_of_concurrent_users>*<required_time_frame_saved>/<nbr_of_server_components_instances>**

Example: If your Siebel Enterprise has 20 concurrent users, you want to save the data of the last hour for all users, and you have three instances of the Object Manager component of the application, the file size should be: 37*20*60/3 = 14,800 Kb. Therefore the **SARM Data File Size Limit** should be set to 15,000,000. The buffer size should be set to 4,000,000. The growth rates of the Web server data is 1/5 the growth of the Application Server data.

➤ **Siebel 7.7 or 7.8**

The amount of data that is written per second in Siebel 7.7 or 7.8 depends on the granularity level and can be calculated in the following way:

➤ **Level 1 (SIEBEL_SarmLevel=1).** The calculation is as follows: **10kb/<nbr_of_concurrent_users>*<required_time_frame_saved>/<nbr_of_server_components_instances>**

Example: If your Siebel Enterprise has 20 concurrent users, you want to save the data of the last hour for all users, and you have three instances of the Object Manager component, the file size should be: 10*20*60/3 = 4,000 Kb. Therefore, the SARM Data File Size Limit should be set to: 4,000,000.

➤ **Level 2 (SIEBEL_SarmLevel=2).** To store more data. The calculation is as follows: **60kb/ <nbr_of_concurrent_users>*<required_time_frame_saved>/ <nbr_of_server_components_instances>**

Example: If your Siebel Enterprise has 20 concurrent users, you want to save the data of the last hour for all users, and you have three instances of the Object Manager component, the file size should be: 60*20*60/3 = 24,000 Kb. Therefore, the SARM Data File Size Limit should be set to: 24,000,000.

Tips

➤ To save disk space, it is recommended to enable SARM only for Object Manager components since Siebel is only measuring the Object Managers time for the User Session trace.

➤ If you restart the Siebel Application Server or the Web server regularly it is recommended to search, in the log folder, for old SARM files that can be deleted. Every time you restart the server a new log file, which includes the Process ID, is created. Only five log files with the same Process ID are kept at a time (the older ones are overwritten). Files with other Process IDs must be deleted manually. This procedure saves disk space and also improves the efficiency of the User Session Breakdown.

➤ It is best if the number of SARM files saved in the SARM folders is minimal. Save only the files you want to retrieve data from. Other files can be moved to another folder (not to a sub-directory of the SARM folder) and can be used later. Too many SARM files in the SARM directories cause the SARM tool to work more slowly.

SARM Parameters

The SARM parameters are as follows:

Siebel Version	Name of SARM Parameter in the Web Server	Name of SARM Parameter for Application Server	Description
Siebel 7.5.3	SIEBEL_ SarmEnabled	SARMEnabled	Indicates whether SARM is enabled or disabled for a Siebel Server Component. The default value is **false**. This parameter can be set at the Siebel Enterprise level, Siebel Application Server level, or Siebel Component level.
	SIEBEL_ SarmMaxMemory	SARMMaxMemory	The maximum size of the SARM memory. This parameter can be set at the Siebel Server or Siebel Server Component level.
	SIEBEL_ SarmMaxFileSize	SARMMaxFileSize	The maximum size of a SARM file. SARM continues to append file segments to the current file until the maximum size is reached. When the limit is reached, SARM starts a new file. The default value is 20,000,000 (~20 MB) and is specified in bytes.

Siebel Version	Name of SARM Parameter in the Web Server	Name of SARM Parameter for Application Server	Description
Siebel 7.7 or 7.8	SIEBEL_ SARMBufferSize	SARMBufferSize	The size of the SARM buffer. The default value is 5,000,000 bytes (~5 MB).
	SIEBEL_ SARMLevel	SARMLevel	The SARM granularity level. The default value is 0. This parameter can be set at the Siebel Server or Siebel Server Component level.
	SIEBEL_ SARMFileSize	SARMFileSize	The maximum size of a SARM data file. The default value is 15,000,000 bytes (~15 MB).
	SIEBEL_ SARMMaxFiles	SARMMaxFiles	The maximum number of SARM files determines how many SARM files should be saved for a session. The recommended value is 5.
	SIEBEL_ SarmPeriod	SARMPeriod	The SARM period is the time when SARM outputs the stored data to the SARM log file regardless of the Buffer size. The default value is 3.

🔍 Troubleshooting Database Breakdown

This section describes how to solve Database Breakdown-related issues:

➤ "Problem When Searching for a Task Using the Siebel Database Breakdown Tool" on page 122

➤ "Only the Total Database Time Chart and not the 15 SQLs Chart is displayed" on page 122

➤ "Error: Cannot Raise Log Level" on page 123

➤ "Error: Could Not Retrieve Log File" on page 123

➤ "Error: Could Not Run BPM Transaction" on page 123

➤ "Error: Database Breakdown Analysis Data for the Transaction Cannot Be Displayed" on page 124

➤ "Limitation: the Siebel Log Monitor Does not Work on a UNIX Platform" on page 124

Problem When Searching for a Task Using the Siebel Database Breakdown Tool

If the Siebel Enterprise uses a gateway with an additional SSL that supplies dynamic IDs for every user session, searching for the proper tasks using the Siebel Database Breakdown tool may be problematic.

To solve the problem:

A possible solution is to find the correlation in the VuGen script and to update the Siebel Application's user in the Siebel Application Configuration.

To do so, select **Admin** > **RTSM Administration**, select the Siebel Enterprises view, select the appropriate Siebel Application CI in Model Explorer, and select the Properties tab. In the Other Properties area, enter the appropriate user name in the **Emulated Transaction User Name** box, and click **OK**.

Tip: It is recommended to use a script with no more than five transactions when using the Database Breakdown diagnostics.

Only the Total Database Time Chart and not the 15 SQLs Chart is displayed

When the Siebel Database SQL Breakdown pie chart displays only the total database time chart and not the 15 SQLs chart, then there were no significant SQL queries to display. The chart displays only the 15 SQL queries that were the most time consuming. If all SQLs were under 1% of the total execution time of the transaction, then this information is not displayed. For details, see "Siebel Database Breakdown Analysis Report" on page 174.

Error: Cannot Raise Log Level

The error message: **Cannot raise log level** is issued in one of the following situations:

➤ A server manager has not been copied to the SiteScope server. For details, see "Copy the srvrmgr Tool and the SARM Analyzer Tool to the SiteScope Server – Details" on page 78.

➤ You did not configure the correct parameters for the Siebel Enterprise CI. For details, see "Troubleshooting Diagnostics Tools" on page 106.

➤ There is no license for Siebel in the SiteScope. For details, see "Check the Siebel license in SiteScope" on page 74.

Error: Could Not Retrieve Log File

When the error message: **Could not retrieve log file** is issued, proceed as follows:

1 Check the log folder of the server where the Siebel application is located.

2 Ensure that it is shared and that there is access to it from SiteScope, so the user can open the shared folder from the SiteScope and copy files from it.

3 Check also that all the relevant Siebel servers have a remote definition on the SiteScope. For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" in *Using SiteScope* in the SiteScope documentation library.

Error: Could Not Run BPM Transaction

When the error message: **Could not run BPM transaction** is issued or when the **BPM Transaction Execution Test** fails, one of the following situations may have occurred:

➤ The BPM server is down.

➤ The connection from HP Business Service Management to the BPM is problematic.

➤ There is a problem with the BPM script.

To solve the problem, access the BPM and run the transaction manually to check if there is a problem with the BPM.

For details on the **BPM Transaction Execution Test**, see "List of Predefined Tests for Siebel Deployment Validator" on page 100.

Error: Database Breakdown Analysis Data for the Transaction Cannot Be Displayed

The error message: **Database breakdown analysis data for the transaction cannot be displayed. This might be because the analysis filters currently set for the transaction exclude the existing data.** is displayed when the time zone and time definitions of the SiteScope server or BPM server used for the Database Breakdown tool are not synchronized with the Siebel server time zone and time definition.

A workaround is to synchronize the time zone and time definition of the servers and if they are synchronized, to rerun the Database Breakdown tool.

Limitation: the Siebel Log Monitor Does not Work on a UNIX Platform

The SiteScope Siebel Log monitor does not work when logs are located on a UNIX platform.

🔍 Troubleshooting Processes

This section describes how to solve processes-related issues.

Processes Tool Does not Function or Files Do Not Get Through SiteScope

➤ Check that the SiteScope user has permission to log to the Siebel machines.

➤ If another user is currently running SiteScope or ran SiteScope when the SiteScope server had not been booted, restart the SiteScope machine and the SiteScope service.

➤ Check that all Siebel servers are defined as remote servers on the SiteScope server.

🔍 **Troubleshooting Tasks**

This section describes how to solve task-related issues.

The No. of Tasks in Error Counter Reports all the Tasks that Have Exited with Error in the Last Hour

In the advanced options of the SiteScope monitor, if you configure the **Siebel Tasks Time Window** parameter to **0**, the **No. of tasks in error** counter displays all the tasks regardless of their start time.

4

Application Management for Siebel Views and Reports

This chapter includes:

Concepts

➤ Diagnostics Tools on page 128

➤ Siebel Views on page 132

Tasks

➤ How to Run the Siebel Database Breakdown Diagnostic Tool on page 136

➤ How to Run the SARM - User Trace Breakdown Diagnostics Tool – Details on page 137

➤ How to Define a Different Log Folder Per Siebel Component CI on page 138

➤ How to Display Siebel Information in BSM on page 139

Reference

➤ Shortcut Menu Options on page 144

➤ Default CITs in the Siebel View on page 144

➤ Application Management for Siebel Views and Reports User Interface on page 146

Concepts

🔷 Diagnostics Tools

You access the Application Management for Siebel information from the Applications menu. The following diagnostics tools are available:

This section includes the following topics:

➤ "SARM - User Trace Breakdown" on page 128

➤ "Database Breakdown Diagnostic" on page 130

➤ "Tasks Diagnostic Tool" on page 131

➤ "Siebel Processes Tool" on page 131

SARM - User Trace Breakdown

The Siebel SARM - User Trace Breakdown tool enables you to view Siebel real user monitoring information. The diagnostic tool processes the data in the User Session Trace output files produced by Siebel Application Response Measurement (SARM) process.

This data can be retrieved for a specific user in a specific time frame. It can also be retrieved for a specific transaction of a prerecorded script. For details, see "SARM - User Trace Breakdown (Run the Diagnostics Tool) Page" on page 149 and "SARM - User Trace Breakdown Dialog Box" on page 154 or "Siebel Views" on page 132.

The tool records logs for each Siebel transaction activity in the Web server or in the application server. It also records data about how long each transaction remains in each tier of the Siebel enterprise: Network, Web Server, Application Server, and Database. Siebel SARM tool logs Siebel real user monitoring data into binary SARM files (with .sarm extension). The transaction activity itself is written into the .sarm files.

HP Business Service Management interacts with SARM Analyzer (a Siebel tool) using remote API calls to SiteScope. These calls activate a batch file, which copies files from Siebel, and then uses the SARM Analyzer to generate user-readable files from the Siebel files. The user-readable files are then copied using SiteScope remote API to HP Business Service Management.

The SARM - User Trace Breakdown diagnostic tool is built over the Siebel's SARM tool. It produces required CSV and XML files as part of the analysis process, in which the Siebel SARM Analyzer package is used. The tool also analyzes and displays a graphical view of the results. It retrieves the SARM data for a specific user, in a specific time frame. It enables retrieving the SARM data for a specific BPM transaction that belongs to a prerecorded script with Siebel breakdown enabled.

In the SARM - User Trace Breakdown tab, you can compare this breakdown per user sessions, user transactions, or application servers to enable you to identify the prime suspect for performance problems. You can also drill down within these logs to determine which layer is responsible for the slow response.

The SARM - User Trace Breakdown diagnostic tool is activated on demand.

Note: The HP Virtual User Generator script must be recorded using the Siebel Web protocol. Select the **Enable Siebel Breakdown** check box while configuring the BPM. For details, see "Default Transaction Breakdown" in *Using End User Management.*

Details on how to use the SARM - User Trace Breakdown diagnostics tool are provided in the "SARM - User Trace Breakdown (Run the Diagnostics Tool) Page" on page 149.

Database Breakdown Diagnostic

The Siebel Database Breakdown diagnostics tool enables you to determine the cause of slow database response time by analyzing the database activity carried out as a result of running a Business Process Step and to extract comprehensive information regarding database time spent by various SQLs. The database activity is logged into database logs created on the Siebel application server.

You analyze Siebel database SQL activity by examining information in the Siebel application server logs. These logs contain a record of SQLs carried out as a result of Siebel components activity.

Logs are constantly created and updated on the Application Server. However, most of the time they are only logging errors, and do not include the extensive information that Database Breakdown can display. To log the extensive database time distribution information, the log level needs to be brought up.

When the user runs Database Breakdown, after defining the analysis' scope (Siebel Enterprise, Application, Business Process Step, and so on, Application Management for Siebel automatically increases (through SiteScope) the database log level for the selected component (if a specific component was selected).

Then, Application Management for Siebel instructs the BPM to run the transaction you selected. During the transaction run, as a result of the higher log level, database-related information is written into the application server log.

When the transaction has finished running, the database log level for the selected component is returned to normal by HP Business Service Management for Siebel.

For details, see "Siebel Database Breakdown Configuration Report" on page 171 and "Siebel Database Breakdown Analysis Report" on page 174.

Tasks Diagnostic Tool

The Siebel tasks diagnostic tool enables you to view details of the Siebel Application Server tasks, for each monitored Siebel Enterprise. For details, see "Siebel Views" on page 132.

Using the Siebel Tasks Diagnostics tool, you can:

➤ Retrieve details of the Siebel Application Server tasks that are running, or were run, on each Siebel Enterprise

➤ Choose to view details of all tasks, regardless of status, or details of only those tasks with a specific status

➤ Choose to view task details for all components in all component groups on all Siebel Application Servers, or for specific components in specific component groups on specific Siebel Application Servers

For details, see "Tasks Diagnostics Tool Report" on page 176 and "Tasks Diagnostics Tool - Advanced Filter Dialog Box" on page 179.

Siebel Processes Tool

The Siebel Processes Diagnostic tool enables you to view details of the operating system processes running on the various Siebel Application Servers, for each monitored Siebel Enterprise. For details, see "Siebel Views" on page 132.

To ensure that Diagnostics tools work properly, check the Diagnostics-related settings. For details, see "How to Verify Diagnostics-Related Settings" on page 83.

Using SiteScope, you can retrieve details of the Siebel Application Server processes that are running, or were run, on each Siebel Enterprise. You can view the details of all processes, regardless of status, or you can view only the processes with a specific status. Similarly, you can choose to view process details for all components in all component groups on all Siebel Application Servers, or for specific components in specific component groups on specific Siebel Application Servers.

When an application has performance/availability issues, you may use the Siebel Processes tool to verify that all Siebel processes are up and running and that none of the processes is using 100% CPU.

For details, see "Processes Report" on page 147 and "Processes Tool - Advanced Filter Dialog Box" on page 149.
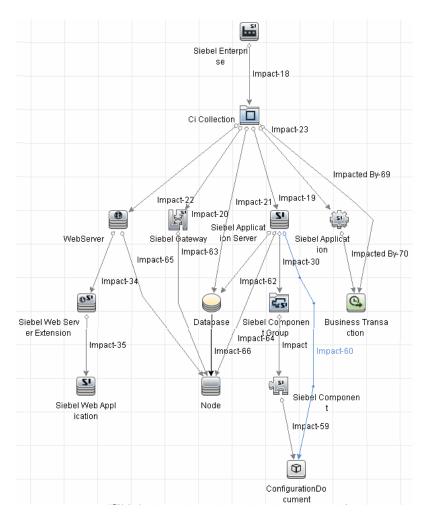
Siebel Views

The Siebel Enterprises view is enabled by default; the other Siebel views must be enabled before they are displayed.

In Service Health, access the Siebel Enterprises view to view information about the Siebel IT entities, the Siebel enterprise metrics monitored by SiteScope monitors, and information about the Siebel business processes/transactions simulated by BPM scripts.

For additional information about views, see "View Topology" in *Using Service Health*.

To display the Siebel Enterprise TQL, select **Admin** > **RTSM Administration** > **Modeling** > **Modeling Studio**, select Views in **Resource Type**, expand **Application** > **Siebel**, and click **Siebel Enterprise**.
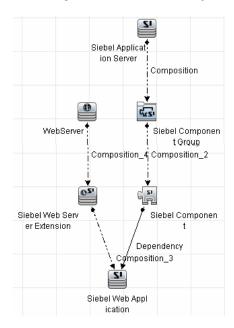
The Siebel Enterprises view appears as follows:

The **Siebel Topology** and **Siebel Web Topology** views are created when you run the discovery job. They display the results of the Siebel discovery and are intermediate views whose information is included in the Siebel Enterprises view.
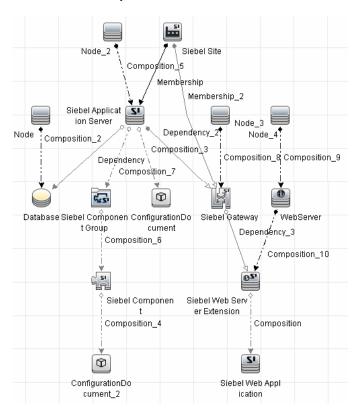
➤ **Siebel Web Topology discovered by SiteScope:**

SiteScope creates the Siebel Web Topology for the SiteScope Siebel Web Server monitor. The CIs are created only for the monitored entities according to the counters that you selected.

➤ **Siebel Topology discovered by SiteScope:**

SiteScope creates the Siebel Topology for the SiteScope Siebel Web Server monitor. The CIs are created only for the monitored entities according to the counters that you selected.

Tasks

⚒ How to Run the Siebel Database Breakdown Diagnostic Tool

This section provides details on running the Siebel Database Breakdown diagnostics tool.

When the user runs Database Breakdown, after defining the analysis scope (Siebel Enterprise, Application, Business Process Step, and so on), Application Management for Siebel automatically increases (through SiteScope) the database log level for the selected component (if a specific component was selected).

Then, Application Management for Siebel instructs the BPM to run the transaction you selected. During the transaction run, as a result of the higher log level, database-related information is written into the application server log.

When the transaction has finished running, the database log level for the selected component is returned to normal by Application Management for Siebel.

To configure the Database Breakdown Diagnostic tool:

1 To run the Database Breakdown tool, select **Applications** > **Application Management for Siebel** > **Database Breakdown** to open the Siebel Database Breakdown Configuration page. For user interface details, see "Siebel Database Breakdown Configuration Report" on page 171.

2 You can also access this page filtered for the selected CI, when you right-click the CI and select the **Siebel Database Breakdown** option.

Note: You can specify a different log folder for each Siebel Component CI. For details, see "How to Define a Different Log Folder Per Siebel Component CI" on page 138.

🔨 How to Run the SARM - User Trace Breakdown Diagnostics Tool – Details

This section describes how to run the SARM - User Trace Breakdown diagnostics tool.

You can view data about the activity taking place in the Web servers and application servers at a specific Siebel Enterprise and for a specific user, in a specified period of time. HP Business Service Management searches all of the SARM files at the Siebel Enterprise, looks for the sessions of the specified user, fetches the appropriate files, runs the SARM analyzer, and lists all of the sessions used by the user.

The task includes the following steps:

➤ "Configure the SARM - User Trace Breakdown Diagnostic Tool parameter" on page 137

➤ "Use the SARM Logs for a specific web and application server" on page 137

➤ "Results" on page 138

1 Configure the SARM - User Trace Breakdown Diagnostic Tool parameter

To configure the SARM - User Trace Breakdown diagnostics tool, select **Applications** > **Application Management for Siebel** > **SARM - User Trace Breakdown to open the SARM - User Trace Breakdown Diagnostic Tool** page. For task details, see "SARM - User Trace Breakdown (Run the Diagnostics Tool) Page" on page 149.

2 Use the SARM Logs for a specific web and application server

Run the SARM - User Trace Breakdown diagnostic tool. The SARM - User Trace Breakdown page indicates the status of each step in the procedure. For details, see "SARM - User Trace Breakdown Dialog Box" on page 154.

After the process is complete, the page closes and the diagnostic results are displayed on the SARM - User Trace Breakdown - Analysis page.

3 Results

The data is then displayed and you can generate different views and pie charts to display the data in a user-friendly manner in the SARM - User Trace Breakdown page. For details, see "Siebel Views" on page 132.

⚑ How to Define a Different Log Folder Per Siebel Component CI

By default, when you run the Database Breakdown tool or the SARM Diagnostics tool, all the database-related information or SARM-related information for the Siebel Application Server CI is kept in the default log folder in Application Management for Siebel per Siebel application.

You can also run the Database Breakdown tool or the SARM Diagnostics tool for each Siebel application, using a different log folder for each Siebel Component CI and for each tool.

You specify the path to the log folders to be assigned to the Siebel Component CI as follows, select **Admin** > **RTSM Administration** > **Modeling** > **IT Universe Manager**, select the Siebel Enterprises view, and right-click the **Siebel Component** CI, and select **Properties**. The Log Folder attribute or the SARM Log Folder attributes are listed in the Configuration Item Properties dialog box. Enter the path to the folders in the **Value** box.

When you run the Database Breakdown tool or the SARM Diagnostics tool and you have selected the **Automatically collect file option** in the **SARM - User Trace Breakdown Diagnostic Tool** page:

➤ If you have specified a path in the Log Folder and SARM Log Folder attributes of the Siebel Component CI instance, the tools use the log files taken from these folders.

➤ If you have not specified a path in the Log Folder and SARM Log Folder attributes, the tools use the log file specified in the Log Folder attribute of the Siebel Application Server CI.

For details about the **Automatically collect file** option, see the Advanced Options section in "SARM - User Trace Breakdown (Run the Diagnostics Tool) Page" on page 149.

For details about the Database Breakdown logs, see "How to Run the Siebel Database Breakdown Diagnostic Tool" on page 136. For details about the SARM Diagnostics tool logs, see "How to Run the SARM - User Trace Breakdown Diagnostics Tool – Details" on page 137.

⚒ How to Display Siebel Information in BSM

Application Management for Siebel is ready. After all these steps are completed, you can view Siebel data in the Service Health, use diagnostic tools, and so on. You can display Siebel information in Service Health using one or more of the capabilities described in this section.@@@change into non-numbered task steps@@@

This task includes the following steps:

➤ "View Siebel information in the Siebel views" on page 139

➤ "View the SARM - User Trace Breakdown Diagnostic report" on page 140

➤ "View the Siebel Database Breakdown Diagnostic report" on page 140

➤ "View the Tasks Diagnostics Tool report" on page 140

➤ "View the Processes Tool report" on page 140

➤ "View Changes Made to Siebel Enterprise CIs" on page 141

➤ "View Configuration File CI details" on page 141

1 View Siebel information in the Siebel views

For details on the views, see "Siebel Views" on page 132.

To enable the other Siebel views, add the **Service Health** bundle and the **Service Level Management** bundle in the View Definition Properties dialog box. For details, see "Query/View Definition Properties Dialog Box" in the *Modeling Guide*.

2 **View the SARM - User Trace Breakdown Diagnostic report**

Application Management for Siebel SARM Diagnostics is a user trace breakdown diagnostic tool that processes the data in the User Session Trace output files produced by Siebel's SARM process. This data can be retrieved for a specific user in a specific time frame. It can also be retrieved for a specific transaction of a prerecorded script.

For details on running the tool, see "How to Run the SARM - User Trace Breakdown Diagnostics Tool – Details" on page 137.

For details on how to display the information, see "Siebel Views" on page 132.

3 **View the Siebel Database Breakdown Diagnostic report**

The Siebel Database Breakdown diagnostic tool enables you to analyze database logs created on the Siebel application server, and extract comprehensive information regarding database time spent by various SQLs.

For details on running the tool, see "How to Run the Siebel Database Breakdown Diagnostic Tool" on page 136.

For details on how to display the information, see "Siebel Database Breakdown Analysis Report" on page 174.

4 **View the Tasks Diagnostics Tool report**

The Siebel tasks diagnostic tool enables you to view details of the Siebel Application Server tasks, for each monitored Siebel Enterprise. For user interface details, see "Tasks Diagnostics Tool Report" on page 176.

5 **View the Processes Tool report**

The Siebel Processes tool enables you to view details of the Siebel Application Server processes, for each monitored Siebel Enterprise. For user interface details, see "Processes Report" on page 147.

6 View Changes Made to Siebel Enterprise CIs

You can assign CIs to keep change information. For details on assigning CIs to keep change information, see the HP Universal CMDB documentation.

When the discovery process discovers changes made to the properties of these CIs, the changes are displayed in the Change report available as a shortcut menu option for each one of the relevant CI types. For user interface details, see "CI Change Report Page" in *Reports*.

7 View Configuration File CI details

For details on viewing the Configuration File CI details, see "View Configuration File CI – Details" on page 142.
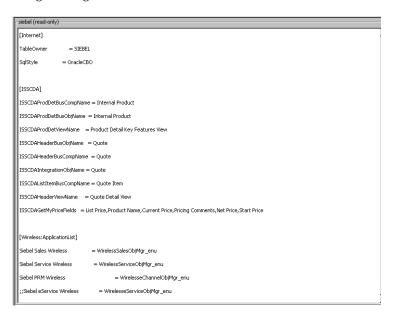
🔨 View Configuration File CI – Details

You can view configuration file details:

➤ **siebel.cfg file.** Right-click the relevant Siebel Application Server CI in the Siebel Enterprises view, select **Properties**, and click **Show document content** to display the details of the **siebel.cfg** file. The **siebel.cfg** configuration file displays information taken from the Siebel application server installation.

```
siebel (read-only)

[Internet]

TableOwner          = SIEBEL

SqlStyle            = OracleCBO


[ISSCDA]

ISSCDAProdDetBusCompName = Internal Product

ISSCDAProdDetBusObjName  = Internal Product

ISSCDAProdDetViewName    = Product Detail Key Features View

ISSCDAHeaderBusObjName    = Quote

ISSCDAHeaderBusCompName  = Quote

ISSCDAIntegrationObjName = Quote

ISSCDAListItemBusCompName = Quote Item

ISSCDAHeaderViewName     = Quote Detail View

ISSCDAGetMyPriceFields   = List Price,Product Name,Current Price,Pricing Comments,Net Price,Start Price


[Wireless:ApplicationList]

Siebel Sales Wireless           = WirelessSalesObjMgr_enu

Siebel Service Wireless          = WirelessServiceObjMgr_enu

Siebel PRM Wireless                    = WirelesseChannelObjMgr_enu

;;Siebel eService Wireless          = WirelesseServiceObjMgr_enu
```

➤ **parameters.cfg file.** Right-click the relevant Configuration File CI in the Siebel Enterprises view, select **Properties**, and click **Show document content** to display details of the **parameters.cfg** file. The **parameters.cfg.** file includes the output of the **list parameters for component** command using srvrmgr.

```
siebel (read-only)

[Internet]

TableOwner          = SIEBEL

SqlStyle            = OracleCBO


[ISSCDA]

ISSCDAProdDetBusCompName = Internal Product

ISSCDAProdDetBusObjName  = Internal Product

ISSCDAProdDetViewName    = Product Detail Key Features View

ISSCDAHeaderBusObjName   = Quote

ISSCDAHeaderBusCompName  = Quote

ISSCDAIntegrationObjName = Quote

ISSCDAListItemBusCompName = Quote Item

ISSCDAHeaderViewName     = Quote Detail View

ISSCDAGetMyPriceFields   = List Price,Product Name,Current Price,Pricing Comments,Net Price,Start Price


[Wireless:ApplicationList]

Siebel Sales Wireless          = WirelessSalesObjMgr_enu

Siebel Service Wireless        = WirelessServiceObjMgr_enu

Siebel PRM Wireless               = WirelesseChannelObjMgr_enu

;;Siebel eService Wireless       = WirelesseServiceObjMgr_enu
```

You can also access this information by selecting **Admin** > **RTSM Administration** > **Modeling** > **IT Universe Manager** > **Properties**. For user interface details, see "Configuration Item Properties Dialog Box" in the *Modeling Guide*.

Reference

🪄 Shortcut Menu Options

In the Siebel-related views, right-click CIs to display a list of the shortcut menu options available in the Siebel Enterprises view. An additional shortcut menu option is **SiteScope Cross-Performance Report** accessed by using the Siebel Cross-Performance option.

For details, see "Service Health Menu Options" in *Using Service Health*.

🪄 Default CITs in the Siebel View

In Service Health, access the Siebel Enterprises view to view information about the Siebel IT entities, the Siebel enterprise metrics monitored by SiteScope monitors, and information about the Siebel business processes/ transactions simulated by BPM scripts. For details about the view, see "Siebel Views" on page 132.

The CITs are as follows

CIT (A-Z)	Icon	Description
Business Transaction		The Business Process Transaction CIs are emulated Siebel transactions executed on a BPM machine. They are used to supply proactive monitoring of end user experience.
CI Collection		The Group CI is a logical container. This is not a Siebel-specific CI. The Siebel Enterprises view includes the following groups: Applications, Business Processes, Hosts, and Locations.

CIT (A-Z)	Icon	Description
Configuration Document		The Configuration File CIs represent the **siebel.cfg** configuration file that includes information from the application server installation or the **parameters.cfg** that includes the output of the list parameters for component command using srvrmgr.
Database		The Database CI represents the database that is holding the data tier. This is not a Siebel-specific CI.
Node		A Node CI represents the physical machine on which a server is installed. This is not a Siebel-specific element.
Siebel Application		The Siebel Application CI represents the Siebel complete solution for an organization's needs in a certain area. For example: marketing, call center, and so forth.
Siebel Application Server		The Siebel Application Server CI represents a server running the business logic tier that supports both back-end and interactive processes for every Siebel client.
Siebel Component		The Component CI represents a process running on the Siebel Application Server, which encapsulates some Siebel application functionality.
Siebel Component Group		The Component Group CI represents an administrative grouping of components comprising an application running on the Siebel Application Server.
Siebel Gateway		The Siebel Gateway server is a coordinating server that routes requests to the correct component and provides enhanced scalability, load balancing, and high availability across the Siebel Enterprise.

CIT (A-Z)	Icon	Description
Siebel Web Application		The Siebel Web Application CI represents the application URL as it exists on the Siebel Web Server Extension.
Siebel Web Server Extension		The Siebel Web Server Extension CI represents the Siebel Web Server Extension installed on the Web server.
Web Server		The Web Server CI represents the Web server that forwards requests to the Siebel enterprise.

🔍 Application Management for Siebel Views and Reports User Interface
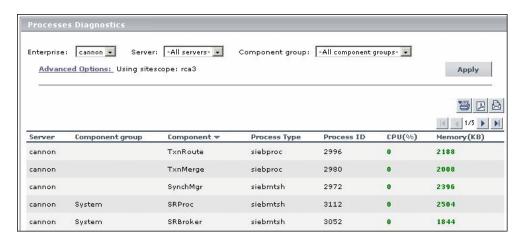
This section describes:

➤ Processes Report on page 147

➤ Processes Tool - Advanced Filter Dialog Box on page 149

➤ SARM - User Trace Breakdown (Run the Diagnostics Tool) Page on page 149

➤ SARM - User Trace Breakdown Dialog Box on page 154

➤ SARM - User Trace Breakdown - Analysis Report on page 155

➤ Siebel Database Breakdown Configuration Report on page 171

➤ Siebel Database Breakdown Analysis Report on page 174

➤ Tasks Diagnostics Tool Report on page 176

➤ Tasks Diagnostics Tool - Advanced Filter Dialog Box on page 179

🔍 Processes Report

This report enables you to view details of the Siebel Application Server processes, for each monitored Siebel Enterprise.

The following is an example of the Processes report.

To access	**Applications** > **Application Management for Siebel** > **Processes**
	You can also access this page filtered for a selected CI, when you right-click the CI in Service Health and select the **Siebel Processes** option. For details, see "Siebel Processes" in *Using Service Health*.
Important information	➤ To sort the processes by a specific column, click the column heading.
	➤ To move between pages, use the **First**, **Previous**, **Next**, and **Last** arrows ⏮ ◀ ▶ ⏭ above the table.
Relevant tasks	"View Configuration File CI – Details" on page 142

User interface elements are described below:

UI Element (A-Z)	Description
Advanced Options	If necessary, click to open the Processes Diagnostics Tool - Advanced Filter page. For details, see "Processes Tool - Advanced Filter Dialog Box" on page 149.
Apply	Click the **Active Filter** button to display the process diagnostic information. The process information you requested is retrieved from the Siebel Application Servers and displayed on the Tasks Diagnostic Tool page.
Component	The name of the component. If the process does not have a task attached, then the Component column is empty.
Component Group	Select the name of the component groups. Select **All component groups** to display the process diagnostics for all of the component groups.
Component Group	The name of the component group. If the process does not have a task attached, then the Component Group column is empty.
CPU (%)	The percentage of the host machine CPU that the relevant process instance is currently using.
Enterprises	Select the name of the Siebel Enterprise.
Memory (KB)	The amount of memory (in KB) that the relevant process instance is currently using.
Process ID	The process identifier.
Process Type	The name of the operating system process that deals with the Siebel process.
Server	Select the name of the application server. Select **All servers** to display the process diagnostics for all of the application servers.
Server	The name of the server on which the process runs.

🔍 Processes Tool - Advanced Filter Dialog Box

This dialog box enables you to filter the list of processes you want to display.

To access	In the Processes Diagnostics Tool page, click the **Advanced Filter** link.

User interface elements are described below:

UI Element (A-Z)	Description
Process Id	Enter the process ID.
Process Type	Select the type of process. Select **All process types** to display the process diagnostics for all of the process types.
Siebel Components	Select the Siebel component. Select **All components** to display the process diagnostics for all of the Siebel components.
Using SiteScope	Select the SiteScope machine you want to use to retrieve process information.

🔍 SARM - User Trace Breakdown (Run the Diagnostics Tool) Page

Application Management for Siebel SARM Diagnostics is a user trace breakdown diagnostic tool that processes the data in the User Session Trace output files produced by Siebel's SARM process. This data can be retrieved for a specific user in a specific time frame. It can also be retrieved for a specific transaction of a prerecorded script.

You can then specify where the following files can be found:

➤ Automatically collected Web and application server logs.

➤ The SARM logs of a specific application server and Web server.

➤ An already generated user session trace XML file for a Siebel Enterprise, a user, and a specific time frame.

To access	Use one of the following:
	➤ **Applications** > **Application Management for Siebel** > **SARM - User Trace Breakdown** to open the SARM - User Trace Breakdown Diagnostic Tool page.
	➤ You can also access this page filtered for the selected CI, when you right-click the CI and select the **Go to** > **Siebel SARM** option. For details, see "Service Health Menu Options" in *Using Service Health*.
Important information	For an example of setting up the tool, see "Example of Setting Up the SARM - User Trace Breakdown Tool:" on page 152.
Relevant tasks	"View Configuration File CI – Details"

User interface elements are described below:

UI Element (A-Z)	Description
Advanced Options	You can run the SARM - User Trace Breakdown diagnostic tool on:
	➤ automatically collected Web and application server logs.
	➤ the SARM logs of a specific application server and Web server.
	➤ an already generated user session trace XML file for a site, a user, and a specific time frame. HP Business Service Management searches all of the SARM files at the Siebel Enterprise, looks for the sessions of the specified user, fetches the appropriate files, runs the SARM analyzer, and lists all of the sessions used by the user that were active within the time frame.
Enterprises	Select the Siebel Enterprise for which you want to view SARM User Trace Breakdown data.

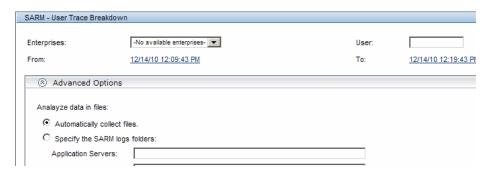| UI Element (A-Z)	Description
From ... To	Click the linked date in **From** or **To** to open a calendar and select a new date and time to change the default date and time.
User	Enter the name of the user whose activity you want to trace.

Advanced Options Area

User interface elements are described below:

UI Element (A-Z)	Description
Automatically collect files	Select to run SARM - User Trace Breakdown diagnostics on all Web and application servers at the Siebel Enterprise. Then select the SiteScopes used to collect the data in the **Using SiteScope** list. This is the default. You can specify a different SARM log folder for each Siebel Component CI. For details, see "How to Define a Different Log Folder Per Siebel Component CI" on page 138.
Run	Click to run the diagnostics tool. The resulting information is displayed in the SARM - User Trace Breakdown - Analysis screen. For details, see "Siebel Views" on page 132.
Specify a User Session Trace File	Select **Specify a User Session Trace File** to work on an already generated user session trace XML file. In the **User Session Trace File** box, enter the path to the trace file. The path is relative to the SiteScope machine. Then select the SiteScopes used to collect the data in the **Using SiteScope** list.

UI Element (A-Z)	Description
Specify the SARM logs folders	Select **Specify the SARM logs folders** to run SARM - User Trace Breakdown diagnostics only on the specified Web and application servers for the Siebel Enterprise: ➤ In the **Application Servers** box, enter the path to the SARM logs of the application servers. ➤ In the **Web Servers** box, enter the path to the SARM logs of the Web servers. The paths are relative to the SiteScope machine. Then select the SiteScopes used to collect the data in the **Using SiteScope** list. This is the default.
Using SiteScope	Enter the SiteScopes used to collect the data.

Example of Setting Up the SARM - User Trace Breakdown Tool:

Select the Siebel Enterprise for which you want to view SARM User Trace Breakdown data, enter the name of the user whose activity you want to trace in the User box, and click the linked date in **From** or **To** to open a calendar. Select a new date and time to change the default date and time.

After you configure the SARM, you can:

➤ **Specify where the files can be found**:

   ➤ **Automatically collected Web and application server logs.** You can run the SARM - User Trace Breakdown diagnostic tool on automatically collected Web and application server logs.

   Note: You can specify a different SARM log folder for each Siebel Component CI. For details, see "How to Define a Different Log Folder Per Siebel Component CI" on page 138.

   ➤ **The SARM logs of a specific application server and Web server.** You can run the SARM - User Trace Breakdown diagnostic tool on the SARM logs of a specific application server and Web server.

   ➤ **An already generated user session trace XML file for a Siebel Enterprise, a user, and a specific time frame.** You can run the SARM - User Trace Breakdown diagnostic tool on an already generated user session trace XML file for a site, a user, and a specific time frame. HP Business Service Management searches all of the SARM files at the Siebel Enterprise, looks for the sessions of the specified user, fetches the appropriate files, runs the SARM analyzer, and lists all of the sessions used by the user that were active within the time frame.

   For details, see "Advanced Options Area" on page 151.

You can then run the diagnostic tool.

🔍 SARM - User Trace Breakdown Dialog Box

When you run the SARM - User Trace Breakdown diagnostic tool, the SARM - User Trace Breakdown page indicates the status of each step in the procedure.
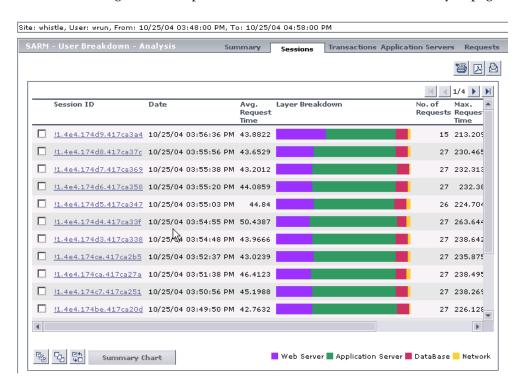
Important information	After the process is complete, the page closes and the diagnostic results are displayed on the SARM - User Trace Breakdown - Analysis page. For details, see "Siebel Views" on page 132.

User interface elements are described below:

UI Element (A-Z)	Description
Analyze Results and Prepare Charts	When the status indicator shows running stripes, the final results are being analyzed and charts are prepared. When the status indicator is complete, the loading has completed.
Check SiteScopes connectivity	When the status indicator shows running stripes, the SiteScopes connectivity is being checked. When the status indicator is complete, the operation has completed.
Extract Application Servers' session data	When the status indicator shows running stripes, the application server session data is being extracted. When the status indicator is complete, the extraction has completed.
Load Web Servers' session data	When the status indicator shows running stripes, the Web server session data is being loaded. When the status indicator is complete, the loading has completed.
Processing	The progress in the current step.
Total Progress	Indicates the total progress of the SARM - User Trace Breakdown diagnostic tool.

✎ SARM - User Trace Breakdown - Analysis Report

This report enables you to view trace breakdown information.

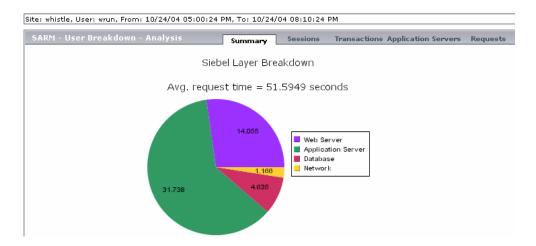The following is an example of the SARM - User Breakdown - Analysis page.

To access	Run the user trace breakdown diagnostic tool. For details, see "SARM - User Trace Breakdown (Run the Diagnostics Tool) Page" on page 149.
Relevant tasks	"View Configuration File CI – Details"

Summary Tab

This tab enables you to view a chart that displays the segmentation between the average Application Server time, Web Server time, Network time, and Database time for all of the relevant requests that were found in the files. For details, see "SARM - User Trace Breakdown - Analysis Report" on page 155.

The following is an example of the Summary page.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Drilldown>	Drilling down from one of the segments in the chart provides a pie chart that displays the segmentation between the sub areas of that segment. If there is another level of specification (available in Siebel 7.7), you can then drill down to the sub area level.
	You can then click segments of the Area Breakdown chart to open the corresponding Sub Area Breakdown chart (if it exists). For details, see "Sub Area Breakdown and Area Breakdown" on page 157.
<Pie chart>	The chart displays the segmentation between the average Application Server time, Web Server time, Network time, and Database time for all of the relevant requests that were found in the files.

Sub Area Breakdown and Area Breakdown

The breakdown is as follows:

Layer Breakdown	Area Breakdown	Sub Area Breakdown
Web Server	N/A	N/A
Application Server	Application Manager	Request Receipt (sessID SeqID)
	Object Manager	Session Re-Login
	Communications Server Services	Communications Client Invoke Method
		Communications Server Invoke Method
	Build Web Page	Build View Layout
		Show Applet, Build View Data
		Build Applet
		Get View Layout
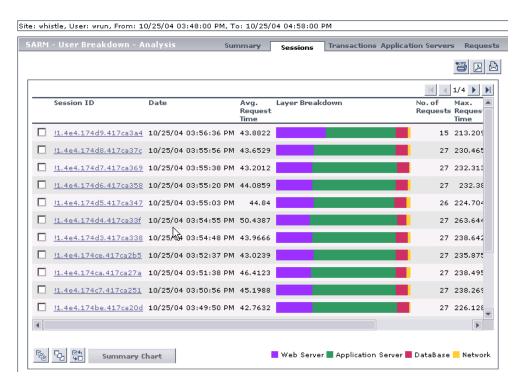
Layer Breakdown	Area Breakdown	Sub Area Breakdown
Database	Database Connector	N/A
Network	N/A	N/A

Sessions Tab

This tab enables you to view the time distribution of the various sessions. For details, see "SARM - User Trace Breakdown - Analysis Report" on page 155.
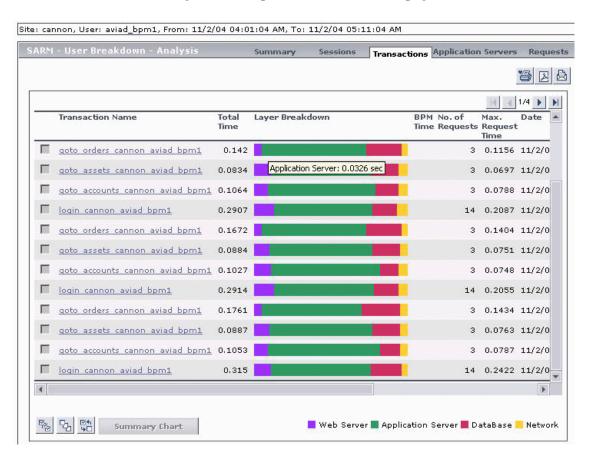
The following is an example of the Sessions page.

User interface elements are described below:

UI Element (A-Z)	Description
Application Server	The name of the application server on which the session is running.
Avg. Request Time (sec)	The average time the request spent in the session.
Date	The timestamp of the session.
Layer Breakdown	The breakdown of the layer into its areas relative to the time spent by the session in each area: Web Server, Application Server, Database, and Network. Tooltips display the average time the session spent in each area.
Max Request Time (sec)	The maximum time spent by a request in the session. Scroll to the right to see the rest of the information.
No. of Requests	The number of requests that ran in the session.
Session Id	The ID of the session. You can drill down from the session ID to display information about the session requests. For details, see "Requests Tab" on page 165.
Summary	You can select one or more sessions and click **Summary** to display a summary chart for the sessions you selected. For details, see "Summary Tab" on page 156.
Task ID	The ID of the task to which the request belongs.
Web Server	The name of the Web server on which the session is running.

Transactions Tab

This tab enables you to view, for each Business Process Monitor transaction, the timestamp of the session it belongs to, the session id, the application server name, the average total time of all requests that belong to that transaction, the number of request and the maximal request time. For details, see "SARM - User Trace Breakdown - Analysis Report" on page 155.

The following is an example of the Transactions page.

User interface elements are described below (unlabeled elements are shown in angle brackets):

| UI Element (A-Z)	Description
<Drilldown from a transaction>	Displays all of the requests that belong to that transaction. For details, see "Requests Tab" on page 165.
<tooltip>	Click any part of the chart to get the tooltip that indicates the time the transaction spent in the layer, area, or sub area.
Application Server	The name of the application server on which the transaction ran.
BPM Time	This column displays the time the invoked transaction ran in BPM (only when the transaction is invoked using Invoke BPM Script). This value is larger than the value in the **Total Time** column as it includes client time, network time, and so on.
	Note: This is displayed only when the SARM User Session Trace breakdown diagnostics has been run after invoking a BPM script monitoring the Siebel Application. Additional tuning of Siebel Application and Web Server environment variables is required because the flush ratio of SARM files is approximately five times slower in the Web Server than in the Application Server, and therefore running SARM with the default value of **SARM_MaxFileSize** variable might not be enough for the SARM User Trace Breakdown diagnostic tool to return data. For details, see "Troubleshooting SARM-Related Issues" on page 106.
Date	The date when the transaction ran.
Layer Breakdown	The breakdown of the layer into its areas relative to the time spend by the transaction in each area: Web Server, Application Server, Database, and Network. Tooltips display the average time the transaction spent in each area.
Max. Request Time	The maximum time spent by any of the requests in the transaction.
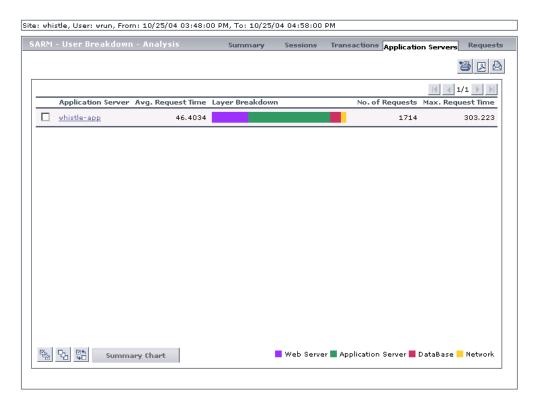
UI Element (A-Z)	Description
No. of Requests	The number of transaction requests that ran in this application server.
Session ID	The ID of the session.
Task ID	The ID of the task to which the transaction belongs.
Total Time	The total time the transaction ran in Siebel.
Transaction Name	The name of the transaction.
Web Server	The name of the Web server on which the transaction ran.

Application Servers Tab

This tab enables you to view a comparison between application servers in terms of times' distribution. For details, see "SARM - User Trace Breakdown - Analysis Report" on page 155.

The following is an example of the Application Servers page.
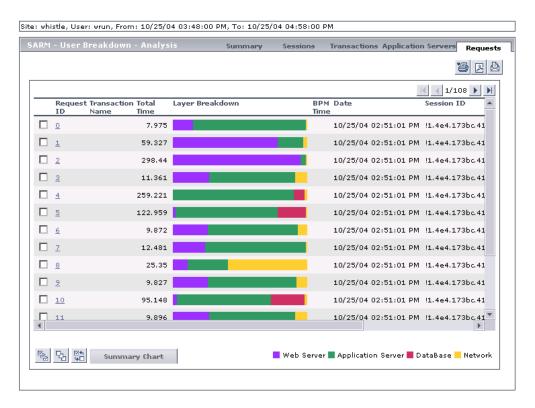
User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Drilldown from an application server>	Displays all of the requests that were executed on that application server. For details, see "Requests Tab" on page 165.
Application Server	The name of the application server. You can drill down from the session ID to display information about the application server. For details, see "Requests Tab" on page 165.
Avg. Request Time	The average time spent by a request executing in this application server.
Layer Breakdown	The time consumption breakdown by layers into its areas relative to the time spent by the request in each area: Web Server, Application Server, Database, and Network. Tooltips display the average time the request spent in each area.
Max. Request Time	The maximum time a request spent in this application server.
No. of Requests	The number of requests that ran in this application server.
Summary	Select one or more application servers and click **Summary** to display a summary chart for the application servers you selected. For more details on the summary chart, see "Summary Tab" on page 156.

Requests Tab

This tab enables you to view, for each request, the request detailed information. For details, see "SARM - User Trace Breakdown - Analysis Report" on page 155.

The following is an example of the Requests page.

User interface elements are described below:

UI Element (A-Z)	Description
Application Server	The name of the application server on which the task ran.

UI Element (A-Z)	Description
BPM Time	Displays the time the invoked request ran in BPM (only when the request is invoked using Invoke BPM Script). This value is larger than the value in the **Total Time** column as it includes client time, network time, and so on.
	Note: The **BPM Time** is displayed only when the SARM User Session Trace breakdown diagnostics has been run after invoking a BPM script monitoring the Siebel Application. Some additional tuning of Siebel Application\Web Server environment variables is required. This is due to the fact that the flush ratio of SARM files is approximately five times slower in the Web Server than in the Application Server, and therefore running SARM with the default value of **SARM_MaxFileSize** variable might not be enough for the SARM User Trace Breakdown diagnostic tool to return data. For details, see "Troubleshooting SARM-Related Issues" on page 106.
Date	The date when the request ran.
Layer Breakdown	The time consumption breakdown by layers into its areas relative to the time the request spent in each area: Web Server, Application Server, Database, and Network. Tooltips display the average time the request spent in each area.
Request ID	The ID of the request.
	You can drill down from the request ID to display information about the area where the request ran. For details, see "Area Details Area" on page 167.
Session ID	The ID of the session on which the request ran. Scroll to the right to see the rest of the information.
Summary	Select one or more application servers and click **Summary** to display a summary chart for the application servers you selected. For more details on the summary chart, see "Summary Tab" on page 156.
Task ID	The ID of the task the request belongs to.

UI Element (A-Z)	Description
Total Time	The total time spent to execute a request.
Transaction Name	The name of the transaction the request belongs to.
Web Server	The name of the Web server on which the task ran.

Area Details Area

To access	In the Requests page, you can drill down from the request ID to display information about the area where the request ran.

User interface elements are described below:

UI Element (A-Z)	Description
Area Name	The name of the area where the request ran. You can drill down from the area name to display information about its sub areas. For details, see "Sub Area Details Area" on page 168.
Avg. Execution Time	The average time spent by the request executing in the area.
Exclusive Memory Max Allocated Sub Area	The amount of memory used by requests that entered only this area.
Max Execution Time	The maximum time spent by the request executing in the area.
Max Response Time SARM node App String 1	The name of the method invoked or workflow process involved.
Max Response Time SARM node App String 2	The name of the method invoked or workflow process involved.
No. of Sub Areas	The number of sub areas in the area.
Non-Recursive Invocations	The number of times requests were invoked (non-recursive invocation) in the area.

UI Element (A-Z)	Description
Recursive Invocations	The number of times requests were invoked by other requests (recursive invocation) in the area.
Summary	Select one or more application servers and click **Summary** to display a summary chart for the application servers you selected. For more details on the summary chart, see "Summary Tab" on page 156.
Total Execution Time	The total time spent by the request executing in the area.

Sub Area Details Area

To access	In the Area Details page, click an area name to display information about its sub areas.

User interface elements are described below:

| UI Element (A-Z)	Description
Area Name	The name of the area where the sub area is located.
Avg. Execution Time	The average time spent by the request executing in the sub area.
Exclusive Memory Max Allocated Instance	The amount of memory used by requests that entered only this sub area.
Max Execution Time	The maximum time spent by the request executing in the sub area.
Max Response Time SARM node App String 1	The name of the method invoked or workflow process involved.
Max Response Time SARM node App String 2	The name of the method invoked or workflow process involved.
No. of Instances	The number of instances of the request.

UI Element (A-Z)	Description
Non-Recursive Invocations	The number of times requests were invoked (non-recursive invocation) in the sub area. Scroll to the right to see the rest of the information.
Recursive Invocations	The number of times requests were invoked by other requests (recursive invocation) in the sub area.
Sub Area Name	The name of the sub area where the request ran. You can drill down from the sub area name to display information about the session requests. For details, see "Instance Details Area" on page 169.
Summary	Select one or more application servers and click **Summary** to display a summary chart for the application servers you selected. For more details on the summary chart, see "Summary Tab" on page 156.
Total Execution Time	The total time spent by the request executing in the sub area.

Instance Details Area

To access	In the Sub Area Details page, click a sub area name to display information about the session requests.

User interface elements are described below:

UI Element (A-Z)	Description
Area Name	The name of the area where the request ran.
Avg. Execution Time	The average time spent by the request executing in the instance.
Instance Name	The name of the instance where the request ran.
Max Execution Time	The maximum time spent by the request executing in the instance.
Max Response Time SARM node App String 1	The name of the method invoked or workflow process involved.
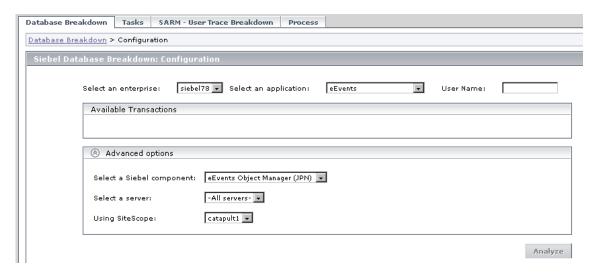
UI Element (A-Z)	Description
Max Response Time SARM node App String 2	The name of the method invoked or workflow process involved.
Non-Recursive Invocations	The number of times requests were invoked (non-recursive invocation) in the instance. Scroll to the right to see the rest of the information.
Recursive Invocations	The number of times requests were invoked by other requests (recursive invocation) in the instance.
Sub Area Name	The name of the sub area where the request ran.
Summary	Select one or more application servers and click **Summary** to display a summary chart for the application servers you selected. For more details on the summary chart, see "Summary Tab" on page 156.
Total Execution Time	The total time spent by the request executing in the instance.

🔍 Siebel Database Breakdown Configuration Report

This report enables you to run the Database Breakdown tool.

The following is an example of the Siebel Database Breakdown Configuration report.

To access	Use one of the following:
	➤ **Applications** > **Application Management for Siebel** > **Database Breakdown** to open the Siebel Database Breakdown Configuration page.
	➤ You can also access this page filtered for the selected CI, when you right-click the CI and select the **Siebel Database Breakdown** option. For details, see "Service Health Menu Options" in *Using Service Health*.
Relevant tasks	"View Configuration File CI – Details" on page 142

Selection Area

User interface elements are described below:

UI Element (A-Z)	Description
Select an application	In the list, select the Siebel application for which you want to analyze data.
Select an enterprise	In the list, select the Siebel Enterprise.
User Name	The value in the **User Name** box appears automatically when you select the application. The appropriate user name has been entered manually by your administrator after discovery has taken place and the monitoring script was recorded, but you can override it. For details, see "How to Deploy the SiteScope Siebel Monitors" on page 86.

Available Transactions Area

This area lists the transactions when you select a Siebel Enterprise and an application in the top part of the page. Click the BPM transaction whose activity you want to analyze. (The list of transactions includes only those for which you have permissions.)

Important information	For diagnostic purposes it is recommended to use a script running a dedicated user. This enables you to make sure diagnosis results refer to the BPM transaction intended to be analyzed.

Advanced Options Area

User interface elements are described below:
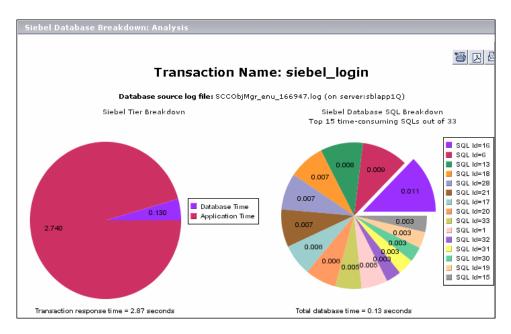
UI Element (A-Z)	Description
Analyze	Click to display the Siebel Tier Breakdown and Siebel Database SQL Breakdown pie charts. For details, see "Siebel Database Breakdown Analysis Report" on page 174.
Select a server	Select a Siebel Application Server in the list. You can also leave **All servers** selected.
Select a Siebel component	Select a Siebel component in the list. Only the log level for that component is brought up.
Using SiteScope	Select the SiteScope machine you want to use to monitor the Siebel component in the list.
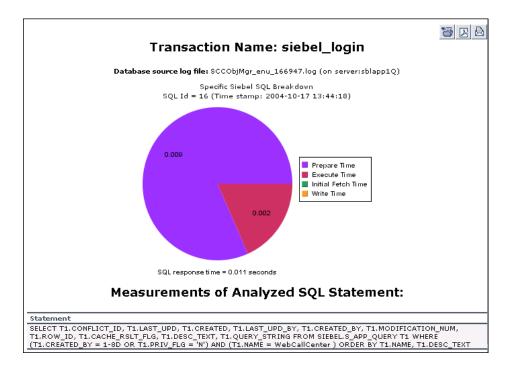
🔍 Siebel Database Breakdown Analysis Report

This report analyzes the Siebel database logs that you have created to determine which of the component SQL operations, or parts of operations, were responsible for slow database response time.

An example of the report:

An example of the detail of one segment of the pie chart:

To access	Click **Analyze** on the Siebel Database Breakdown: Configuration (Advanced Option) page.
Relevant tasks	"View Configuration File CI – Details" on page 142

User interface elements are described below:
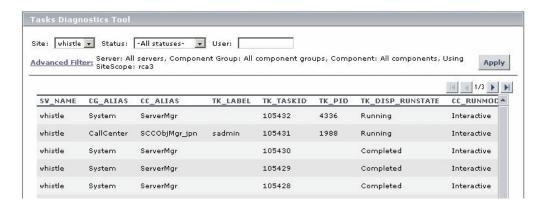
UI Element (A-Z)	Description
Siebel Database SQL Breakdown Pie Chart	Displays a breakdown of up to 15 of the most time-consuming SQLs.

UI Element (A-Z)	Description
Siebel Tier Breakdown Pie Chart	Shows the transaction's database time relative to its application time.
Specific SQL Breakdown Pie Chart	Click, in the Siebel Database SQL Breakdown pie chart, a section representing the required SQL, to view the database-specific time distribution of that specific SQL. For each SQL operation, you can view the various database times: preparation time, execution time, initial fetch time, total time, and write time (time stamp). This enables you to isolate the exact segment responsible for the delay in the database response time. Underneath the Specific SQL Breakdown pie chart, you can view the corresponding SQL statement.

✒ Tasks Diagnostics Tool Report

This report enables you to view details of Siebel Application Server tasks.

To access	Use one of the following:
	➤ **Applications** > **Application Management for Siebel** > **Tasks** to open the Task Diagnostics Tool page.
	➤ You can also access this page filtered for the selected CI, when you right-click the CI and select the **Siebel Tasks in Error** or **Siebel Running Tasks** option. For details, see "Service Health Menu Options" in *Using Service Health*.
Important information	➤ To sort the tasks by a specific column, click the column heading.
	➤ To move between pages, use the arrows $\vert\blacktriangleleft\;\blacktriangleleft\;\blacktriangleright\;\blacktriangleright\vert$ above the table.
Relevant tasks	"View Configuration File CI – Details" on page 142

User interface elements are described below:

UI Element (A-Z)	Description
Advanced Filter	If necessary, click the link to filter the list of tasks. For details, see "View Configuration File CI – Details" on page 142.
Apply	When you click the **Apply** button, the task information you requested is retrieved from the Siebel Application Servers and displayed on the Tasks Diagnostic Tool page.
CC_ALIAS	The name of the component the task belongs to.
CC_INCARN_NO	The number of times the task was restarted.
CC_RUNMODE	The mode used to execute the task: **Interactive** or **Batch**.
CG_ALIAS	The name of the component group the task belongs to.
Enterprise	Select the Siebel site/enterprise for which you want to view task data.

UI Element (A-Z)	Description
Status	Select the specific status—**Running**, **Paused**, **Stopping**, **Completed**, **Exited with Error**, or **Killed**. Alternatively, you can select to view tasks of all statuses.
SV_NAME	The name of the server on which the task is running.
TK_DISP_RUNSTATE	The state of the task: **Running**, **Paused**, **Stopping**, **Completed**, **Exited with Error**, or **Killed**.
TK_END_TIME	The time when the task stopped executing.
TK_IDLE	For future use.
TK_LABEL	The name of the user who is running the tasks. Some tasks (such as the ones belonging to the system component group) do not have a user.
TK_PARENT_T	The task that caused this task to execute.
TK_PID	The operating system process ID that deals with the task. One process can handle more than one task. This column displays data only for tasks whose TK_DISP_RUNSTATE is **running**.
TK_PING_TIM	For future use.
TK_START_TIME	The time when the task started to execute.
TK_STATUS	A description of the task—added by the task. If **TK_DISP_RUNSTATE** is **Exited with Error**, **TK_STATUS** displays the error message.
TK_TASKID	The ID of the task.
TK_TASKTYPE	The urgency of the task.
User	To focus on the tasks of a specific user, fill in the user name in the User box.

🔍 **Tasks Diagnostics Tool - Advanced Filter Dialog Box**

Use the advanced filter to filter the list of tasks you want to display.

To access	In the Task Diagnostics Tool page, click the **Advanced Filter** link to open the Tasks Diagnostics Tool Advanced Filter page.

User interface elements are described below:

UI Element (A-Z)	Description
Component	Select the specific component for which you want to view task data.
Component group	Select the specific component group for which you want to view task data.
Server	Select the specific server whose task data you want to view.
Using SiteScope	Select the SiteScope machine you want to use to retrieve task data from the Siebel Application Server, if you do not want Application Management for Siebel to use the default SiteScope machine.

Part III

Application Management for SOA

5

HP Business Service Management for SOA

This chapter includes:

Concepts

Tasks

Concepts

🔷 SOA Solution Overview

HP Business Service Management enables you to monitor your Service Oriented Architecture (SOA) environment, by monitoring the performance of SOA components within the environment. The data is collected by the following HP Business Service Management components:

➤ Discovery and Dependency Mapping jobs identify and map the SOA-based applications in your system from the UDDI registry and from the Web services deployed on IBM WebSphere, BEA WebLogic, Oracle Application Server, and IIS containers. For more information, see "SOA Data Flow Management Modules" on page 188.

➤ Dedicated SiteScope monitors collect Web service metrics and UDDI server health data. For more information, see "SiteScope Monitors for SOA" on page 195.

➤ Business Process Monitors collect Web service performance data using BPM transactions that run Web services scripts. The scripts create the CIs and the relationships in the HP Universal CMDB. For more information, see "Run BPM Transactions for SOA" on page 205.

➤ Diagnostics probes collect Web service performance and availability metrics directly on the Web server machines. For more information, see "Integration of HP Diagnostics Data with SOA" on page 192. Diagnostics data is displayed in SOA reports and views.

BPM and SiteScope are used for synthetic monitoring of Web services while Diagnostics is used for real monitoring of Web services calls.
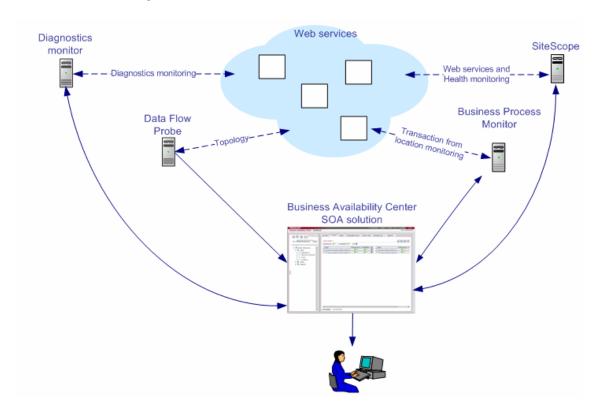
The collected data is used to build the SOA views and reports available from **Applications** > **Application Management for SOA**. For details, see "SOA Views and Their Components" on page 222.

Service Level Management

To gain visibility into performance or availability issues affecting Service Level Agreements (SLAs), you create SLAs centered around your Application Management for SOA Web Services Configuration Items (CIs). For details on SLAs, see "Service Level Management - Overview" in *Using Service Level Management*.

🔩 Architecture

The following diagram illustrates the components of Application Management for SOA.

All monitors create their own topology in the Run-time Service Model (RTSM). In addition to user transactions, BPM also sends topology data and SOA samples (events and performance) to the RTSM. Automatic discovery adds more information about the SOA CIs and their relationships in the RTSM.

This section includes the following topics:

➤ "Components of the Application Management for SOA Architecture" on page 186

➤ "Data Aggregation" on page 187

➤ "Sample" on page 188

Components of the Application Management for SOA Architecture

The architecture of the Application Management for SOA solution includes the following components:

➤ The Data Flow Probe communicates with RTSM. The RTSM server collects information on changes made to a CI's properties. Those changes include changes of the SOA infrastructure: hosts, application servers, and others) and functional changes of the Web services (changes to WSDL (Web Services Description Language); for example if a new parameter or a new operation was added or if an operation was removed). This information is stored in the History database, and is available in the SOA-related views in HP Business Service Management. For details on the History database, see the *HP Business Service Management Database Guide* PDF. For details on the change feature, see "View changes made to SOA CIs" on page 232.

The appropriate discovery jobs (in Data Flow Management) are used by the Data Flow Probe to discover, identify, and map the SOA-based applications in your system, starting from the UDDI registry, and continuing with Web services deployed on IBM WebSphere, BEA WebLogic, Oracle Application Server, and IIS (Internet Information Services). This information is then used to create SOA-related CIs and other CIs in the RTSM. It also creates the hierarchy of CIs displayed in the SOA UDDI Registry, the SOA Web Services, the SOA Rogue Services, and other views. A rogue service is a service which is not registered in the UDDI registry.

➤ BPM collects data on the performance and availability of Web services by running transactions that run Web services scripts. The script enters the CIs and relationships corresponding to the incoming BPM samples into the RTSM. BPM data is available in the SOA reports when you select the **Synthetic** parameter. For details, see each report description in "SOA Views and Reports User Interface" on page 235. For details on the samples, see "Data Samples for Business Process Monitor" in *Reports*.

➤ SiteScope monitors the Web services and retrieves Web services metrics and UDDI server health data. When working with SiteScope 9.50 and above, the CIs and relationships corresponding to the incoming SiteScope samples are created by the relevant assignments. SiteScope data is available in the SOA reports when you select the **Synthetic** parameter. For details, see each report description in "SOA Views and Reports User Interface" on page 235.

➤ The Diagnostics Monitor monitors real-user traffic to the Web services and operations and sends the information to the Diagnostics server. The Diagnostics server uses an SDK (Software Development Kit) to send the topology to the RTSM and the samples to BSM. The relevant assignments assign the HIs and KPIs to the relevant CIs. Diagnostics data is available in the SOA reports when you select the **Real Data** parameter. For details, see each report description in "SOA Views and Reports User Interface" on page 235.

Service Health tabs and reports are used as the central console for viewing all of the data and analyzing it. For concept details, see "Introducing Service Health" in *Using Service Health*.

Data Aggregation

HP Business Service Management uses data aggregation to make data handling and management more efficient and to improve the speed and performance of report generation. For more information on data aggregation in HP Business Service Management, see "Data Aggregation" in *Reports*.

Sample

Application Management for SOA solution uses measurements from the
ws_perf_aggr_t sample type. For details, see "Sample: SOA Event
(ws_event_aggr_t)" in *Reports*.

SOA Data Flow Management Modules

HP Business Service Management includes discovery patterns for
monitoring your SOA environment.

The Discovery and Dependency Mapping modules listed in this section,
discover the Web services and WSDL files that relate to your SOA
infrastructure. A WSDL file contains several sections that can be mapped to
different Configuration File CIs. For example, the service operations can be
mapped to one CI and the service binding information to a different CI.
This practice enables sharing similar definitions across Web services.

When a module is run, it creates CIs in the RTSM, corresponding to the
discovered elements. The appropriate BSM views are automatically
populated with the created CIs, according to the TQL for each view. For
more information about the discovery modules and mechanisms, see
"Discovery Overview" in the *HP Universal CMDB Discovery and Integration
Content Guide*.

Note: BSM also supports nested WSDL files.

The Discovery and Dependency Mapping modules are listed in the following table:

Module (A - Z)	Description
Application - Webservices Module	The module contains the UDDI registry pattern and is mainly responsible for mapping the service providers, Web services, and WSDL files that are discovered from the UDDI registry (for UDDI versions 2 and 3). This information is presented in the SOA UDDI view.
	For information about the Application - Webservices module, see "UDDI Registry Discovery" in the *HP Universal CMDB Discovery and Integration Content Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.
	For details on the SOA UDDI view, see "SOA Views and Their Components" on page 222.
	Note: WSDL files should be placed in the UDDI registry according to the following UDDI hierarchy (from the UDDI technical specification by OASIS): **BusinessService** > **TemplateBinding** > **TModel** > **OverViewDoc**. They cannot be found in any other location.

Module (A - Z)	Description
J2EE - WebLogic Module	The module discovers Web services and their WSDL files, deployed on BEA WebLogic servers. The resulting CIs for the Web services, Web service operations, and configuration files are presented in the WebLogic Topology view (along with other components discovered on the WebLogic servers) and are added to the SOA Web Services view and SOA UDDI view, as relevant.
	For information about the J2EE - WebLogic module, see "WebLogic Discovery" in the *HP Universal CMDB Discovery and Integration Content Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.
	For details on the SOA UDDI and SOA Web Services views, see "SOA Views and Their Components" on page 222.
J2EE - WebSphere Module	The module discovers WSDL files deployed on IBM WebSphere servers, and parses the WSDL to identify the Web service components. The resulting CIs for the Web services, Web service operations, and configuration files are presented in the WebSphere Topology view (along with other components discovered on the WebSphere servers) and are added to the SOA Web Services view and SOA UDDI view, as relevant.
	For information about the J2EE - WebSphere module, see "WebSphere Discovery" in the *HP Universal CMDB Discovery and Integration Content Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.
	For details on the SOA UDDI and SOA Web Services views, see "SOA Views and Their Components" on page 222.

Module (A - Z)	Description
Oracle iAS (Oracle Application Server) Module	The module discovers the Oracle Application Server.
	For details on discovering Oracle application servers, see "J2EE Discovery Wizard" in the *RTSM Data Flow Management Guide*.
Web Servers - IIS Module	The module discovers Web services and their WSDL files deployed on Microsoft IIS servers. The discovery process creates CIs for the discovered Web services, Web service operations, and configuration (WSDL) files. These CIs are added to the SOA Web Services view and SOA UDDI view, as relevant, and the Web service CIs are displayed in the IIS Topology view (with other components discovered on the IIS servers).
	For information about the Web Servers - IIS module, see "Microsoft Internet Information Services (IIS) Discovery" in the *HP Universal CMDB Discovery and Integration Content Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.
	For details on the SOA UDDI and SOA Web Services views, see "SOA Views and Their Components" on page 222.

✿ Integration of HP Diagnostics Data with SOA

Using BSM with HP Diagnostics, enables you to view, in BSM applications, end-to-end performance information for Web services that are monitored by HP Diagnostics. You can also directly access the HP Diagnostics application to view Web services reports.

The Web service information is collected by HP Diagnostics probes installed on the Web Server machine. The probes detect Web service traffic on the machine and identify Web service operations for the Web services. Part of the monitoring data, collected for each Web service operation, is stored in HP Diagnostics, while the rest of the data is stored in BSM.

HP Diagnostics sends the topology of Web services, which includes the Web service, its operations and also the monitors, to the RTSM, but does not send the WSDL files. The relevant assignments assign the HIs and KPIs appropriate for each CI in the topology.

The key attributes of a Web service are its target name space and service name. For information about the view, see "SOA Views and Their Components" on page 222.

For information about deploying the HP Diagnostics probes, and accessing the HP Diagnostics application from BSM, see the *HP Diagnostics User's Guide* (accessible from the BSM Help menu after registering the HP Diagnostics server).

Note: HP Diagnostics monitoring is supported for Web services based on SOAP over HTTP/S protocols.

Availability Calculation

The availability of a Web service/operation is calculated using the **error_count** field of the SOA Performance sample. Depending on the data source, the availability errors may include SOAP faults. The data sources fill in the **error_count** field according to the following table:

Data Source (Types of Samples)	Error_count Field (part of the SOA Performance sample)		REST Web Services
	SOAP Services		
	SOAP Faults	HTTP Errors	
BPM (performance and error samples)	ALL All errors generated by the Business Process Monitor are real errors.	ALL Reported as an error in the Performance sample.	None
SiteScope (performance sample)	ALL All errors generated by the SiteScope scripts are real errors.	ALL Reported as an error in the Performance sample.	None
Diagnostics (performance, event, and error samples)	Only configured SOAP faults The **Receiver** SOAP fault is considered as an error by default. The **VersionMismatch**, **MustUnderstand**, **DataEncoding**, and **UnknownSender** SOAP faults are not considered as errors for the Performance sample but are sent as events in the event sample. The payload capture information is stored only in Diagnostics.	None Diagnostics does not have the ability to recognize HTTP errors.	HTTP status code 5xx-6ss are considered as server side errors and are reported in **error_count** towards availability calculation

⚙ Integration of HP SOA Systinet

BSM can integrate with the HP SOA Systinet platform, enabling you to better manage and monitor your business services, and to understand the business impact of Web services. The integration also enables you to streamline the contracts information defined in HP SOA Systinet with your SLAs in BSM.

For details on enabling the integration, see "Enable HP SOA Systinet integration – optional" on page 200.

The integration with HP SOA Systinet provides the capabilities described in the following sections:

➤ **HP SOA Systinet service model is available in BSM**

You can run the Application - Web Services discovery pattern to discover the content of your HP SOA Systinet Registry, so that the HP SOA Systinet service model is available in BSM. For concept details, see "Discover UDDI Processes" in the *HP Universal CMDB Discovery and Integration Content Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.

➤ **You can use the drilldown links available in Service Health and Application Management for SOA, to open HP SOA Systinet directly at the page for the selected Web service**

HP SOA Systinet provides information on the Web service, such as the contracts on the service, policies and their compliancy, usage plans, and other general information. This information can be useful for solving problems and for understanding their impact on the business.

In Service Health, you can link to HP SOA Systinet to open the page for the selected Web service. For details on the link, see "Systinet Web Service Data" in *Using Service Health*.

> ➤ **In HP SOA Systinet, you can view service performance status (availability, performance, and so on) derived from BSM**

You can also link to the Health report in BSM for the selected service. This information can help consumers understand and evaluate service status.

For information about HP SOA Systinet, including service contracts and how to view service performance status derived from BSM, see the HP SOA Systinet documentation.

SiteScope Monitors for SOA

You deploy dedicated SiteScope monitors to collect Web service metrics and UDDI server health data. The collected data is used to calculate KPI values in the SOA views, and can be viewed in reports of the HP Business Service Management for SOA application.

The SiteScope monitors used to monitor your SOA environment are:

> ➤ **UDDI Monitor.** Used to perform a search in the UDDI Server. Each time the monitor is run, SiteScope checks if the UDDI Server can find any business entity. For details, see "UDDI Monitor Overview" in *Monitor Reference* in the SiteScope Help.

You can deploy this monitor using the Monitor Deployment Wizard. For details, see "Monitor Deployment Wizard Overview" in *Using System Availability Management*.

You can also deploy this monitor from System Availability Management. For details, see "How to Deploy a Monitor" in *Using SiteScope* in the SiteScope Help.

> ➤ **Web Service Monitor.** Used to check the availability of a Web service accepting Simple Object Access Protocol (SOAP) requests. The Web Service Monitor checks that the service can send a response to the client in a certain amount of time and verifies that the SOAP response is correct based on match specifications. For details, see "Web Service Monitor Overview" in *Monitor Reference* in the SiteScope Help. This monitor is used for Service Level Management rules.

You can deploy this monitor using the Monitor Deployment Wizard. For details, see "Monitor Deployment Wizard Overview" in *Using System Availability Management*.

You can also deploy this monitor from System Availability Management. For details, see "How to Deploy a Monitor" in *Using SiteScope* in the SiteScope Help.

➤ **Technology Web Service Integration Monitor.** Used to integrate Web service event data or metrics data from an existing EMS system with BSM. For details, see "Technology Web Service Integration Monitor" in *Monitor Reference* in the SiteScope Help.

You can also deploy this monitor only from System Availability Management. For details, see "How to Deploy a Monitor" in *Using SiteScope* in the SiteScope Help.

Tip: Application Management for SOA works only with metrics and not with events. To view SOA data in Business Service Management, you must configure the relevant SiteScope monitors (listed above), so that the monitors send metrics to Business Service Management.

Anti-Aging Enrichment

When you run a Web services script, the script checks the RTSM for the Web service CIs mentioned in the script. If the CI already exists, the script adds the **Monitored_by_BPM** attribute to existing **Operations CI.** If the CI does not exist, the BPM creates the **Web Service CI** -> **Operation CI** topology with a Monitored_by_BPM attribute.

In the RTSM, CIs that had no activity over a specified period of time are removed from the database by the aging mechanism. The **Operation CIs** are sent once to the RTSM by the BPM, are not refreshed over time, and are candidates for removal by the aging mechanism. If the **Operation CI** is erased from the RTSM, the **Web Service CI** is also automatically deleted by the aging mechanism.

The BPM_WS_ANTI_AGING TQL is run periodically in the RTSM to prevent the removal of those CIs. The TQL searches for the **Web Service CI -> Operations CI with Monitored_by_BPM** attribute subgraph. When it encounters the subgraph, it automatically postpones the deletion of those CIs.

In addition, when you erase the script from Monitor Administration, the **Monitored_by_BPM** attribute is erased from the Operations CIs in the RTSM, the **Web Service CI -> Operations CI** topology becomes incomplete and is therefore automatically deleted by the aging mechanism.

Tasks

❦ How to Monitor the SOA Environment

This section describes the processes used to monitor a SOA environment using Service Health and using Application Management for SOA reports.

Note:

➤ To discover all the Web Services attached to your network you must use Discovery and Dependency Mapping.

➤ When you are working with a large amount of Web Services, you must use Discovery and Dependency Mapping to discover the SOA architecture of your network.

➤ To Monitor Web Services without discovering them first, you do not need to perform Discovery and Dependency Mapping as the SiteScope and BPM monitors are able to build the CI topology and to transfer data directly from the WSDL files.

➤ When you know the Web Services WSDL files, you do not need to perform Discovery and Dependency Mapping because the SiteScope and BPM monitors are able to build the CI topology and to transfer data directly from the WSDL files.

➤ Diagnostics analyzes the calls and detects the Web Services, and uses that knowledge to build the CI topology and to transfer data to BSM.

This task includes the following steps:

➤ "Check that you have a valid license" on page 199
➤ "Perform Data Flow Management – optional" on page 199
➤ "Enable HP Diagnostics Integration and Deploy Diagnostics probes – optional" on page 200

➤ "Enable HP SOA Systinet integration – optional" on page 200

➤ "Deploy SiteScope monitors – optional" on page 200

➤ "Create Business Process Monitor applications – optional" on page 201

➤ "Customize how you monitor SOA in Service Health" on page 201

➤ "Enrich the SOA Model from scripts defined in Monitor Administration - optional" on page 201

➤ "Customize SOA reports – optional" on page 201

➤ "Set the appropriate access permissions for the reports" on page 202

➤ "View SOA information" on page 202

1 Check that you have a valid license

To view the Application Management for SOA application, you must have an Application Management for SOA license. For concept details, see "License Management Overview" in *Platform Administration*.

2 Perform Data Flow Management – optional

You can deploy the appropriate discovery patterns to discover the SOA architecture on your network. HP Business Service Management includes discovery patterns for monitoring your SOA environment. The discovery patterns are deployed from **Admin** > **RTSM Administration** > **Discovery** > **Job Configuration**.

➤ **UDDI Monitor.** Used to discover Web Services in the UDDI Server. Each time that the monitor is run, SiteScope checks if the UDDI Server can find a Web Service. For details, see "UDDI Monitor Overview" in *Monitor Reference* in the SiteScope Help.

➤ **Application Server.** Discover Web Services running on application server instances (IIS, Weblogic and others).

For information about running discovery, see "How to Use Discovery Control Panel – Basic Mode Workflow" in the *RTSM Data Flow Management Guide*.

For information about the SOA discovery modules, see "SOA Data Flow Management Modules" on page 188.

3 Enable HP Diagnostics Integration and Deploy Diagnostics probes – optional

To view metrics collected by HP Diagnostics probes installed on the Web server machines, register the Diagnostics server in BSM. For concept and task details, see "HP Diagnostics and HP Business Service Management Integration" on page 381.

Note: HP Diagnostics monitoring is supported for Web services based on SOAP over HTTP/S protocols.

---

4 Enable HP SOA Systinet integration – optional

If you are running HP SOA Systinet, you can integrate it with BSM to enable more unified management and monitoring of your business services, and to understand the business impact of Web services.

To enable the HP SOA Systinet and BSM integration, you must register the HP SOA Systinet server in BSM. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

a Select **Applications**.

b Select **BSM for SOA**.

c In the **BSM for SOA - Systinet Settings** table, locate **Systinet server host and port**. Define the host name and port, if required.

5 Deploy SiteScope monitors – optional

If you want dedicated SiteScope monitors to provide metrics on your SOA components, you must deploy the monitors. For task details, see "Deploy SiteScope SOA Monitors" on page 203.

6 Create Business Process Monitor applications – optional

If you want your SOA views to include performance metrics for running transactions on your Web servers, you must define the Business Process Monitor applications and transactions. For task details, see "Run BPM Transactions for SOA" on page 205.

7 Customize how you monitor SOA in Service Health

The relevant assignments assign the HIs and KPIs appropriate for each CI in the topology. To customize these assignments, select **Admin** > **Service Health** > **Assignments**. For details, see "How to Define a KPI or HI Assignment" in *Using Service Health*.

8 Enrich the SOA Model from scripts defined in Monitor Administration - optional

If required, you can enrich the SOA model using scripts that define Web Services. Those scripts are created in HP Virtual User Generator and run in Monitor Administration. For details, see "Enrich the SOA Model From Scripts" on page 207.

9 Customize SOA reports – optional

The Application Management for SOA reports enable you to view and analyze the health of Web services or operations access by proactively monitoring the availability, response time, and throughput of selected Web services or operations, to selected consumers or servers, as well as the number of calls, SOAP faults, and slow calls to selected Web services or operations, by selected consumers or servers.

You can customize SOA reports. For task details, see "How to Customize SOA Reports" on page 233.

10 Set the appropriate access permissions for the reports

The availability of report data for a specific user is dependent on:

➤ The application access permissions granted that user. For details on granting permissions, see "Permissions Tab (User Management)" in *Platform Administration*.

➤ The view permission, which determines the SOA reports permissions, because the reports are based on views (except for the Top Metrics Report). For details on granting permissions, see "Permissions Tab (User Management)" in *Platform Administration*.

➤ The views that are assigned to SOA. Only those views are available in the SOA reports. To add a view to the list of views available in the SOA reports, attach the view to the SOA bundle. To do that, click **Admin** > **RTSM Administration** > **Modeling** > **Modeling Studio**, select the view, click the **View Definition Properties** button 🖬 in **View Mode**, and select the SOA bundle in the **Bundle** box.

➤ The report filters specified by the administrator. Those filters limit access to specific data. For details, see "Active Filter Dialog Box" on page 235.

11 View SOA information

You can view SOA information in:

➤ Service Health. After your SOA monitoring environment is set up, you can view SOA monitoring data in Service Health, Service Level Management, and the Application Management for SOA application using views and reports. For details, see "How to View SOA Data in BSM" on page 231.

➤ Application Management for SOA reports. For details, see "SOA Views and Reports User Interface" on page 235.

🔧 **Deploy SiteScope SOA Monitors**

Note: Perform this task only when working with SiteScope 9.0.

This task is part of a higher level task. For details, see "How to Monitor the SOA Environment" on page 198.

You deploy dedicated SiteScope monitors to collect Web service metrics and UDDI server health data. The collected data is used to calculate KPI values in the SOA views, and can be viewed in reports of the HP Business Service Management for SOA application.

SiteScope monitors for SOA monitoring can be deployed from the Monitor Deployment Wizard, or from System Availability Management.

This task includes the following steps:

➤ "Use the Monitor Deployment wizard" on page 204

➤ "Manually attach SiteScope monitors" on page 205

Use the Monitor Deployment wizard

You can create and map SiteScope monitors directly on the SOA CIs created by the discovery process, using the Monitor Deployment Wizard. The SiteScope monitoring CIs generated by the SiteScope monitors are then deployed on the UDDI Registry and Web Service Operation CIs, creating a **Monitored By** relationship between them. For user interface details, see "Monitor Deployment Wizard" in *Using System Availability Management*.

Example:

1 Proceed as explained in "Monitor Deployment Wizard" in *Using System Availability Management*.

2 In the left pane of the Select Configuration Items to Monitor page, select the relevant SOA view. Select the CIs you would like monitored and move them to the right pane. You can map Web service operations to Web Service Monitors and UDDI Registry CIs to the UDDI Registry Monitors.

If the Web Service Operation CIs that you move to the right pane are already monitored, then they are displayed in italics with an **Already monitored** message.

3 Click **Next**. The Select Templates to Apply page opens. The left pane lists all the available templates in the wizard, including the Web Services Monitors and UDDI Monitors templates used for the SOA monitors, and the SiteScope templates for host if the hosts on which the Web services are deployed are also selected. Expand the template to see the monitors that are deployed by the template. The right pane lists the CI types (CITs) for the CIs selected in the previous page of the wizard. If you added Web Service Operation CIs to the right pane at the previous stage of the wizard, then the wizard automatically matches them with the Web Services Monitors template, and displays the Web Service Operation CIT in the right pane with the template attached.

4 Proceed with the wizard as indicated in "Monitor Deployment Wizard" in *Using System Availability Management*.

The added Web Service Monitor CIs are given default names as follows:
Synthetic Monitor On <name of relevant Web Service Operation CI>

Manually attach SiteScope monitors

If the monitors are deployed from System Availability Management, you must manually attach them to SOA discovery CIs. This is done in **Admin > RTSM Administration** > **Modeling** > **IT Universe Manager**. For concept details, see "Working with CIs" in the *Modeling Guide*.

For details on the SiteScope monitors used to monitor your SOA environment, see "SiteScope Monitors for SOA" on page 195.

🖈 Run BPM Transactions for SOA

You can deploy Business Process applications containing transaction monitors to actively monitor Web service performance. The transaction monitors run scripts that emulate Web service requests from end users, supplying end-to-end availability and response time metrics from varied and remote locations. The metrics are used for the BPM Transaction from Location CIs that are created in the RTSM.

You map the created business process monitoring CIs to the SOA CIs created by the discovery process, to produce an integrated SOA Web Services view.

Note: Business process monitoring data is not available in the Application Management for SOA application.

This task is part of a higher level task. For details, see "How to Monitor the SOA Environment" on page 198.

This task includes the following steps:

➤ "Create scripts in HP Virtual User Generator" on page 206
➤ "Define Business Process applications" on page 206
➤ "View Business Process Monitoring CIs in the views" on page 206

1 **Create scripts in HP Virtual User Generator**

Create scripts in HP Virtual User Generator that emulate the Web service requests. For details, see the *HP Virtual User Generator User's Guide*.

2 **Define Business Process applications**

Perform the following steps:

a Define Business Process applications in **Admin** > **End User Management** > **Monitors**, using the Business Process Monitor Application Configuration Wizard.

b Add to the applications, the relevant transaction monitors that run the HP Virtual User Generator scripts for Web service requests.

c Assign the applications to BPM machines/instances at the required locations.

For concept details, see "Business Process Monitor Administration" in *Using End User Management*.

3 **View Business Process Monitoring CIs in the views**

After BPM has run the scripts, the resulting BPM Transaction from Location CIs are added to the RTSM and displayed in the monitors views and the End Users views. For information about the hierarchy of these views, see "Setting the View Hierarchy" in the *Modeling Guide*.

To map the SOA CIs in the SOA Web Services view (discovered during the discovery process) to the relevant Business Process Step CIs and BPM Transaction from Location CIs, you must manually attach the business process monitoring CIs to the higher level CIs. This is done in **Admin** > **RTSM Administration** > **Modeling** > **IT Universe Manager**. For details, see "Attaching Existing CIs" in the *Modeling Guide*.

🦅 **Enrich the SOA Model From Scripts**

You can enrich the SOA model with scripts defined in the Monitor administration to create a relationship between Node CIs and Web Service CIs, and to view status changes for the Web Service CI when the status of the Node CI monitored by SiteScope changes.

This feature is supported for HP Virtual User Generator/Service Test 9.10, LoadRunner 9.10, and BPM 7.50 and higher.

BPM up to version 9.0. BPM sends SOA data via HTTP, using the BAC API. Web Data Entry (WDE) converts the data into two UDX samples: SOA Performance and SOA Event (errors are reported in this sample). The samples are sent according to the schedule.

BPM from version 9.0. BPM sends SOA data directly to BSM using the two UDX samples: SOA Performance and SOA Event (errors are reported in this sample). The samples are sent according to the schedule.

When BPM sends samples, the data is displayed in the Application Management for SOA Application under the **Synthetic** data type.

Limitations:

➤ To be supported, a Web Service script must have a WSDL version 1.1, and the WSDL file, which describes the Web Service and the Web Service operations, supplied with the script should use WSDL version 1.1.

➤ REST Web Services can be monitored by BPM, but SOA data reporting is not supported (they do not have a WSDL file); only regular errors are reported. SOAP_request calls are not supported because they do not have WSDL.

➤ HP Virtual User Generator/LoadRunner do not support Web Services protocols on Unix.

➤ Drilldown operations are not supported between SOA and End User Management reports.

This task is part of a higher level task. For details, see "How to Monitor the SOA Environment" on page 198.

This task includes the following steps:

➤ "Record a script in HP Virtual User Generator" on page 208

➤ "Create a BPM application" on page 209

➤ "Run the Web Service script" on page 209

1 Record a script in HP Virtual User Generator

You can define Web Services inside scripts in HP Virtual User Generator/ Service Test or LoadRunner. You can record Web Service calls with different operations. Each operation call is then reported as a different transaction. For details on defining scripts in HP Virtual User Generator, see HP Virtual User Generator documentation.

A Web Service script does not need to include user transactions to produce data. If more than one script uses the same CI, a single CI is created. A CI is deleted if none of the scripts use it.

For each SOA script, HP Virtual User Generator creates a file. The file is used by the End User Management administrator to add the relevant SOA CIs to the model (Web Service, Operation, and Monitor CIs). The file is generated or updated after each save/update operation is done using HP Virtual User Generator/Service Test. The file is included in the runtime files used for exporting to a zip file using HP Virtual User Generator.

Note: If you are using legacy scripts recorded with HP Virtual User Generator up to version 9.0, data reporting is supported by BPM, but you must add the SOA CIs to the model. To add the SOA CIs, download the script from CRS, open the script in HP Virtual User Generator 9.10 once and save the script (the script is saved in the new format), upload the new script version in CRS, and reload the script version in End User Management for relevant monitors.

For each Web service call, the following line is added to the file, regardless of the status of the Web service call:

<operation_name>; <web_service_name>; <target_namespace>; <wsdl_name/location>

where **<wsdl_name/location>** must locate the relevant WSDL if there is more than one WSDL.

An operation called more than once in the script is represented by one line in the file. The order of the operations in the script is not important.

WSDL files should be imported into the script.

If you override manually the endpoint (name of port) address in HP Virtual User Generator, the new address is reported to BPM.

BPM ignores the **Define each step as a transaction** option in HP Virtual User Generator settings.

The WSDL file and the Operations file are zipped together with other script files.

If more than one WSDL file is created for one Web Service script (set of hierarchic WSDL files), HP Virtual User Generator places them in one folder.

2 **Create a BPM application**

Create a new application and its BPM configuration in End User Management Administration. For details, see "Business Process Monitor Application Configuration Wizard" in *Using End User Management.*

3 **Run the Web Service script**

If you have set the SOA license, you are running the script in HP Virtual User Generator, and the operations file appears in the script, the **Enable SOA breakdown** option is automatically enabled in Monitor Administration, and the SOA Performance and SOA Events samples from the operation are reported to BSM.

BPM sets the **Define each step as a transaction option = true** when the script is a Web Service script.

BPM plays the script and reports SOA samples by wrapping each operation call within an automatic transaction. The automatic transaction is provided by LoadRunner. The automatic transactions are not displayed in Monitor Administration and are not counted in the licensed number of transactions for BPM.

BPM can distinguish between SOA faults and other faults (HTTP or other).

If the operation already exists (added to the RTSM by Discovery and Dependency Mapping), the relevant HIs and KPIs are assigned to the existing operations CIs. The SOA Monitor CI and the BPM Web Service Monitor CIs, as well as their performance and the event, are displayed in the SOA UDDI view in Service Health.

When you attach a Web Service script to an application, a CI is created. The CI status is changed to **No data** when the application is stopped, when you do not attach it to a monitor, or if the script is old.

The following topology is created in the RTSM: **Web Service CI** -> **Operations CI**. The topology is maintained by the anti-aging enrichment mechanism. For details, see "Anti-Aging Enrichment" on page 196.

BPM for SOA CIs are included in the model only when the RTSM includes the following information:

➤ **WS name**, **OP name**, and **target name space** CIs exist and the **enable field** value is **true** for these CIs.

➤ Each operation (add/remove/update script, version/change check box) in Monitor Administration updates this information.

🛠 How to Monitor SOA Environment in Service Health – Use-Case Scenarios

This section provides use-case scenarios that show how you can use the Application Management for SOA reports to find the source of problems.

Note: For a task related to this scenario, see "How to Monitor the SOA Environment" on page 198.

This section includes the following topics:

➤ "Availability Problem – Use-Case Scenario" on page 211

➤ "Performance Problem – Use-Case Scenario" on page 214

➤ "Throughput Problem – Use-Case Scenario" on page 217
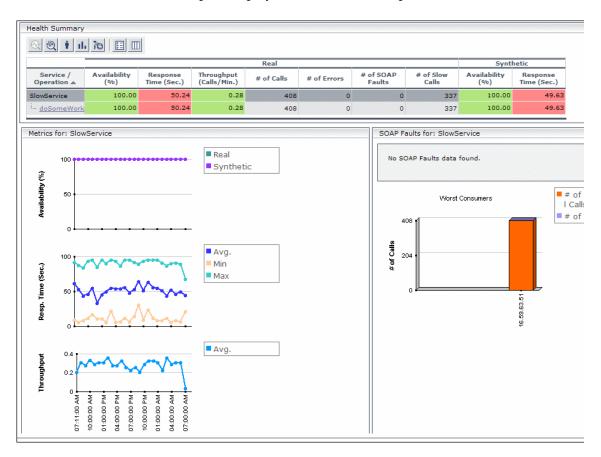
Availability Problem – Use-Case Scenario

The Service Health Console page displays, in the SOA Web Services view, a service availability problem. There is no problem with the system. The problem seems to be with the MedRecWebServices Web service.
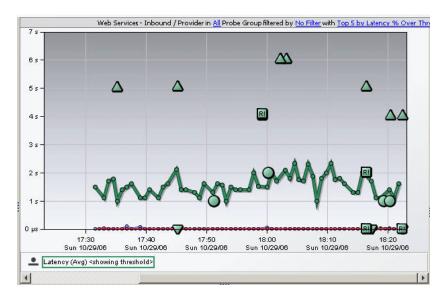
You want to drill down to the SOA Health report to understand where the problem is located. Click the down arrow to the right of the CI and select **Reports** > **Web Services Health**.

The Health Report displays the health of the operations.

A suspect operation is found. Select the appropriate operation and click the button to access Diagnostics for the selected operation.

Diagnostics displays the SOAP fault that caused the problem.

You can view the SOAP fault information to find the root cause of the problem. For details, see HP Diagnostics documentation.

Performance Problem – Use-Case Scenario

The Service Health Console page displays, in the SOA Web Services view, a service performance problem. There is no problem with the system. The problem seems to be with the SlowService Web service.
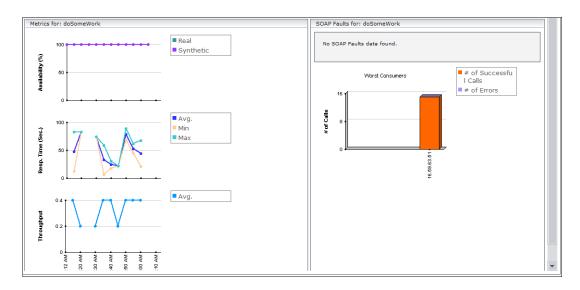
To drill down to the SOA Health report, click the down arrow to the right of the CI in the Console page, and select **Reports** > **Web Services Health**.

The Health Report opens.

A suspect operation is found. Click the appropriate operation.
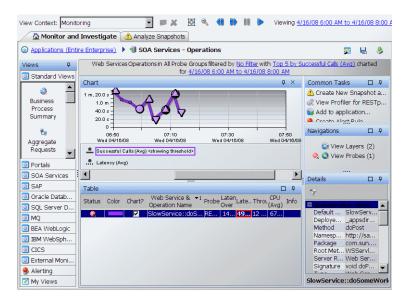
The Health report for the relevant operation opens. Scroll down and view the graphs.
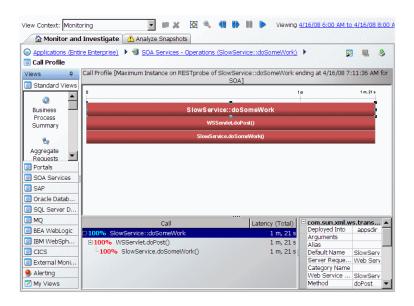
The **Throughput** graph does not indicate service overload.
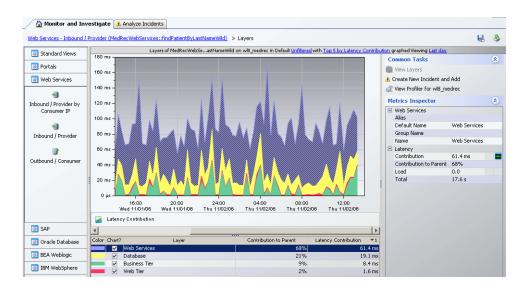
Select the operation and click the **Drill down to Diagnostics Operations View** button to drill down to Diagnostics.

In Diagnostics, you can drill down from each instance to its call profile.

You can then view the layers breakdown of the Web Service operations and find out how much time was spent in each layer (Web Service, database, and so on). For details, see HP Diagnostics documentation.
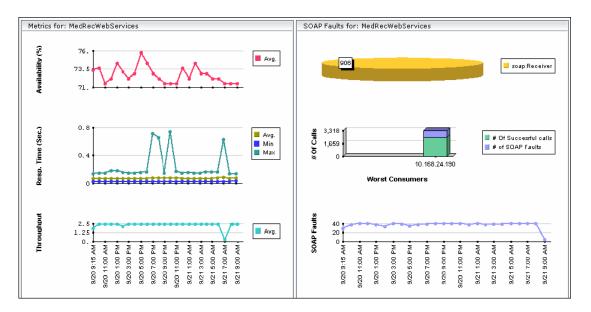
Throughput Problem – Use-Case Scenario

The Service Health Console page displays, in the SOA Web Services view, a service performance problem. There is no problem with the system. The problem seems to be with the MedRecWebServices Web service.

To drill down to the SOA Health report, click the down arrow to the right of the CI in the Console page, and select **Reports** > **Web Services Health**.

A problematic operation (addRecord) is found. Both the response time and throughput of the operation indicate a problem. A suspected reason for the response time would be an overloaded service. You can view the correlation between the response time and the throughput in the Metrics section.

After you assess that the reason is a throughput problem, you can drill down and find the consumers that overload the service.

🔍 Troubleshooting and Limitations

This section describes troubleshooting and limitations for Application Management for SOA.

➤ **The SOA reports reflect the relative view of the user.** Therefore, if in a customized view, specific operations are attached to a Web service, the SOA reports based on the view display information related only to the Web service and the selected operations. Other operations connected to the Web service in the RTSM are not displayed.

In addition, the SOA reports, except for the Top Metrics report, do not work if, when working with customized views, you do not check that the Web services and operations are attached to each other.

➤ **Monitors not added to customized views.** If the monitors attached to the operations are not added to the customized view, the SOA reports display information that does not take into consideration the thresholds defined in the monitors.

6

HP Business Service Management for SOA Views and Reports

This chapter includes:

Concepts

➤ SOA Views and Their Components on page 222

➤ Application Management for SOA Reports on page 229

Tasks

➤ How to View SOA Data in BSM on page 231

➤ How to Customize SOA Reports on page 233

Reference

➤ SOA Views and Reports User Interface on page 235

Concepts

☘ SOA Views and Their Components

The SOA views include Web services performance, availability, and throughput (load on the Web service) information. The information is collected by SiteScope, BPM, and Diagnostics. They monitor traffic to selected Web services, operations, endpoints, or servers. The data enables you to analyze the detected performance issues, and helps you to identify the cause of delays. In addition, the views display information about the system status impacting the Web service, as well as change information.

In the RTSM Administration, a Web service discovered on an application server (WebLogic, WebSphere, Oracle Application Server, or IIS) has a relationship with the application server host (the host is a child of the Web service). For example, when you monitor the host's CPU, the Node CI is assigned a System KPI that propagates to the Web service CI. This relationship helps to triage Web service problems, when the Web service has a performance/availability problem due to a system issue.

This section also includes the following topics:

➤ "CIs Discovered by the Discovery Process" on page 222

➤ "SOA Views in Service Health" on page 223

➤ "SOA Topology Discovered by SiteScope" on page 228

➤ "Accessing Other Information" on page 228

CIs Discovered by the Discovery Process

The following CIs are discovered by the SOA discovery processes. For details, see "SOA Data Flow Management Modules" on page 188.

The default KPIs are described in "List of Service Health KPIs" in *Using Service Health*.

The CIs discovered by the discovery process are:

CI Name	Icon	Description
UDDI Registry		The UDDI Registry CIs represent the UDDI registries that were discovered in your network.
Business Unit		The Business Unit CIs represent the service providers discovered in your network.
Web Service Monitor		The Web Service Monitor CIs represent the Web services monitors discovered in your network.
Web Services		The Web Services CIs represent the Web services discovered in your network.
Web Service Operation		The Web Service Operation CIs represent the operations discovered in your network.
Configuration File		The Configuration File CIs represent the URLs of the WSDL pages used by the Web service. Changes to Configuration Files can be displayed in the Change report. For user interface details, see "CI Change Report Page" in *Reports*.

SOA Views in Service Health
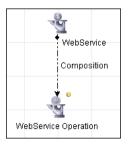
HP Business Service Management for SOA displays information about the performance, availability, and throughput of the UDDI registry, Web services, operations, SiteScope monitors, SiteScope Web services monitors, and nested WSDLs in the following views:

➤ **SOA Monitored Web Services View**

Includes all of the Web services discovered by Discovery and Dependency Mapping or created by SiteScope, BPM or HP Diagnostics that are stored in the RTSM and are currently monitored.
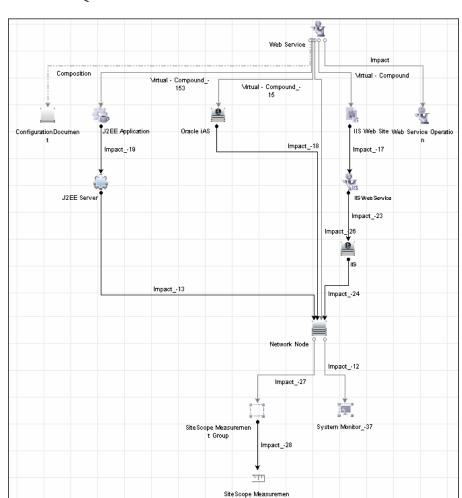
The TQL for the view is built as follows:

➤ **SOA Web Service View**

Includes all of the Web services that were discovered and stored in the RTSM.
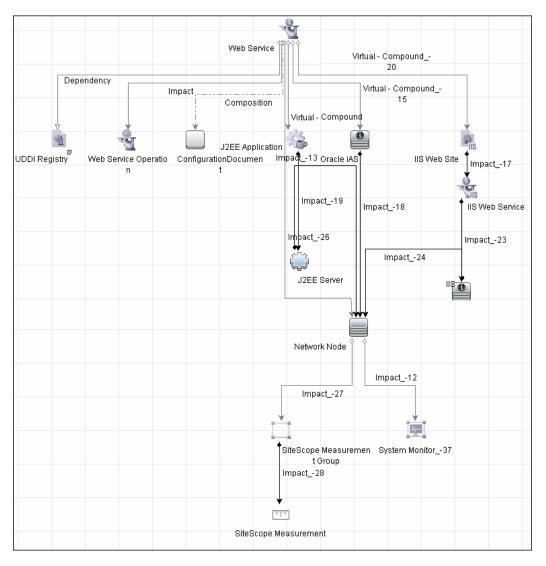
The TQL for the view is built as follows:

➤ **SOA Rogue Services View**

Includes all of the Web services that were discovered and stored in the RTSM and that are not registered in the UDDI registry. They also appear in the SOA Web Services View.

The TQL for the view is built as follows:
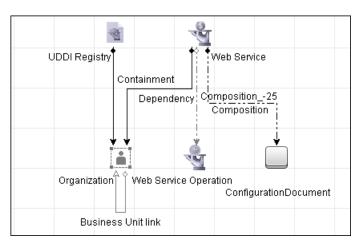
➤ **The SOA UDDI View**

The SOA UDDI view represents information obtained by running the Application - Web Services discovery process. The view includes the UDDI registries, all the Web services discovered from the registries, their operations, and WSDL. The Web service providers (represented by the business unit) are also discovered and related to their respective Web services.
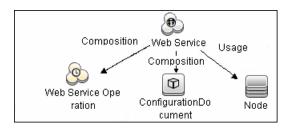
Note: Nested WSDL files are mapped to Configuration File CIs. For details, see "View Configuration File CI details" on page 231.

The TQL for the view is built as follows:

SOA Topology Discovered by SiteScope

The SOA UDDI view also includes the following topology, which is created for the SiteScope Web Service monitor.

Note: The SiteScope Web Service Monitor CI replaces the legacy SiteScope Monitor CI for the Web Service monitor instances when upgrading from previous versions of SiteScope to SiteScope 9.50. During the upgrade, the SiteScope Monitor CI is removed from the RTSM. The removal causes the CI to also be removed automatically from pattern, perspective, or template views where it was included or from SLAs to which it was attached.

Accessing Other Information

From the SOA views you can:

➤ Drilldown to the Application Management for SOA reports that present detailed metrics information about the performance, availability, and throughput over time of the selected CI. The reports also display the total number of calls, the number of calls that are slow or end with a SOAP fault, the least available Web services/operations, the slowest Web services/operations, consumer information, server information, and so on. For details on the reports, see "SOA Views and Reports User Interface" on page 235.

➤ Use the shortcut menus to access additional information; for example to access the HP Diagnostics application. For details, see "Service Health Menu Options" in *Using Service Health*.

➤ Access User reports. User reports provide a list of all of the custom reports, trend reports, and custom links that have been defined in the system, that the current user has permissions to view. You can display the reports in Excel format, create custom reports, trend reports, and so on. For details, see "Report Manager Overview" in *Reports*.

Application Management for SOA Reports

The Application Management for SOA reports enable you to view and analyze the health of Web services or operations access by proactively monitoring:

➤ The availability, response time, and throughput of selected Web services or operations, to selected consumers or servers.

➤ The number of calls, SOAP faults, and slow calls to selected Web services or operations, by selected consumers or servers.

For details on working with HP Business Service Management reports, see "CI Status Reports User Interface" in *Reports*.

Application Management for SOA Reports

The Application Management for SOA tab includes the following reports:

➤ **Health report.** Displays health metrics for the selected Web services, operations, consumers, or endpoints in a selected view. For details, see "Health Report" on page 246.

➤ **Top Metrics report.** Displays the top metrics information about the traffic to and from all of the monitored Web services or operations. For details, see "Top Metrics Report" on page 279.

➤ **Metric Analysis report.** Displays the performance of a metric, over time, by measuring access to selected Web services or operations, by an endpoint, or a consumer. You can group the data by server, consumer, or endpoint. For details, see "Metric Analysis Report" on page 259.

➤ **Metrics Over Time report.** Displays the performance of multiple metrics, over time, by measuring access to selected Web services or operations, by an endpoint, or a consumer. For details, see "Metrics Over Time Report" on page 266.

➤ **Consumer Summary report.** Displays specific metrics for all of the consumers accessing the selected Web services or operations in a selected view. For details, see "Consumer Summary Report" on page 240.

➤ **Server and Endpoint Summary report.** Displays a drillable summary of the metrics for all of the servers on which the selected Web services or operations of a selected view are running. For details, see "Server and Endpoint Summary Report" on page 272.

➤ **Metric Analysis report.** Displays the performance of a single metric related to a selected view and selected CIs, over time. For details, see "Metric Analysis Report" on page 259.

Tasks

⚒ How to View SOA Data in BSM

This section describes how to view SOA in Service Health.

This task includes the following steps:

1 View SOA information in BSM

After your SOA monitoring environment is set up, you can view SOA monitoring data in relevant views in Service Health, in Service Level Management, and the Application Management for SOA application using views and reports. For details, see "SOA Views and Their Components" on page 222.

2 View Configuration File CI details

Right-click a Configuration File CI in the SOA UDDI View, select **Properties**, and click **Show document content** to display the contents of the configuration file that includes the contents of the WSDL page corresponding to the URL.

Note: Nested WSDL files are mapped to the Configuration File CIs.

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2005 U (http://www.xmlspy.com) by mrkef (mrkef) -->
<wsdl:definitions xmlns:impl="http://company.com/accountsvc/account"
xmlns:intf="http://company.com/accountsvc/account" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
targetNamespace="http://company.com/accountsvc/account">
          <wsdl:types>
                    <schema elementFormDefault="qualified"
targetNamespace="http://company.com/accountsvc/account"
xmlns="http://www.w3.org/2001/XMLSchema">
                              <element name="getAccount">
                                        <complexType>
                                                  <sequence/>
                                        </complexType>
                              </element>
                              <element name="getAccountResponse">
                                        <complexType>
                                                  <sequence/>
```

Nested WSDL appear in Model Explorer as a list of Configuration File CIs under the main Configuration File CI. For example:

```
http://<server_name>/uddi/doc/wsdl/account.wsdl
http://<server_name>/uddi/doc/wsdl/account_binding.wsdl
http://<server_name>/uddi/doc/wsdl/account_portType.wsdl
```

For user interface details about Model Explorer, see "View Selector" in *Using Service Health*.

3 View changes made to SOA CIs

Changes made to the properties of all types of CIs and functional changes of the Web services are discovered by different types of discoveries. The CI properties can be: changes of the SOA infrastructure: hosts, application servers, and so on. Functional changes of the Web services can be changes to WSDL; for example if a new parameter or a new operation were added or if an operation was removed. Both types of changes are displayed in the Change report available as a shortcut menu option for each one of the relevant CI types.

For details on the Change report, see "CI Change Report Page" in *Reports*.

For details on the Application - Web Services, WebSphere, WebLogic, and IIS discoveries, see the *HP Universal CMDB Discovery and Integration Content Guide*. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.

4 **View SOA Reports**

The Application Management for SOA reports enable you to view and analyze the health of Web services or operations. For details, see "Application Management for SOA Reports" on page 229.

🦴 **How to Customize SOA Reports**

Note: All the steps in the task are optional and can be performed in any order.

The following steps describe how you can customize SOA reports.

➤ "Customize the number of web services or operations displayed in the SOA reports" on page 234

➤ "Customize the number of elements displayed in the Top Metrics Reports" on page 234

Customize the number of web services or operations displayed in the SOA reports

You can customize the number of Web services or operations that can be displayed in a SOA report. The default value is 20.

To customize the number of Web services or operations that can be displayed in a SOA report, select the **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** page:

➤ Select **Applications**.

➤ Select **BAC for SOA**.

➤ In the **BAC for SOA - General Settings** table, locate **Max. number of selectable CIs in SOA reports**. Change the value as required.

Customize the number of elements displayed in the Top Metrics Reports

You can customize the number of elements that can be displayed in a Top Metrics report. The default value is 5.

To customize the number of elements that can be displayed in a Top Metrics report, select the **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** page:

➤ Select **Applications**.

➤ Select **BAC for SOA**.

➤ In the **BAC for SOA - General Settings** table, locate **Top Metrics Size**. Change the value as required.

Reference

🔖 SOA Views and Reports User Interface

This section describes:

🔖 Active Filter Dialog Box

This dialog box enables you to filter SOA reports.

To access	In the Health, Top Metrics, Metrics Over Time, Consumer Summary, or Server and Endpoint Summary reports, click **Active Filters**.
Important information	The Active Filter dialog box may display one or more tabs depending on the report where you clicked **Active Filters**. You can select items from each tab to create more complex filters.

Web Service/Operations Tab

User interface elements are described below:

UI Element (A-Z)	Description
Number of Selected Operations	Indicates the number of Operation CIs that you have selected.
Number of Selected Web Services	Indicates the number of Web Service CI that you have selected.
Search	Click the **Search** link to search for a specific CI in the current view or in all views.
Selected CIs	Select one of the following: ➤ **Web Services.** Displays a check box only for the Web services CIs appearing in the view. ➤ **Operations.** Displays a check box only for the operation CIs appearing in the view. You can select up to 20 Web services or operations. You can modify that limit in the Infrastructure Settings. For details, see "Customize the number of web services or operations displayed in the SOA reports" on page 234.
View	Select the appropriate view and select the relevant CIs in the view. Only views for which the user has permission and that have been assigned to SOA are displayed in the list. For additional information on the available views, see "SOA Views in Service Health" on page 223.

Metrics Tab

Important information	The Metrics tab is displayed when you click **Active Filter** in the Metrics Over Time report.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Metrics>	Select the metrics you want to display in the report.

Endpoint/Consumer Tab

Important information	You can enter, separated by semi-colons (;), up to three Server IPs, Endpoints, or Consumers in the fields of the Endpoint/Consumer tab.
	You can use the following format: <string>* in the Consumer field to display all the consumers whose names start with the string.

User interface elements are described below:

UI Element (A-Z)	Description
Consumer	You can filter by consumer information, for consumers registered in HP Diagnostics, by entering one of the following: ➤ The consumer ID (it can be an IP address, an IP range, an HTTP header, or a payload in SOAP requests). ➤ The consumer subunit name, which is the name of the IP range where the customer is located. ➤ The consumer details taken from the payload; for example Web Service http custom header value or Web service SOAP payload value (soap-header/soap-envelope/soap-body). ➤ **Other** to search for all non-registered consumers that access the server or endpoint listed in the Server IP or End Point box. The consumer information can be any string, up to 100 characters, including wildcards. **Note:** ➤ Use a semi-colon (;) to separate the values in the fields. ➤ Do not enter more than 3 values can be selected in each field. ➤ Use **<string>*** to display all the consumers whose names start with the string. **Note:** For performance reasons, the wildcard can be located only on the right most side on the string. For details, see the *HP Diagnostics Installation and Configuration Guide*.

UI Element (A-Z)	Description
Endpoint	Enter the monitored endpoint. The value depends on the data source.
	For HP Diagnostics, it is the application server instance name (defined in HP Diagnostics).
	For BPM and SiteScope, it is the port name/endpoint (depending on the WSDL version) that the user select from the WSDL when creating the script/monitor.
	Note:
	➤ Use a semi-colon (;) to separate the values in the fields.
	➤ Do not enter more than 3 values can be selected in each field.
Server IP	Enter the server IP address to display information about the consumers accessing specific servers.
	You can also use a wildcard (*****) as the end of the string.
	Note:
	➤ Use a semi-colon (;) to separate the values in the fields.
	➤ Do not enter more than 3 values can be selected in each field.

Views

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Views>	Select a view.
	The View box lists the views you are permitted to display.
	This dialog box is displayed when you click **Active Filters** in the Top Metrics report.

✨ Consumer Summary Report

This report displays specific metrics for all of the consumers accessing the selected Web services or operations in a selected view.

To access	**Application > Application Management for SOA**, click the **Application Management for SOA** tab, and select the **Consumer Summary Report** option.
Important information	When you select **Real**, the Consumer Summary Report displays information only for the consumers that were registered in the Diagnostics system. All other consumers are aggregated and presented as **Others**. **Note:** You can add this report as a component in MyBSM. For details, see "EUM High-Level Status Page" in *Using MyBSM*.
Relevant tasks	"How to View SOA Data in BSM" on page 231

Report Settings

UI Element (A-Z)	Description
<Common report elements>	For details, see "Common Report and Page Elements" in *Reports*.

UI Element (A-Z)	Description
Active Filter	If relevant, click the **Active Filter** link to select the appropriate conditions for the report. For details, see "Active Filter Dialog Box" on page 235.
Real/Synthetic	Select one of the following: ➤ **Real.** To display data from the Diagnostics data collector. ➤ **Synthetic.** To display data from the SiteScope and Business Process monitors. **Note:** ➤ When you generate a SOA report, the **Data Type** selection is displayed in the top part of the report. ➤ When SiteScope or BPM monitors a web service operation that is monitored by HP Diagnostics, Business Service Management receives data from both HP Diagnostics (as real user data) and from SiteScope/BPM (as synthetic user data) describing the same web service operation. This is because HP Diagnostics has no way of knowing if the data was generated by real user or by synthetic user, it simply collects the data for all hits performed on the web service operation it monitors.

Consumer Summary Area

This area displays the health metrics for all of the consumers accessing the selected Web services or operations. If, in the Active Filters, you also select specific consumer, endpoint, or server, the health metrics are further filtered by these selections.

The following is an example of the Consumer Summary area.

Consumer ▲	Availability (%)	Response Time (Sec.)	Throughput	# of Calls	# of Errors	# of SOAP Faults	# of Slow Calls
16.59.44.183	60.00	0.04	236.12	340,013	136,004	136,004	0
Other	59.96	0.07	2.21	3,177	1,272	1,272	0

Important information	The Consumer Summary area is the same in the View as Graph and View as Table tabs.
See also	"Availability Calculation" on page 193

User interface elements are described below:

UI Element (A-Z)	Description
	Drills down to the Health Report for the selected element. For details, see "Health Report" on page 246.
# of Calls	The total number of calls accessed by the specific consumer.
# of Errors	The total number of failed calls by the specific consumer. A failed call is a call that was not performed due to the unavailability of the Web services or operations. **Configurable:** The SOAP faults affecting the availability can be configured in HP Diagnostics when the call is monitored by HP Diagnostics.
# of Slow Calls	The number of slow calls by the specific consumer. A slow call is a call with a response time longer than the predefined threshold. **Note:** The value displayed by **# of Slow Calls** is different from the value of the **Total Threshold Violation** in HP Diagnostics. In HP Diagnostics the **Total Threshold Violation** includes the overall number of violation from all the calls and in BSM **# of Slow Calls** includes only the violations of the successful calls.
# of SOAP Faults	The total number of SOAP faults that occurred in calls by the specific consumer.

UI Element (A-Z)	Description
Availability	The availability of the selected Web services or operations accessed by the specific consumer. The availability is calculated as the number of successful calls made by the specific consumer divided by the total number of calls made by the specific consumer, multiplied by 100. The background is colored according to the comparison between the Web service worst availability and the threshold specified in the Availability KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.
Consumer	The consumer information. For details on the different consumer details, see the Consumer description in the End Point/Consumer Tab in "Active Filter Dialog Box" on page 235. Click the consumer name to drill down to the Health Report for the selected element. For details, see "Health Report" on page 246.
Response Time (sec.)	The average response time (in seconds) of the selected Web services or operations accessed by the specific consumer. The background is colored according to the comparison between the Web service worst response time and the threshold specified in the Response Time KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.
Throughput (calls per min.)	The number of calls, per minute by the specific consumer. The background is colored according to the comparison between the Web service worst throughput and the threshold specified in the Throughput KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.

Worst Consumer Area

This area displays the successful and faulty calls of the worst five consumers accessing the selected Web services, operations, or servers.

The following is an example of the Worst Consumer area.

Important information	The Worst Consumer displays the same information in the View as Graph and View as Table tabs.
	Each tab in the graph represents a different consumer and displays the number of successful calls (in green) and the number of failed calls (in purple).
	Move the pointer over a tab in the graph to display a tooltip that indicates the consumer, the number of errors, successful calls, SOAP faults, and the number of successful calls.
	The X-axis displays the consumer information while the Y-axis displays the number of calls.

User interface elements are described below:

UI Element (A-Z)	Description
# of Calls	The total number of calls accessed by the specific consumer.
# of Errors	The total number of failed calls by the specific consumer. A failed call is a call that was not performed due to the unavailability of the Web services or operations.
	Configurable: The SOAP faults affecting the availability can be configured in HP Diagnostics when the call is monitored by HP Diagnostics.
# of SOAP Faults	The total number of SOAP faults that occurred in calls by the specific consumer.
# of Successful calls	The number of successful consumer calls.
<Drilldown>	Click a bar to access the Health report filtered for the consumer.
Consumer	The consumer information. For details on the different consumer details, see "Active Filter Dialog Box" on page 235.
	Click the consumer name to drill down to the Health Report for the selected element. For details, see "Health Report" on page 246.

Health Report

This report displays health metrics for the selected Web services, operations, server, endpoint, or consumer in a selected view.

To access	Use one of the following:
	➤ **Applications** > **Service Health**, select a view in Model Explorer:
	➤ In Model Explorer, right-click a specific Web Service or Operation CI, and select the **Reports** > **Health Report** option. The Health Report is filtered by the specific Web service or operation. For details, see "360° View" in *Using Service Health*.
	➤ In Service Health, in the **360°** tab, right-click a specific Web Service or Operation CI, and select **Reports** > **Health Report**. The Health Report is filtered by the specific Web service or operation. For details, see "360° View" in *Using Service Health*.
	➤ **Applications** > **Application Management for SOA**, and select the **Health Report** option.

Important information	To enable you to find all available Web Services/operations, the Health report automatically shows all selected Web Services/operations even when they do not have data. You can also check if the Web Service/operation has only **Synthetic** data or no data at all (**Real** or **Synthetic**) and decide to remove the Web Service/operation from the list in the filter.
	Note:
	➤ You must configure the REST Web Services in the HP Diagnostics application. After configured, their topology is sent by HP Diagnostics to the RTSM. REST Web Services are not SOAP Web Services, therefore they provide errors and not SOAP faults. Consequently, the Health report does not display REST Web Services in the report areas that display SOAP faults. The Health report displays how many requests were made to the URL corresponding to the REST Web Service and how many of those requests failed.
	➤ You can add this report as a component in MyBSM. For details, see "EUM High-Level Status Page" in *Using MyBSM*.
Relevant tasks	"How to View SOA Data in BSM" on page 231
See also	"Availability Calculation" on page 193

Report Settings

UI Element (A-Z)	Description
<Common report elements>	For details, see "Common Report and Page Elements" in *Reports*.
Active Filter	If relevant, click to select the appropriate conditions for the report. For details, see "Active Filter Dialog Box" on page 235.
Real/Synthetic	Select one of the following: ➤ **Real.** To display data from the Diagnostics data collector. ➤ **Synthetic.** To display data from the SiteScope and Business Process monitors. **Note:** When you generate a SOA report, the **Data Type** selection is displayed in the top part of the report. When you select **Real**, each level of the report (except for **Endpoint**) also displays data for **Synthetic**. When you select **Synthetic**, the report displays only information relevant to **Synthetic**.
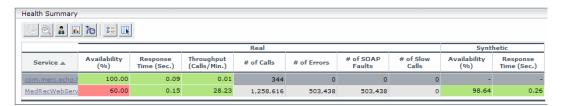
Health Summary Area

Depending on the selection you made in the Active filter, the Health summary area can display:
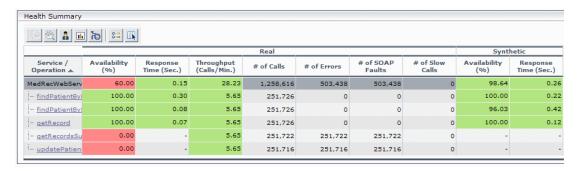
➤ A list of same level items (Web services, operations, endpoints, consumers).

➤ A tree (Web service/Operations, Operation/Endpoints, Endpoints).

To display other metrics information, click the required item. See the bullets above for details.

When you select more than one service in the Active Filter, the report displays the following data:

Health Summary

Service ▲	Real							Synthetic	
	Availability (%)	Response Time (Sec.)	Throughput (Calls/Min.)	# of Calls	# of Errors	# of SOAP Faults	# of Slow Calls	Availability (%)	Response Time (Sec.)
com.merc.echo.	100.00	0.09	0.01	344	0	0	0	-	-
MedRecWebServ	60.00	0.15	28.23	1,258,616	503,438	503,438	0	98.64	0.26

When you select one service in the Active Filter, the report displays the following data:

Health Summary

Service / Operation ▲	Real							Synthetic	
	Availability (%)	Response Time (Sec.)	Throughput (Calls/Min.)	# of Calls	# of Errors	# of SOAP Faults	# of Slow Calls	Availability (%)	Response Time (Sec.)
MedRecWebServ	60.00	0.15	28.23	1,258,616	503,438	503,438	0	98.64	0.26
findPatientByI	100.00	0.30	5.65	251,726	0	0	0	100.00	0.22
findPatientBy:	100.00	0.08	5.65	251,726	0	0	0	96.03	0.42
getRecord	100.00	0.07	5.65	251,726	0	0	0	100.00	0.12
getRecordsSu	0.00	-	5.65	251,722	251,722	251,722	0	-	-
updatePatien	0.00	-	5.65	251,716	251,716	251,716	0	-	-

Important information	The Health Summary area is the same in the View as Graph and View as Table tabs.
	Click the required element in the Health Summary report to access details on the health of the element's components. For details on the elements' components, see "Health Summary Area" on page 248.
	Use the breadcrumbs to retreat to the levels from which you drilled down.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
	Drilldown to Consumers Summary report. Opens the Consumer Summary report for the selected element. For details, see "Consumer Summary Report" on page 240.
	Drilldown to Metrics Over Time report. Opens the Metrics Over Time report for the selected element. For details, see "Metrics Over Time Report" on page 266.
	Note: This drilldown (**Diagnostics Operations**) is available only for non-Web Service CIs. **Drilldown to Diagnostics Operations view.** Opens the Diagnostics report relevant for the CI you selected in the table (for example the Diagnostics Operations view for an Operation CI) for the selected element. For details, see the *HP Diagnostics User's Guide*.

UI Element (A-Z)	Description
	Note: This drilldown (**Diagnostics Web Service Topology**) is available only for Web Service CIs. **Drilldown to Diagnostics Web Service Topology View**Opens the Diagnostics Service Topology view for the selected Web Service CI. The graph displays the real-time connections that exist between the selected Web Service CI and other Web Service CIs, for the same timeframe as the report. For details, see the *HP Diagnostics User's Guide*.
	Opens the HP SOA Systinet application, focused on the relevant Web service. This option is relevant only when there is an integration between BSM and HP SOA Systinet. For details on the integration with HP SOA Systinet, see "Integration of HP SOA Systinet" on page 194.
<Real> # of Calls	The total of calls to the specific item. This is a metric taken from the Diagnostics sample.
<Real> # of Errors	The total number of failed calls based on the data from the Diagnostics data collector. A failed call is a call that was not performed due to availability problems of the Web services operations. It can be a receiver SOAP fault or an HTTP status code of 5xx-6xx if the call is to a REST service. Note that not all REST services use HTTP status code to indicate failure.

UI Element (A-Z)	Description
\<Real\> # of SOAP Faults	The total number of SOAP faults that occurred in calls by the specific consumer based on the data from the Diagnostics data collector.
\<Real\> Availability	The availability of the item based on the data from the Diagnostics data collector. The background is colored according to the thresholds specified in the Availability KPI definition. The availability is calculated as the number of successful calls to the item, divided by the total number of calls to the item, and multiplied by 100.
\<Real\> Throughput (Calls/Min.)	The number of calls to the item per minute based on the data from the Diagnostics data collector. The background is colored according to the thresholds specified in the Throughput KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.
\<Real\> Response Time (sec.)	The response time (in seconds) of the item based on the data from the Diagnostics data collector. The background is colored according to the thresholds specified in the Response Time KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.
\<Synthetic\> Availability (%)	The availability of the item based on the data from the SiteScope or Business Process monitors. The background is colored according to the thresholds specified in the Availability KPI definition. The availability is calculated as the number of successful calls to the item, divided by the total number of calls to the item, and multiplied by 100. **Note:** If you monitor the same Web Service with both SiteScope and BPM (not recommended), the threshold defined in BPM is used to color the background.

UI Element (A-Z)	Description
<Synthetic> Response Time (sec.)	The response time (in seconds) of the item based on the data from the SiteScope or Business Process monitors. The background is colored according to the thresholds specified in the Response Time KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.
Namespace	The namespace of the Web service.
Service Operation Service/Operations Operation/Endpoint Endpoint	The name of the item whose health metrics are provided in the Health Summary. Click the required element to access details on the health of the element's components.
Web Service	The Web service.

Metrics Area

The Metrics area displays metrics information for the item listed in the first row of the Health Summary area. If multiple items were selected in the Active Filters, the Errors area displays the average information for all of the selected items.

Important information	You can drill down from each point in the graphs to display more detailed information about the period of time represented by that point. You can drill down to the smallest unit of time (1 hour).

Graph Format

User interface elements are described below:

UI Element (A-Z)	Description
Availability (%)	The graph displays the availability of the item over the selected time frame of the report in graph format. It displays both real and synthetic data when the **Real** Data Type is selected, or only synthetic data when the **Synthetic** Data Type is selected. The legend indicates what is displayed. **Note:** The Availability of a service in a **Real** data source does not always display the reality. For example, if the server is down, the calls do not get to the Web service, the Availability of a service in a **Real** data source indicates that no one called the Web service while the Availability of a service under **Synthetic** data source indicates that the situation is bad.
Response Time (sec)	The graph displays the response time (in seconds) of the item over the selected time frame of the report in graph format. The Response Time graph displays information about the **Average Response Time (sec.)** (purple line), the **Max Response Time (sec.)** (turquoise line), and the **Min Response Time (sec.)** (orange line).

UI Element (A-Z)	Description
Throughput	The graph displays the number of calls to the item per minute, over the selected time frame of the report in graph format. The title line of the Metrics area includes the name of the item whose metrics are displayed. If the Health Summary area displays a tree of Operation/Servers the title line of the Metrics area is **Aggregated data for selected operations**.

Table Format

User interface elements are described below:

UI Element (A-Z)	Description
# of Calls	The total number of calls to the item, per time unit.
# of Errors	The total number of calls to the item, that failed due to availability problems of the item, per time unit. **Configurable:** The SOAP faults affecting the availability can be configured in HP Diagnostics when the call is monitored by HP Diagnostics.
# of SOAP Faults	The total number of calls to the item, that failed due to a SOAP fault, per time unit.
Availability (%)	The availability of the item, based on the data from the Diagnostics data collector, per time unit.
Max Response Time (sec.)	The highest response time (in seconds) of the item, per time unit.
Min Response Time (sec.)	The lowest response time (in seconds) of the item, per time unit.
Response Time (sec.)	The response time (in seconds) of the item, per time unit.
Synthetic Availability (%)	The availability of the item, based on the data from the SiteScope monitors, per time unit.
Throughput (Calls/ Min)	The number of calls to the item per minute of the time unit.
Time	The time units (hour) of the selected time period.

Errors Area

The Errors area displays information for the item listed in the first row of the Health Summary area. If multiple items were selected in the Active Filters, the Errors area displays average information for all of the selected items.

Important information	➤ If you have selected to display synthetic data, the Errors area displays only the **Worst Consumers** graph.
	➤ If you have selected to display real data, the Errors area displays all the graphs listed below.

Graph Format

User interface elements are described below:

UI Element (A-Z)	Description
# of Errors	Shows the number of calls to the specific item that ended in a SOAP fault over the selected time period.
	The title line of the Errors area or of the SOAP Faults table includes the name of the item whose metrics are displayed. If the Health Summary area displays a tree of Operation/Servers the title line of the Errors area is **Aggregated data for selected operations**.
	Configurable: The SOAP faults affecting the availability can be configured in HP Diagnostics when the call is monitored by HP Diagnostics.

257

UI Element (A-Z)	Description
Pie chart	Represents the faults distribution by type of SOAP fault that occurred when accessing the item during the specified time period. The types of error are: **VersionMismatch**, **MustUnderstand**, **Sender**, **Receiver**, and **DataEncodingUnknown**. The tooltip displays the number of faults of the type represented by the slice. The legend lists the SOAP Fault types.
Worst Consumers	Displays, for the five worst consumers (with the largest number of faulty calls), the number of successful calls (in orange) and the number of calls that ended in error or SOAP faults (in purple) to the item.

Table Format

User interface elements are described below:

UI Element (A-Z)	Description
SOAP Faults Distribution	Shows the percentage of the occurrence of each type of SOAP fault compared to the total number of SOAP faults: **VersionMismatch**, **MustUnderstand**, **Sender**, **Receiver**, or **DataEncodingUnknown**.
SOAP Faults and Errors Overtime	Displays the total number of calls to the selected item that ended in a SOAP fault and the total number of calls to the selected item that ended in an error, over the selected time period, per unit of time.
Worst Consumers	Displays the number of calls to the selected item that ended in an error in the **# of Errors** column, the number of calls to the selected item that ended in a SOAP fault in the **# of SOAP Faults** column, the number of successful calls to the selected item in the **# of Successful Calls** column, and the total number of calls in the **# of Calls** column, per consumer, for the five worst consumers (with the largest number of faulty calls).

Metric Analysis Report

This report displays the performance of a single metric related to a selected view and selected CIs, over time.

To access	**Applications** > **Application Management for SOA**, and select the **Metric Analysis Report** option in the Application Management for SOA tab.
Important information	You can add this report as a component in MyBSM. For details, see "EUM High-Level Status Page" in *Using MyBSM*.
Relevant tasks	"How to View SOA Data in BSM" on page 231

Report Settings

UI Element (A-Z)	Description
<Common report elements>	For details, see "Common Report and Page Elements" in *Reports*.
Active Filter	If relevant, click the **Active Filter** link to select the appropriate conditions for the report. For details, see "Active Filter Dialog Box" on page 235.
Group by	Select to group the performance of the metrics by **Servers**, **Consumers**, **Endpoints**, or not to group the metrics. The selection of one of the groups causes the report to display information for each value of the selected group.

UI Element (A-Z)	Description
Metrics	Select the metric, whose performance during the selected time period, you want to display. You can select:
	➤ **Availability.** The average availability (in percentage) of the selected Web services or operations, running on the selected servers, and accessed by the selected consumer during the selected time frame of the report.
	➤ **Throughput (Calls/Min).** The number of calls running on the selected server, by the selected consumer, per minute, during the selected time frame of the report.
	➤ **Avg. Response Time (sec.).** The average response time (in seconds) of the selected Web services or operations, running on the selected server, by the selected consumer during the selected time frame of the report.
	➤ **# of Calls.** The total number of calls, running on the selected server, by the selected consumer, during the selected time frame of the report.
	➤ **# of SOAP Faults.** The total number of SOAP faults that occurred in calls by the specific consumer.
	➤ **# of Errors.** The total number of faulty calls, running on the selected server, by the selected consumer, during the selected time frame of the report. A faulty call is a call that fails due to the unavailability of the called item.
	➤ **# of Slow Calls (only for real data).** The total number of slow calls, running on the selected server, by the selected consumer, during the selected time frame of the report. A slow call is a call with a response time that is longer than the predefined threshold.

UI Element (A-Z)	Description
Real/Synthetic	Select one of the following: ➤ **Real.** To display data from the Diagnostics data collector. ➤ **Synthetic**. To display data from the SiteScope and Business Process monitors. **Note:** When you generate a SOA report, the **Data Type** selection is displayed in the top part of the report.
Selected CIs	Opens the Selected CIs dialog box where you can select the relevant CI. For details, see "Selected CIs Dialog Box" on page 271.

General Tab

The tab displays the metric behavior over time. If you have selected a group, the graph displays the metric behavior for each value of the selected group. For example, the graph may display the metric behavior for customer 1 and for customer 2.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<legend>	The legend lists each metric and the color of the metric in the graph.
<tooltip>	Move the mouse over a point in the graph to display the value of the metric and the time.
X-axis	Represents the time period and granularity you selected for the report.
Y-axis	Represents the range of values of the metric for the selected time period.

Breaches Tab

This tab is available only when you select the **Avg. Response Time (sec.)** metric.

The tab displays by the percentage of violation (breach) of the threshold by the **Avg. Response Time (sec.)** metric over the report time period. In the example below, the threshold was not breached at any time.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<legend>	The legend lists the metric and the color of the metric in the graph.
<tooltip>	Move the mouse over a point in the graph to display the percentage of the breach and the time.
X-axis	Represents the time period and granularity you selected for the report.
Y-axis	Represents the threshold violations in percentages.

Moving Averages Tab

The tab displays the metric behavior over time (green line). In addition (blue line), it displays the average of the previous 5 points for each point in the metric behavior over time (green line). This provides information about the behavior of the metric at each point in time compared to the average of the metric behavior for the previous 5 points in time. You can, for example, see that the response time at a specific point is much higher than the previous average. User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<legend>	The legend lists the metric and the color of the metric in the graph as well as the color of the moving average.

UI Element (A-Z)	Description
<tooltip>	Move the mouse over a point in the graph to display the value of the metric, the value of the moving average, and the time.
X-axis	Represents the time period and granularity you selected for the report.
Y-axis	Represents the range of values of the metric for the selected time period.

Analysis Tab

The tab displays, in table format, the information displayed in the other tabs. User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
	Below Moving Average. The icon indicates that the value displayed in the table is below the moving average for the past 5 previous samplings.
	Above Threshold Percentile. The icon indicates that the value displayed in the table is .
	Above Moving Average. The icon indicates that the value displayed in the table is above the moving average for the past 5 previous samplings.
<Common report elements>	For details, see "Common Report and Page Elements" in *Reports*.

UI Element (A-Z)	Description
<Drilldown>	Click an underlined value in a cell to display the available drilldowns. Select: ➤ **Drilldown to Health report.** To display the Health report for the selected Web service or operation for the selected time period. For details, see "Health Report" on page 246. ➤ **Drilldown in time range.** To regenerate the Metric Analysis report with a new time range that corresponds to the time range of the original cell and a corresponding finer granularity. The General tab of the report is automatically displayed with the new time range.
<First_column>	The first column of the table lists the values of the group by element you selected in the report's filter. It can be: **Consumers**, **Servers**, **Endpoints**. If you do not select a group, the first column displays the metric's values for the report's time frame.
<Other columns>	The other columns list the values of the metric for the report's time frame and granularity.
<Tooltip>	Move the mouse over a cell in the table to display the value of the group, metric, minimum and maximum of the metric's value during the report's time frame, the time, the threshold and the threshold violation (when the metric is **Avg. Response Time (sec.)**), the moving average status, and the moving average for the last 5 points. Consumers: 16.55.249.85 Avg. Response Time (sec.): 0.007 Minimum: 0.000 Maximum: 0.010 Time: 8/1 02:00:00 PM Threshold Status: Normal Threshold Violation: 0.000 % Threshold: 0.0 % Moving Average Status: Normal Moving Average(5): 0.007

🔍 Metrics Over Time Report

This report displays the performance of selected metrics related to a selected view and selected CIs, over time.

To access	**Applications** > **Application Management for SOA**, and select the **Metrics Over Time Report** option in the Application Management for SOA tab.
Important information	Move the pointer over a tab in the appropriate graphs to display the tooltip that includes the information listed in the table. ➤ For a Web service: ➤ For an operation: The tooltip displays the following information: ➤ **Namespace.** The namespace of the Web service. ➤ **Web Service/Operation.** The name of the selected Web service/operation. ➤ **<metric>.** The value of the metric at this point. **Note:** You can add this report as a component in MyBSM. For details, see "EUM High-Level Status Page" in *Using MyBSM*.
Relevant tasks	"How to View SOA Data in BSM" on page 231

Report Settings

UI Element (A-Z)	Description
<Common report elements>	For details, see "Common Report and Page Elements" in *Reports*.
Active Filter	If relevant, click the **Active Filter** link to select the appropriate conditions for the report. For details, see "Active Filter Dialog Box" on page 235.
Real/Synthetic	Select one of the following: ➤ **Real.** To display data from the Diagnostics data collector. ➤ **Synthetic**. To display data from the SiteScope and Business Process monitors. **Note:** When you generate a SOA report, the **Data Type** selection is displayed in the top part of the report.

Graph and Table Settings

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<graph details>	The View as Graph tab displays the selected metric performance of the selected Web services, operations, endpoints, or consumers, during the selected time frame of the report. The graph legend indicates the color used to display the metric information of the Web services if Web services were selected or operations if Operations were selected in the Active Filters.
<right-click a point in the graph>	To display the Available Drilldowns menu, and select: ➤ **Drilldown to Health Report.** To display the Health report for the selected Web service or operation for the selected time period. For details, see "Health Report" on page 246. ➤ **Time Range Drilldown.** To display the metrics for the selected Web service or operation for the selected time period.

UI Element (A-Z)	Description
<table details>	The View as Table tab displays the selected Web services, or operations performance of the selected metric, during the selected time frame of the report. The table displays the Web service, operation, or both, the namespace of the Web service, and the value of the metric per time unit.
Generate	Click to generate the report.

UI Element (A-Z)	Description
Metrics	Select the metric whose performance during the selected time period, you want to display. You can select: ➤ **Availability.** The average availability (in percentage) of the selected Web services or operations, running on the selected servers, and accessed by the selected consumer during the selected time frame of the report. ➤ **Throughput.** The number of calls running on the selected server, by the selected consumer, per minute, during the selected time frame of the report. ➤ **Avg. Response Time (sec.).** The average response time (in seconds) of the selected Web services or operations, running on the selected server, by the selected consumer during the selected time frame of the report. ➤ **# of Calls.** The total number of calls, running on the selected server, by the selected consumer, during the selected time frame of the report. ➤ **# of Errors.** The total number of faulty calls, running on the selected server, by the selected consumer, during the selected time frame of the report. A faulty call is a call that fails due to the unavailability of the called item. ➤ **# of Slow Calls.** The total number of slow calls, running on the selected server, by the selected consumer, during the selected time frame of the report. A slow call is a call with a response time that is longer than the predefined threshold. ➤ **# of SOAP Faults.** The total number of SOAP faults that occurred in calls by the specific consumer.
View as Graph tab	Click to display the report in graph format.
View as Table tab	Click to display the report in table format.

🔍 Selected CIs Dialog Box

This dialog box enables you to filter SOA reports.

To access	In the Health, Top Metrics, Metrics Over Time, Consumer Summary, or Server and Endpoint Summary reports, click **Selected CIs**.

User interface elements are described below:

UI Element (A-Z)	Description
Browse View	Select the appropriate view and select the relevant CIs in the view. Only views for which the user has permission and that have been assigned to SOA are displayed in the list. For additional information on the available views, see "SOA Views in Service Health" on page 223. **Note:** To add a view to the list of views available in the SOA reports, attach the view to the SOA bundle. To do that, click **Admin** > **RTSM Administration** > **Modeling** > **Modeling Studio**, select the view, click the **View Definition Properties** button 🗐 in **View Mode**, and select the SOA bundle in the **Bundle** box.
Search	Click the **Search** link to search for a specific CI in the current view or in all views.
Selected CIs	Select one of the following: ➤ **Web Services.** Displays a check box only for the Web services CIs appearing in the view. ➤ **Operations.** Displays a check box only for the operation CIs appearing in the view. You can select up to 20 Web services or operations. You can modify that limit in the Infrastructure Settings. For details, see "Customize the number of web services or operations displayed in the SOA reports" on page 234.

🔍 Server and Endpoint Summary Report

This report displays a drillable summary of the metrics for all of the servers or endpoints on which the selected Web services or operations of a selected view are running.

To access	**Application** > **Application Management for SOA**, click the **Application Management for SOA** tab, and select the **Server and Endpoint Summary Report** option.
Important information	When you select **Real**, the report displays information only for the consumers that were registered in the Diagnostics system. All other consumers are aggregated and presented as **Others**.
	The report is available only if the Server IP field exists in the sample.
	Move the pointer over a tab in a graph to display a tooltip that indicates the number of errors, successful calls, SOAP faults, and the total number of calls to the selected server.
	Server IP: 16.59.56.159 # of Errors: 0 # of Successful calls: 5,549 # of SOAP faults: 0 # of Calls: 5,549 Available Drilldowns: Drill Down to Health Report Drill Down to Endpoint Summary report
	Note: You can add this report as a component in MyBSM. For details, see "EUM High-Level Status Page" in *Using MyBSM*.
Relevant tasks	"How to View SOA Data in BSM" on page 231

Report Settings

User interface elements are described below:

UI Element (A-Z)	Description
<Common report elements>	For details, see "Common Report and Page Elements" in *Reports*.
Active Filter	If relevant, click the **Active Filter** link to select the appropriate conditions for the report. For details, see "Active Filter Dialog Box" on page 235.
Real/Synthetic	Select one of the following: ➤ **Real.** To display data from the Diagnostics data collector. ➤ **Synthetic.** To display data from the SiteScope and Business Process monitors. **Note:** When you generate a SOA report, the **Data Type** selection is displayed in the top part of the report.
Report Granularity	Select one of the following: ➤ **Servers.** To display the Server and Endpoint Summary report with information about the servers. ➤ **Endpoints.** To display the Server and Endpoint Summary report with information about the endpoints.

Server/Endpoint Summary Area

This area displays the health metrics for all of the servers/endpoints on which the selected Web services or operations are running. If, in the Active Filters, you also select specific endpoint or consumer, the health metrics are further filtered by the selected endpoint or consumer.

The following is an example of the Server/Endpoint Summary area.

Important information	The Server Summary area is the same in the View as Graph and View as Table tabs.

User interface elements are described below:

UI Element (A-Z)	Description
	Drilldown to Health report. Drills down to the Health Report for the selected element. For details, see "Health Report" on page 246.
	Drilldown to Endpoint Summary Report. Drills down to the Endpoint Summary Report for the selected element. For details, see "Server and Endpoint Summary Report" on page 272.

UI Element (A-Z)	Description
# of Calls	The total number of calls to the server accessed by the Web services, operations, or consumer.
# of Errors	The total number of errors that occurred in calls by the specific consumer.
	Configurable: The SOAP faults affecting the availability can be configured in HP Diagnostics when the call is monitored by HP Diagnostics.
# of Slow Calls	The number of slow calls that occurred in calls by the specific consumer.
	A slow call is a call with a response time that is longer than a predefined threshold.
	Note: The value displayed by **# of Slow Calls** is different from the value of the **Total Threshold Violation** in HP Diagnostics. In HP Diagnostics the **Total Threshold Violation** includes the overall number of violation from all the calls and in BSM **# of Slow Calls** includes only the violations of the successful calls.
# of SOAP Faults	The total number of SOAP faults that occurred in calls by the specific consumer.
Availability (%)	The availability of the server accessed by the selected Web services, operations, or consumer. The availability is calculated as the number of successful calls made to the server divided by the total number of calls made to the server, multiplied by 100.
	The background is colored according to the threshold specified in the Availability KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.
Endpoint	The name of the endpoint.
	Note: This column is displayed only when you select the **Endpoints** report granularity.
	Click the endpoint to drill down to the Health Report for the selected element. For details, see "Health Report" on page 246.

UI Element (A-Z)	Description
Response Time (sec.)	The average response time (in seconds) of the server accessed by the selected Web services, operations, or consumer. The background is colored according to the threshold specified in the Response Time KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.
Server	The IP address of the server. Click the gray arrow to the right of the server to display drilldown menu options where you can select the **Drilldown to Health Report** or **Drilldown to Endpoint Summary Report** options to access the relevant report for the element.
Throughput (calls per min.)	The number of calls, per minute, to the server by the selected Web services, operations, or consumer. The background is colored according to the threshold specified in the Throughput KPI definition. For details, see "HI and KPI Definitions" in *Using Service Health*.

Worst Server Area

This area displays the successful and faulty calls of the worst five servers/ endpoints accessed by the selected Web services, operations, or consumer.

The following is an example of the Worst Server area.

Important information	The Worst Server area and the Worst Endpoint area display the same information in the View as Graph and View as Table tabs.
	Each tab in the graph represents one of the five worst servers or endpoints and displays the number of successful calls (in red) and the number of faulty calls (in purple).

User interface elements are described below:

UI Element (A-Z)	Description
# of Calls	The total number of calls to the server accessed by the Web services, operations, or consumer.
# of Errors	The number of calls to the server that ended with an error. **Configurable:** The SOAP faults affecting the availability can be configured in HP Diagnostics when the call is monitored by HP Diagnostics.
# of SOAP Faults	The total number of SOAP faults that occurred in calls by the specific consumer.
# of Successful calls	The number of calls to the server that were successful.
Endpoint	The name of the worst endpoint.
Server	The IP address of the worst server.

🔍 Top Metrics Report

This report displays the top metrics information about the traffic to and from all of the monitored Web services or operations in a specific view.

To access	**Applications** > **Application Management for SOA**, click the **Application Management for SOA** tab and select the **Top Metrics** option.
Important information	Move the pointer over a tab in the appropriate graphs to display the tooltip that includes the information listed in the table. **Details** Namespace: http://example.org Name: creditLoanApprovalService Availability (%): 100.00 Avg. Response Time (Sec.): 0.00 # of Calls: 9,921 # of Errors: 0 # of SOAP Faults: 0 # of Slow Calls: 1 Drill Down to Health Report **Note:** You can add this report as a component in MyBSM. For details, see "EUM High-Level Status Page" in *Using MyBSM*.
Relevant tasks	"How to View SOA Data in BSM" on page 231

Report Settings

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Common report elements>	For details, see "Common Report and Page Elements" in *Reports*.
Active Filter	If relevant, click the **Active Filter** link to select the appropriate conditions for the report. For details, see "Active Filter Dialog Box" on page 235.

UI Element (A-Z)	Description
Real/Synthetic	Select one of the following: ➤ **Real.** To display data from the Diagnostics data collector. ➤ **Synthetic.** To display data from the SiteScope and Business Process monitors. **Note:** When you generate a SOA report, the **Data Type** selection is displayed in the top part of the report.

Top Area

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
	Health report drilldown. In the View as Table tab: ➤ Opens the Health Report of the Web service's operation in table format for the selected Web Service. ➤ Opens the Health Report of the operation's servers in table format, for the selected operation.
<bar in graph>	From the View as Graph tab, click the bar that corresponds to: ➤ a specific Web service to open the Health Report of the Web service's operations in graph format. ➤ a specific operation to open the Health Report of the operation's servers in graph format.
Report Granularity	Select: ➤ **Web services** to display the top metrics information for the selected Web services. ➤ **Operations** to display the top metrics information for the selected operations.

Web Services-Related Graphs

User interface elements are described below:

UI Element (A-Z)	Description
Least Active Web Services	Displays the five Web services that received the lowest number of calls (that is, were least used), during the selected time frame of the report. Each tab represents the total number of calls to the Web service. This graph is displayed if you have selected the **Web Services** report granularity. For details on the table columns, see "Web Services-Related Table" on page 285.
Least Available Web Services	Displays the availability of the five Web services with the lowest availability, during the selected time frame of the report. The availability is calculated as the number of successful calls to the Web service, divided by the total number of calls to the Web service, and multiplied by 100. This graph is displayed if you have selected the **Web Services** report granularity. For details on the table columns, see "Web Services-Related Table" on page 285.

UI Element (A-Z)	Description
Most Active Web Services	Displays the five Web services with the highest number of calls, during the selected time frame of the report. Each tab represents the total number of calls to the Web service. This graph is displayed if you have selected the **Web Services** report granularity. For details on the table columns, see "Web Services-Related Table" on page 285.

UI Element (A-Z)	Description
Slowest Web Services	Displays the five slowest Web services in the selected time frame of the report. A slow Web service is defined as having the longest response time (no matter the threshold value). Each tab represents the average of the response times for the Web service during the time frame of the report. This graph is displayed if you have selected the **Web Services** report granularity. For details on the table columns, see "Web Services-Related Table" on page 285.

UI Element (A-Z)	Description
Web Services with Most Errors	Displays the five Web services with the largest number of failed values, during the selected time frame of the report. Each tab represents the total number of calls that ended in errors, received by the Web service. This graph is displayed if you have selected the **Web Services** report granularity. For details on the table columns, see "Web Services-Related Table" on page 285.
Web Services with Most Slow Calls	Displays the five Web services with the highest number of slow calls, in the selected time frame of the report. A slow call is defined as a call that lasts longer than a predefined threshold. Each tab represents the total number of slow calls received by the Web service. This graph is displayed if you have selected the **Web Services** report granularity. For details on the table columns, see "Web Services-Related Table" on page 285.

Web Services-Related Table

User interface elements are described below:

UI Element (A-Z)	Description
# of Calls	The total number of calls to the specific Web service during the selected time frame of the report.
# of Errors	The number of calls to the specific Web service, during the selected time frame of the report, that failed due to the unavailability of the Web service. **Configurable:** The SOAP faults affecting the availability can be configured in HP Diagnostics when the call is monitored by HP Diagnostics.
# of Slow Calls	The number of slow calls to the specific Web service during the selected time frame of the report. A slow call is a call with a response time that is longer than a predefined threshold. **Note:** The value displayed by **# of Slow Calls** is different from the value of the **Total Threshold Violation** in HP Diagnostics. In HP Diagnostics the **Total Threshold Violation** includes the overall number of violation from all the calls and in BSM **# of Slow Calls** includes only the violations of the successful calls.
# of SOAP Faults	The number of calls to the specific Web service, during the selected time frame of the report, that ended in SOAP faults.
Availability (%)	The average availability of the Web service during the selected time frame of the report. The availability is calculated as the number of successful calls to the Web service, divided by the total number of calls to the Web service, and multiplied by 100.
Avg. Response Time (sec.)	The average response time (in seconds) of the Web service during the selected time frame of the report.

UI Element (A-Z)	Description
Name	The name of the selected Web service.
NameSpace	The name space of the Web service.

Operations-Related Graphs

User interface elements are described below:

UI Element (A-Z)	Description
Least Active Operations	Displays the five operations that received the lowest number of calls (that is, were least used), during the selected time frame of the report. Each tab represents the total number of calls to the operation. This graph is displayed if you have selected the **Operations** report granularity. For details on the table columns, see "Operations-Related Table" on page 289.

UI Element (A-Z)	Description
Least Available Operations	Displays the availability of the five **operations** with the lowest availability, during the selected time frame of the report. The availability is calculated as the number of successful calls to the **operation**, divided by the total number of calls to the operation, and multiplied by 100. This graph is displayed if you have selected the **Operations** report granularity. For details on the table columns, see "Operations-Related Table" on page 289.
Most Active Operations	Displays the five operations with the highest number of calls, during the selected time frame of the report. Each tab represents the total number of calls to the operation. This graph is displayed if you have selected the **Operations** report granularity. For details on the table columns, see "Operations-Related Table" on page 289.

UI Element (A-Z)	Description
Operations with Most Errors	Displays the five **operations** with the largest number of calls with errors, during the selected time frame of the report. Each tab represents the total number of errors received by the **operation**. This graph is displayed if you have selected the **Operations** report granularity. For details on the table columns, see "Operations-Related Table" on page 289.
Operations with Most Slow Calls	Displays the five operations with the highest number of slow calls, in the selected time frame of the report. A slow call is defined as a call that lasts longer than a predefined threshold. Each tab represents the total number of slow calls received by the operation. This graph is displayed if you have selected the **Operations** report granularity. For details on the table columns, see "Operations-Related Table" on page 289.

UI Element (A-Z)	Description
Slowest Operations	The Slowest Operations graph displays the five slowest operations in the selected time frame of the report. A slow operation is defined as having the longest response time (no matter the threshold value). Each tab represents the average of the response times for the operation during the time frame of the report. This graph is displayed if you have selected the **Operations** report granularity. For details on the table columns, see "Operations-Related Table" on page 289.

Operations-Related Table

The Least Active Operations, Slowest Operations, Operations with Most SOAP Faults, Operations with Most Slow Calls, Most Active Operations, or Least Active Operations tables includes the following elements:

UI Element (A-Z)	Description
# of Calls	The total number of calls to the specific operation during the selected time frame of the report.
# of Errors	The number of calls to the specific operation, during the selected time frame of the report, that failed due to the unavailability of the operation. **Configurable:** The SOAP faults affecting the availability can be configured in HP Diagnostics when the call is monitored by HP Diagnostics.

UI Element (A-Z)	Description
# of Slow Calls	The number of slow calls to the specific operation during the selected time frame of the report. A slow call is a call with a response time that is longer than a predefined threshold.
	Note: The value displayed by **# of Slow Calls** is different from the value of the **Total Threshold Violation** in HP Diagnostics. In HP Diagnostics the **Total Threshold Violation** includes the overall number of violation from all the calls and in BSM **# of Slow Calls** includes only the violations of the successful calls.
# of SOAP Faults	The total number of SOAP faults that occurred in calls by the specific consumer.
	The column is displayed only when you select the **Real** data type.
Availability (%)	The average availability of the operation during the selected time frame of the report. The availability is calculated as the number of successful calls to the operation, divided by the total number of calls to the operation, and multiplied by 100.
Avg. Response Time (sec.)	The average response time (in seconds) of the operation during the selected time frame of the report.
Name	The name of the operation.
NameSpace	The name space of the Web service that runs the operation.
Web Service	The name of the Web service that runs the operation.

Part IV

Integrations

7

Business Service Management Integration with Other Applications

This chapter includes:

Concepts

Concepts

♣ Business Service Management Integration with Other Applications Overview

BSM has the ability to integrate with Business Technology Optimization (BTO) products, with applications that are part of BSM, and with external applications.

These integrations enable the flow of data from application to application as well as the flow of events from the applications to BSM and to its Operations Management component, depending on the applications. You can drill down from BSM to some of the relevant applications.

Consult the relevant BSM_<version_number>_Release_Notes.pdf for details about the supported versions.

Note: The following section contains references to the **Integrations Catalog**, which can be found at http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3. To access this catalog you must have an HP Passport ID. (Note that not all of the integrations that are listed in this section are also listed in the Integrations Catalog.)

Network Node Manager i (NNMi)

The integration between NNMi 9.00 and BSM 9.10 provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
(1) NNMi events -> Operations Management events. If you have an Event Management Foundation license, the NNMi events are displayed in the Event Browser in Operations Management. You can also access the NNMi console from the Operations Management Event Browser. (If BSM is also integrated with HPOM, these events are also displayed in HPOM. You can also access the NNMi console from HPOM.) For more details, see item 344 in the Integrations Catalog: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=344.	The NNMi events are sent using the BSM Integration Adapter to BSM. This agent implementation of the HP NNMi—HPOM integration is the preferred solution for integrating HPOM with NNMi.	"Integrate Network Node Manager i (NNMi) with BSM" on page 353 "HP NNMi—HPOM Integration (Agent Implementation)" in *NNMi Deployment Reference* "HP BSM Integration Adapter" on page 407

What the Integration Gives You	How the Integration Works	Where to Get the Details
(2) NNMi events -> BSM health indicators. If the NNMi events have corresponding health indicators, the health indicators affect the status of the relevant CIs in applications such as Service Health and Service Level Management.	The NNMi events are sent using the BSM Integration Adapter to BSM. This agent implementation of the HP NNMi—HPOM integration is the preferred solution for integrating HPOM with NNMi.	"Integrate Network Node Manager i (NNMi) with BSM" on page 353 "HP BSM Integration Adapter" on page 407
(3) NNMi topology -> BSM RTSM topology. The topology integration populates the BSM Run-time Service Model (RTSM) with the NNMi network topology. BSM stores each device, interface, IP address and a few other artifacts in the NNMi network topology as a Configuration Item (CI) and includes it in the relevant views.	The topology data flows (are pushed) one way from NNMi to BSM RTSM (this is the preferred implementation.	"Integrate Network Node Manager i (NNMi) with BSM" on page 353 "HP Business Service Management Topology" in the *NNMi Deployment Reference* "Viewing HP Network Node Manager (NNMi) Data From Real User Monitor Reports" in *Using End User Management* "Limitations" on page 298

What the Integration Gives You	How the Integration Works	Where to Get the Details
(4) BSM -> NNMi - drilldown. You can also configure a link to the NNMi management server, that enables you to drill down from various EUM reports, MyBSM, and other locations, to NNMi where you can display trace route information between the client and the destination machine. You can also use URL tools to launch a browser that enables you to connect to the NNMi Management server and further analyze incoming events in NNMi. NNMi user interface components (network maps, items detailed information dialogs, etc.) can be displayed directly inside BSM's UI Mash-Up framework. This enables for integration of network-centric views into for example the MyBSM portal views.	The topology data flows (are pushed) one way from NNMi to BSM RTSM. From BSM, users can connect directly into network maps or detailed information dialogs provided by NNMi's direct URL access.	"Integrate Network Node Manager i (NNMi) with BSM" on page 353 "HP Business Service Management Topology" in the *NNMi Deployment Reference* "Viewing HP Network Node Manager (NNMi) Data From Real User Monitor Reports" in *Using End User Management*

Note: If you are performing an integration between NNMi 9 and BSM, NNMi sends the topology information into the RTSM. Before performing this integration, read the information located in the HP NNMi – HP BSM Topology Integration Best Practices PDF.

Limitations

If the NNMi topology is not synchronized with the BSM RTSM topology, the **Monitored by** property of the BSM CIs corresponding to the NNMi CIs are empty, and these CIs are not displayed in the System Monitors only Perspective, System Hardware Monitoring and System Software Monitoring views.

🍀 HP Operations Manager

This integration provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
(1) HPOM events -> Operations Management events. If you have an Event Management Foundation license, the events are displayed in the Event Browser in Operations Management.	The bi-directional synchronization of events between HPOM and Operations Management.	"Configure Operations Management Connections - Overview" on page 324 "Limitations" on page 300

What the Integration Gives You	How the Integration Works	Where to Get the Details
(2) HPOM events -> BSM health indicators. If the HPOM events have corresponding health indicators, the health indicators affect the status of the relevant CIs in applications such as Service Health and Service Level Management.	Based on the incoming events from HPOM, corresponding health indicators are set for the related CIs in BSM.	"Health Perspective" in *Using Operations Management*
(3) BSM -> HPOM - Drilldown. In addition, you can drilldown from Service Health to the HPOM application. For details on the drilldown, see "Service Health Menu Options" in *Using Service Health*. For more details, see item 416 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=416.	Based on the incoming events from HPOM, corresponding health indicators are set for the related CIs in BSM.	"Operations Manager Actions" in *Using Operations Management* "Service Health Menu Options" in *Using Service Health*
(4) BSM alerts -> HPOM events. The alert integration enables the display of events triggered by the BSM alerts, in HPOM. When a specific BSM CI Status alert, SLA alert, or EUM alert is triggered, a corresponding event is automatically sent to the HPOM applications, to proactively alert the operator about a problem in the system. For more details, see item 199 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=199.	The alerts are mapped to events using the Event Model.	"Generate Events in HP Operations Manager when BSM Alert is Triggered" on page 347
(5) HPOM topology -> RTSM topology. If you have the Event Management Foundation license enabled, the HPOM topology (HPOM Services) can synchronize with the BSM RTSM topology.	The OM Services are synchronized with BSM and, using corresponding mapping rules, are transformed into CIs stored in the RTSM.	"Topology Synchronization" in *Using Operations Management*

Limitations

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

HP SiteScope

This integration provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
(1) SiteScope events -> Operations Management events and health indicators. If you have an Event Management Foundation license, the events corresponding to SiteScope metrics status changes and alerts are displayed in the Event Browser in Operations Management. Whether you have an Event Management Foundation license or you do not, if the SiteScope events have corresponding event type indicators (ETIs), the health indicators affect the status of the relevant CIs in BSM applications such as Service Health and Service Level Management.	If SiteScope is configured as a data collector for BSM's Operations Management, SiteScope sends data about SiteScope metrics status changes and alerts to Operations Management using the HP Operations agent technology.	"How to Enable SiteScope to Send Events to HPOM or BSM" in *Using System Availability Management* See the *HP Business Service Management Deployment Guide* PDF in the HP BSM Documentation Library "Integrating SiteScope with Business Service Management Applications" in *SiteScope-Business Service Management/ Operations Manager Integration Best Practices* in the SiteScope Help

What the Integration Gives You	How the Integration Works	Where to Get the Details
(2) SiteScope events -> HPOM events. Events generated from SiteScope metrics status changes and alerts are displayed in HPOM.	If SiteScope is configured to report events to HPOM, SiteScope sends data about SiteScope metrics status changes and alerts to HPOM using the HP Operations agent technology.	"How to Enable SiteScope to Send Events to HPOM or BSM" in *Using System Availability Management* "Integrating SiteScope with Business Service Management Applications" in *SiteScope-Business Service Management/ Operations Manager Integration Best Practices* in the SiteScope Help

What the Integration Gives You	How the Integration Works	Where to Get the Details
(3) SiteScope events -> Operations Management events and health indicators using HPOM. If you have an Event Management Foundation license, events generated from SiteScope metrics status changes and alerts are sent to Operations Management using HPOM. If the SiteScope events have corresponding event type indicators (ETIs), the health indicators affect the status of the relevant CIs in BSM applications such as Service Health and Service Level Management.	If SiteScope is configured to report events to HPOM, SiteScope sends data about SiteScope metrics status changes and alerts to HPOM using the HP Operations agent technology.	"How to Enable SiteScope to Send Events to HPOM or BSM" in *Using System Availability Management* "Configure Operations Management Connections" on page 323 See the *HP Business Service Management Deployment Guide* PDF in the HP BSM Documentation Library "Integrating SiteScope with Business Service Management Applications" in *SiteScope-Business Service Management/ Operations Manager Integration Best Practices* in the SiteScope Help

What the Integration Gives You	How the Integration Works	Where to Get the Details
(4) SiteScope metrics -> BSM metrics and health indicators. If the SiteScope metrics have health indicators assigned to them, these health indicators affect the status of the relevant CIs in BSM applications such as Service Health and Service Level Management.	SiteScope sends metrics to BSM.	"How to Configure the Integration Between SiteScope and BSM" in *Using System Availability Management* "Integrating SiteScope with Business Service Management Applications" in *SiteScope-Business Service Management/ Operations Manager Integration Best Practices* in the SiteScope Help
(5) SiteScope metrics -> Performance Perspective in Operations Management. SiteScope collects metrics data, and logs it to the Operations agent data store, which is installed on the SiteScope host. When a user in Performance Perspective in BSM draws or designs a graph, Performance Perspective collects metrics data from the Operations agent data store for the selected CI, which is monitored by SiteScope, and draws the graph.	SiteScope uses the HP Operations agent to make its metrics data available to BSM (Performance Perspective in Operations Management). To enable SiteScope to report metrics, the HP Operations agent must be installed on the SiteScope server.	"Reporting Metrics Using the HP Operations Agent" in *Using System Availability Management* "Integrating SiteScope with Business Service Management Applications" in *SiteScope-Business Service Management/ Operations Manager Integration Best Practices* in the SiteScope Help

What the Integration Gives You	How the Integration Works	Where to Get the Details
(6) SiteScope metrics -> Performance Manager graphs. SiteScope collects metrics data, and logs it to the Operations agent data store, which is installed on the SiteScope host. When a user in Performance Manager draws or designs a graph, Performance Manager collects metrics data from the Operations agent data store for the selected node in Performance Manager that is monitored by SiteScope, and draws the graph.	SiteScope uses the HP Operations agent to make its metrics data available to HP Operations Manager (Performance Manager). To enable SiteScope to report metrics, the HP Operations agent must be installed on the SiteScope server.	"Reporting Metrics Using the HP Operations Agent" in *Using System Availability Management* "Integrating SiteScope with Business Service Management Applications" in *SiteScope-Business Service Management/ Operations Manager Integration Best Practices* (SiteScope Help)
(7) SiteScope metrics -> HP Diagnostics data. SiteScope forwards metrics to HP Diagnostics, displaying a more complete view of the performance of the application server that is monitored by Diagnostics. The metrics can provide insight into the infrastructure components onto which the application servers are deployed.	SiteScope forwards metrics to HP Diagnostics using Diagnostics Integration Preferences.	"Diagnostics Integration Overview" in *Using SiteScope* in the SiteScope Help

What the Integration Gives You	How the Integration Works	Where to Get the Details
(8) SiteScope event -> NNMi. The SiteScope-NNMi event integration enables SiteScope to forward events from SiteScope monitors (metrics status changes and alerts), and displays the event data in the NNMi incident console. (SiteScope 11.10 and NNMi 9.10 or later) For more details, see item 483 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=483.	SiteScope sends SNMP traps to NNMi. The SNMP traps are converted to NNMi incidents. From the resulting incidents, an NNMi console user can launch SiteScope in the context of that monitor (using the URL in the SNMP trap format sent to the NNMi server).	"Sending SiteScope Events to NNMi" in *Using System Availability Management* "HP NNMi-HP SiteScope Events Integration" in HP SiteScope" in *NNMi Deployment Reference* included on the NNMi product media
(9) SiteScope metrics -> NNMi. The SiteScope-NNMi metric integration enables SiteScope to forward metrics data from SiteScope monitors (metrics status changes and alerts) to NNMi. (SiteScope 11.10 and NNMi 9.10 or later) For more details, see item 483 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=483.	The HP NNMi-HP SiteScope System Metrics integration populates the NNM iSPI Performance for Metrics Network Performance Server (NPS) with system metrics data collected by SiteScope monitors using the Generic Data Integration.	"Reporting Metrics to NNMi" in *Using System Availability Management* "HP NNMi-HP SiteScope Events Integration" in HP SiteScope" in *NNMi Deployment Reference* included on the NNMi product media

What the Integration Gives You	How the Integration Works	Where to Get the Details
SiteScope events and alarms -> Execute OO flows. The HP Operations Orchestration (OO) SiteScope integration enables administrators to build OO flows that are integrated with HP SiteScope. The integration allows OO administrators to connect specific events or alarms in SiteScope to the execution of OO flows. For more details, see item 225 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=225.	The administrator builds OO flows using SiteScope operations (which use SiteScope API calls) in OO Studio. For example, you can create flows that automatically create monitors in SiteScope when a new server is added, or delete monitors when the server is decommissioned.	The *HP Operations Orchestration SiteScope Integration Guide* in the OO documentation set

🍀 HP Service Manager (SM)

The integration of Business Service Management with HP Service Manager provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
(1) HP Service Manager incidents -> Service Health Number of Open Tickets KPI and SLAs in Service Level Management. HP Service Manager incident raw data is sent to BSM to determine incident management-related metrics such as Number of Open Tickets and the MTTR, MTBF, MTBSI KPIs. You can view, in Service Health, Service Manager Number of Open Incidents and manage, in Service Level Management, SLAs over Serviceability KPIs based on Service Manager incidents. For more details, see item 57 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=57.	Incident raw data is collected by SiteScope monitors and sent to BSM. The relevant topology is created in RTSM using the HP Service Manager EMS integration.	"EMS Integration Administration" on page 421 Open the main page of the online documentation library, locate the Solutions and Integration column (on the right) and click the HP Service Manager Integration link. The interactive document is also available from the documentation update site located at http://h20230.www2.hp.com/selfsolve/manuals.
(2) BSM Service Health -> HP Service Manager - drilldown. From Service Health, the user can drill down to the HP Service Manager ticket using the right-click menu. For details, see "Service Health Menu Options" in *Using Service Health*. For more details, see item 58 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=58.	Incident raw data is collected by SiteScope monitors and sent to BSM. The relevant topology is created in RTSM using the HP Service Manager EMS integration.	"EMS Integration Administration" on page 421 Open the main page of the online documentation library, locate the Solutions and Integration column (on the right) and click the HP Service Manager Integration link.

What the Integration Gives You	How the Integration Works	Where to Get the Details
(3) BSM alerts -> HP Service Manager incidents. You can configure specific CI Status alerts, SLA alerts, or EUM alerts to automatically open a corresponding incident in HP Service Manager, to proactively alert the operator about a problem in the system.		Open the main page of the online documentation library, locate the Solutions and Integration column (on the right) and click the HP Service Manager Integration link.
(4) HP Service Manager planned changes and incidents -> BSM Service Health. HP Service Manager planned changes and incidents are queried, online, every time the user selects a CI in BSM Service Health Planned Changes and Incident tab, and the information is displayed in that tab. For more details, see items 243 and 245 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=243, and http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=245.	This integration is based on federating data from HP Service Manager. Incidents and planned changes are federated on demand and presented in Business Service Management.	Open the main page of the online documentation library, locate the Solutions and Integration column (on the right) and click the HP Service Manager Integration link.
(5) HP Service Manager -> BSM - drilldown. From HP Service Manager 9.20 you can drill down to the BSM Business Impact report from the relevant CI using the **Launch Business Impact Report** option. For more details, see item 381 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=381.		HP Service Manager documentation For details, see "Business Impact Report" in *Using Service Health*.

What the Integration Gives You	How the Integration Works	Where to Get the Details
(6) HP Service Manager incidents -> Operations Management incidents attached to events (incident generation). Operations Management systems can automatically or manually generate HP Service Manager incidents from Operations Management events, if you have an Event Management Foundation license. For events that have a corresponding incident, the current state of the incident can be directly viewed in the External Information tab of the Operations Management Event Browser. Operations Management events, and subsequent updates, can be forwarded to a supported HP Service Manager system that has been configured as a connected server within Operations Management. Appropriate events can be automatically forwarded to external servers using filters specified in forwarding rules. For more details, see item 337 in the Integrations Catalog, at http:// support.openview.hp.com/sc/solutions/ integrations.jsp?intid=337.	Events can be forwarded to HP Service Manager servers that have been configured as connected servers. Appropriate events can be automatically forwarded to external servers (See event Forwarding to External Servers).	HP Service Manager documentation "How to Create a Connection to an External Event Processing Server" in *Using Operations Management* "Event Forwarding to External Servers" in *Using Operations Management*
(7) Operations Management -> HP Service Manager - drilldown. From Operations Management, the user can drill down to the HP Service Manager ticket from the event in the Event Browser, if configured to do so. For more details, see item 337 in the Integrations Catalog, at http:// support.openview.hp.com/sc/solutions/ integrations.jsp?intid=337.	For Service Manager servers that are configured as "connected external servers", you can drill down to the Service Manager system from the External Info Tab (or context menu).	HP Service Manager documentation The Operations Management-HP Service Manager integration is described in the *OMi Extensibility Guide* and HP Service Manager online help. *"External Info Tab"* in *Using Operations Management*

🔩 HP Operations Orchestration (OO)

The integration between BSM and OO provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
Launch OO runbooks from Service Health. Business Service Management provides a number of predefined mappings between CIs and OO run books. This mapping and the integration procedure enable you to manually launch OO run books from the Service Health applications.	In BSM, predefined mappings between CIs and OO run books.	"Predefined Mappings" on page 371 "HP Operations Orchestration Integration" on page 359
Launch OO runbooks from Operations Management. If you have an Event Management Foundation license, when an event is opened in Operations Management, if the CI for this event has a run book assigned to it, you can run it manually.	The OO run book parameters are populated using the map to the CI or event attributes.	"Run Book Mapping Configuration Wizard" on page 374 "HP Operations Orchestration Integration" on page 359
Automatically launch OO runbooks from Operations Management. You can configure rules to automatically run a Run Book or a series of Run Books in the context of an event.	Configure a rule that automatically runs the relevant Run Book if the event matches the predefined parameters.	"Introduction to Run Book Automation" in *Using Operations Management*

Limitations

If you are planning to integrate both BSM with OO and HP Service Manager with OO, it is recommended to perform the HP Service Manager-OO integration before the BSM-OO integration due to use of SSL certificates in both integrations. You then need to modify the export string in OO for the BSM and OO integration.

HP Release Control (RC)

The integration between BSM and Release Control. Release Control provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
Release Control -> **Service Health - data.** Release Control data sent to Service Health. You can view: ➤ The Number of Planned Changes, Number of Actual Changes, or Latent (unauthorized) Changes KPIs, in the last 24 hours, for the selected CI, in the Service Health 360° tab, in BSM. For details, see "360° View" in *Using Service Health*. ➤ Change Requests are managed by Release Control. The Change Requests related to the selected CI, are displayed for the selected CI in the Service Health 360° tab, in BSM. The time frame for the Change Requests is from 7 days before the Change Requests start date to 7 days after. For details, see "360° View" in *Using Service Health*. For more details, see item 244 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=244.	BSM receives data about the planned changes, number of actual changes, and latent changes from Release Control using the **RCKpiActualChangeAdapter**, **RCKpiLatentChangeAdapter**, and **RCKpiPlannedChangeAdapter** provided by Release Control. BSM receives data about the change requests from Release Control using the **RcChangeAdapter** provided by Release Control.	"How to Configure KPIs as Federated in HP Business Availability Center 8.x or Business Service Management 9.x" in *HP Release Control User Guide*

What the Integration Gives You	How the Integration Works	Where to Get the Details
Service Health to Release Control - data. Service Health data is sent to Release Control. You can view any of the KPIs assigned to the selected CI in Release Control in the Director module by clicking the KPI button. For details, see RC documentation.	Release Control receives information about all the federated KPIs (for example: System Availability, System Performance, and so on) BSM has provided with the **BACKPIsAdapter**.	"How to Configure KPIs as Federated in HP Business Availability Center 8.x or Business Service Management 9.x" in *HP Release Control User Guide*

To integrate Release Control (version 9.11 and earlier) and BSM:

RTSM is the BSM operational storage and stores only CIs that are relevant to BSM operational use cases. It does not support a direct integration with Release Control.

To integrate BSM with Release Control you must:

1 Install an external CMDB. For details, see "Integrating Multiple CMDBs" in *Data Flow Management*.

2 Configure the topology synchronization between the CMDB and RTSM. This combination will serve as a CMS. For details, see "Topology Synchronization" in *Using Operations Management*.

3 To display Release Control information in BSM Service Health and BSM information in Release Control you must configure the relevant Adapters (for details about the Adapters, see the table above). For details on configuring the Adapters, see "How to Configure KPIs as Federated in HP Business Availability Center 8.x or Business Service Management 9.x" in *HP Release Control User Guide*.

4 To correctly integrate RC Change Requests into the Changes and Incidents tab in Service Health, if you integrate RC 9.11 or earlier, do the following:

   a Navigate to the Adapter Management page and in the Resources pane select **RcChangeAdapter** > **Configuration Files** > **convertFields.properties**.

   b Append the following line to the end of the file: **urgency=urgency**

   c Create a new properties file called **RcChangeAdapter/ urgency.properties** and add the following lines:

```
# File format:
# RC urgency value=uCMDB urgency value
Critical=1_critical
High=2_high
Normal=3_average
Low=4_low
#UNKNOWN= there is no available value in uCMDB: 'it_process_urgency_enum'
```

   d Save the file.

CLIP

Closed Loop Incident Process (CLIP) is an integrated solution that brings together HP offerings for BSM, IT Service Management (ITSM), and Business Service Automation (BSA). It enables integrated processes that help the IT operations and service desk teams to predict, detect, and remedy problems that could affect the business performance.

For details on implementing the CLIP solution, access the latest version of the CLIP documentation under the **Application Performance Management (BAC)** product section on the HP Software Support Product Manuals site (http://support.openview.hp.com/selfsolve/manuals). To enter the site, you must log on with your HP Passport ID.

🔶 HP Diagnostics

The integration of BSM applications with HP Diagnostics enables the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
(1) HP Diagnostics data -> BSM Service Health. You can view HP Diagnostics data in the Diagnostics View in Service Health and Service Level Management	The integration of HP Diagnostics with BSM.	"How to View HP Diagnostics Data in HP Business Service Management" on page 383
(2) BSM -> HP Diagnostics - drilldown. In BSM, you can drill down to HP Diagnostics.		"Service Health Menu Options" in *Using Service Health*

What the Integration Gives You	How the Integration Works	Where to Get the Details
(3) HP Diagnostics -> SiteScope - drilldown. You can drill down directly from the HP Diagnostics user interface to SiteScope data directly when working with HP Diagnostics and SiteScope (without Business Service Management).		"Integrations" in the *HP Diagnostics User's Guide/Online Help*
(4) BSM EUM reports -> HP Diagnostics - drilldown. In BSM End User Management reports, you can drill down to HP Diagnostics to display snapshots of server requests for specific pages.		"Viewing HP Diagnostics Data From End User Management Reports" in *Using End User Management*
(5) BSM Transaction Management -> HP Diagnostics. You can drill down from BSM TV Event Analysis report to the Diagnostics Hosts and Diagnostics Server views.		"Working with Other Applications in BSM > HP Diagnostics" in *Using Transaction Management*
(6) Events from HP Diagnostics to health indicators in BSM. Status (coloring) for event-based health indicators is sent to BSM from HP Diagnostics when there is a threshold violation on relevant metrics. Thresholds (on CIs) are set in HP Diagnostics. Metric-based health indicators and KPIs use business rules to calculate status based on the data samples sent from Diagnostics.	The threshold violation event data is sent to BSM using the OM agent and IAPA components installed with the Diagnostics Commander Server.	"Integrations" in the *HP Diagnostics User's Guide/Online Help*

♣ NetScout and Third Party Applications

This section describes the different integrations between BSM and third party applications and points to the relevant documentation for details.

This section describes the following topics:

➤ "NetScout nGenius" on page 318

➤ "About BSM Integrations with Third-Party Applications" on page 319

NetScout nGenius

The integration between BSM and NetScout nGenius provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
NetScout alarms -> KPIs and HIs in BSM Service Health. Packets of data about applications running through specific switches and routers are analyzed by NetScout nGenius. Alarms about problems in these applications are send by NetScout to BSM using the SiteScope NetScout Event monitor and are displayed in the NetScout view in Service Health. The NetScout EMS integration creates the appropriate topology in RTSM, and the relevant view in Service Health. The NetScout view includes CIs that represent the application alarms.	The SiteScope NetScout Event monitor.	"NetScout nGenius Integration" on page 455
BSM Service Health -> NetScout - drilldown. You can drill down from Service Health to NetScout application, from the NetScout View, to display detailed information about the problem.	Right-click menu options.	"NetScout nGenius Integration" on page 455

About BSM Integrations with Third-Party Applications

Note: For best practices on integrating third-party data with BSM applications and the integration type to use, see the "Best Practices for Integrating Third-Party Data" on page 387.

The integration between BSM and third-party applications provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
Third-party data -> BSM metrics, events, topology, and health indicators. The custom EMS integration of third-party applications with BSM uses the SiteScope Technology Integration monitors to bring topology, metrics, and events from the third-party EMS data sources. Third-party data is mapped to health indicators. The health indicators and KPIs use business rules to calculate the status of the relevant CI in applications such as Service Health and Service Level Management. The data is displayed in related views in Service Health, Service Level Management, and System Availability Management reports.	The SiteScope Technology Integration monitors.	"EMS Integration Administration" on page 421
Third-party data -> Operations Management events and health indicators. If the user has an Event Management Foundation license, third-party sources (for example Microsoft System Center Operations Manager (SCOM), Oracle Enterprise Manager, or other products) use the BSM Integration Adapter to configure policies that enable sending events to Operations Management and managing these events in the Event Browser. If the third-party events are mapped to event type indicators, the corresponding health indicators, and KPIs affect the status of the relevant CIs in applications such as Service Health and Service Level Management.	The BSM Integration Adapter.	"HP BSM Integration Adapter" on page 407

🦠 HP Universal CMDB

The integration between BSM and HP Universal CMDB provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
BSM <-> HP Universal CMDB - Topology exchange. BSM integrates with HP Universal CMDB to enable sharing topologies (CIs and relationships) between instances and enabling a consistent CI ID in an environment. This feature is necessary for the integration and for resolving reconciliation issues. For more details, see item 328 in the Integrations Catalog, at http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=328.	Uses the Configuration Management System (CMS) topology. A single RTSM instance is configured to be the CMS and the global ID generator. Synchronization is achieved using the topology sync two options: pull and push.	"Integrating Multiple CMDBs" in *RTSM Data Flow Management Guide* "Topology Synchronization" in *Using Operations Management* RTSM Best Practices PDF

🔵 BSM - BSM

The integration between BSM and BSM provides the following capabilities:

What the Integration Gives You	How the Integration Works	Where to Get the Details
BSM events <-> BSM events. Exchange of events between the BSMs.	Event synchronization from domains to BSM. Event synchronization between the tiers. Topology synchronization between the BSMs.	"Integrating Multiple CMDBs" in *RTSM Data Flow Management Guide* "Topology Synchronization" in *Using Operations Management*

8

Configure Operations Management Connections

This chapter includes:

Concepts

Tasks

Concepts

🔹 Configure Operations Management Connections - Overview

HP Operations Manager (HPOM), can be integrated into your BSM environment becoming a data source for BSM Operations Management. Both HP Operations Manager for Windows and HP Operations Manager for UNIX (HP-UX and Linux) are supported (See the BSM 9.10 *Readme* for supported versions and required patches).

Note: Patch levels can change. Refer to http://support.openview.hp.com/ to ensure that the HPOM management server has all the latest patches.

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

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

Tasks

🔧 How to Configure Operations Management Connections

This task describes how to configure Operations Management connections

This task includes the following steps:

1 Set up the HPOM Management Server system as a Connected Server

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

For task details, see "How to Create a Connection to an HPOM Server" in in *Using Operations Management*.

2 Establish a Trust relationship between BSM and external servers

For connection and communication between BSM and external servers such as:

➤ HPOM hosts

➤ other BSM hosts where Operations Management is running

➤ Load Balancers

➤ BSM 9.x Server with an event channel license

establish a trust relationship between the various servers.

For task details, see "How to Establish a Trust Relationship between BSM and External Servers" on page 327.

To verify the trusted relationship, see "How to Verify the Trusted Relationship Between the BSM Processing Server and an External Server" on page 330.

3 Configure the HPOM forwarding policy

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

➤ **HPOM for Windows.** For task details, see "How to Configure the HPOM for Windows Forwarding Policy" on page 331.

➤ **HPOM for UNIX.** For task details, see "How to Configure the HPOM for UNIX Forwarding Policy" on page 335 .

4 Import content packs

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

For task details, see "How to Import Content Packs" on page 339.

5 Validate event synchronization

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

For task details, see "How to Validate Event Synchronization" on page 341.

6 Limit the number of CIs that BSM evaluates (optional)

The fewer CIs that the CI Resolver has to process, the better performance you will experience with Operations Management.

For task details, see "How to Limit the Number of CIs Used by CI Resolution" in *Using Operations Management*.

7 Synchronize the topology

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

For task details, see "How to Run Dynamic Topology Synchronization" and "How to Run Basic Topology Synchronization" in *Using Operations Management*.

🔓 How to Establish a Trust Relationship between BSM and External Servers

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

When establishing a trust relationship between BSM and HPOM, the BSM processing server should serve as the certificate server for all BSM gateway servers.

Note: If you have a "typical" BSM installation (Data Processing Server and Gateway Server installed on the same system), execute all steps for the Data Processing Server on this common BSM system.

Note: If an HPOM agent is already installed on the server where BSM is later installed, the BSM installation overwrites the agent's certificate store. In this case, you must establish a new trust relationship between the BSM processing servers and the HPOM management server.

To establish a trust relationship between the Data Processing Servers and external servers, complete the following steps:

1 On the BSM Data Processing Server, execute the following command:

 ovcert -exporttrusted -file omi.cert -ovrg server

2 On the external system, execute the following command:

 ovcert -exporttrusted -file other.cert -ovrg server

3 Copy **other.cert** from the external system to the BSM Data Processing Server.

4 Copy **omi.cert** from the BSM Data Processing Server to the external server.

5 On the BSM Data Processing Server, execute the following commands:

 ovcert -importtrusted -file other.cert

 ovcert -importtrusted -file other.cert -ovrg server

6 On the external server, execute the following commands:

 ovcert -importtrusted -file omi.cert

 ovcert -importtrusted -file omi.cert -ovrg server

7 If an HPOM agent was installed on the system before the BSM server was installed, execute the following command on all Gateway servers:

<HPBSM_install_dir>/bin/setup-secure-communication.bat <BSM processing server>

Default location:

Windows: C:\HPBSM\bin\setup-secure-communication.bat

Linux:/opt/HP/BSM/bin/setup-secure-communication.bat

Tip: If you are not sure whether the agent was installed first, use the command **ovconfchtg -edit** to check the **hp.XplConfig.ovconfchg** file. If **sec.cm.client.certificate_server** is set to the HPOM Management Server, then the agent was not installed first.

---

8 If you have a multi-server deployment, execute the following command on all Gateway Servers:

ovcert -updatetrusted

Note: During deployment, certificates for Gateway Servers are requested and granted for each Gateway Server. For details, see the *HP Business Service Management Deployment Guide* PDF.

---

9 If you are using a virtual interface for server pooling, where your data sources are not communicating directly with the BSM Gateway Server, perform the following task.

a Request server and client certificates from your Certificate Authority for the virtual interface.

If you do not have a Certificate Authority, you can issue a certificate from the BSM Data Processing server with the following command:

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

      b Import these certificates to the virtual interface.

🎋 How to Verify the Trusted Relationship Between the BSM Processing Server and an External Server

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

To check the connection between the BSM Processing Server and an external server, complete the following steps:

1 From the external host, verify that communication to the BSM installation is possible (the return value should be eServiceOk) by executing the following command on the Gateway Server for single Gateway Server deployments or the Load Balancer for multiple Gateway Server deployments:
bbcutil -ping https://<man-in-the-middle or single_gateway_server>

Example of the command result:

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

2 From the HP BSM Processing Server host, verify that communication with the external server host is possible (the return value should be eServiceOk) by executing the following command:
bbcutil -ping https://<external server hostname>

Example of the command result:

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

🪁 How to Set Up the HPOM Management Server as a Connected Server

Setup the HPOM management server system as connected server so that you can run actions and tools from Operations Management, and retrieve instructions from the HPOM management server. For details, see "How to Create a Connection to an HPOM Server" in *Using Operations Management*.

🪁 How to Configure the HPOM for Windows Forwarding Policy

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

Before setting up a policy and to avoid overwriting the current settings, verify whether a policy of the type **Server-based Flexible Management** is already active on the HPOM for Windows server. If a policy does not exist, create a new policy as described in the section "Create a New Policy (New Installation Only)" on page 331. If a policy already exists and is active, adapt the policy as described in the section "Adapt an Active Policy" on page 333.

Create a New Policy (New Installation Only)

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

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

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

3 Verify that no Server-based Flexible Management policy exists. If such a policy does exist, go to "Adapt an Active Policy" on page 333.

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

The Server-based Flexible Management Editor dialog opens.

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

```
TIMETEMPLATES
# none

RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
  SECONDARYMANAGERS
  ACTIONALLOWMANAGERS

  MSGTARGETRULES
    MSGTARGETRULE DESCRIPTION "Forward all messages rule"
      MSGTARGETRULECONDS
      MSGTARGETRULECOND DESCRIPTION "Forward all messages"

      MSGTARGETMANAGERS
        MSGTARGETMANAGER
        TIMETEMPLATE "$OPC_ALWAYS"
        OPCMGR IP 0.0.0.0 "<HP BSM 9.00 fully qualified host name>"
```

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

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

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

For details about load balancing and high availability, see "High Availability for HP Business Service Management" in the *HP Business Service Management Deployment Guide* PDF.

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

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

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

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

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

All Tasks > **Deploy on**

The Deploy server policy on dialog box opens.

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

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

Adapt an Active Policy

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

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

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

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

If such a policy does not exist, go to "Create a New Policy (New Installation Only)" on page 331.

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

```
TIMETEMPLATES
# none

RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
  SECONDARYMANAGERS
  ACTIONALLOWMANAGERS

  MSGTARGETRULES
    MSGTARGETRULE DESCRIPTION "Forward all messages rule"
      MSGTARGETRULECONDS
      MSGTARGETRULECOND DESCRIPTION "Forward all messages"

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

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

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

---

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

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

For details about load balancing and high availability, see "High Availability for HP Business Service Management" in the *HP Business Service Management Deployment Guide* PDF.

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

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

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

🔨 How to Configure the HPOM for UNIX Forwarding Policy

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

Before setting up a policy and to avoid overwriting the current settings, verify whether the **msgforw** message forwarding policy is already active on the HPOM server. If the **msgforw** message forwarding policy does not exist, create a new policy as described in the section "Create a New Policy (New Installation Only)" on page 335. If the **msgforw** message forwarding policy already exists and is active, adapt the policy as described in the section "Adapt an Active Policy" on page 337.

Create a New Policy (New Installation Only)

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

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

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

---

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

3 Insert the following text in new policy file:

```
TIMETEMPLATES
# none

RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
  SECONDARYMANAGERS
  ACTIONALLOWMANAGERS

  MSGTARGETRULES
    MSGTARGETRULE DESCRIPTION "Forward all messages rule"
      MSGTARGETRULECONDS
      MSGTARGETRULECOND DESCRIPTION "Forward all messages"

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

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

---

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

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

For details about load balancing and high availability, see "High Availability for HP Business Service Management" in the *HP Business Service Management Deployment Guide* PDF.

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

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

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

7 Restart the server processes as follows:

/opt/OV/bin/OpC/opcsv -stop

/opt/OV/bin/OpC/opcsv -start

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

Adapt an Active Policy

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

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

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

---

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

vi <policy file name>

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

```
TIMETEMPLATES
# none

RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Forward all messages to OMi"
  SECONDARYMANAGERS
  ACTIONALLOWMANAGERS

  MSGTARGETRULES
    MSGTARGETRULE DESCRIPTION "Forward all messages rule"
      MSGTARGETRULECONDS
      MSGTARGETRULECOND DESCRIPTION "Forward all messages"

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

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

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

---

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

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

For details about load balancing and high availability, see "High Availability for HP Business Service Management" in the *HP Business Service Management Deployment Guide* PDF.

5 Enter the following command to check for syntax errors in the new policy text:

/opt/OV/bin/OpC/opcmomchk -msgforw <policy file name>

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

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

7 Restart the server processes as follows:

/opt/OV/bin/OpC/opcsv -stop

/opt/OV/bin/OpC/opcsv -start

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

🔧 How to Import Content Packs

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

Note: Content packs delivered with BSM are usually automatically imported from the default directory during installation and on every BSM startup.

Any package that has not already been loaded, and which does not have unresolved package dependencies (references to packages, which are neither already loaded nor in the same folder), is loaded during this startup.

For details, see the *HP Business Service Management Deployment Guide* PDF.

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

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

To import content packs, complete the following steps:

Note: To load all content packs delivered with BSM, you can use the following command line tool on the Gateway Server: **<HPBSM>\bin\bsm_content_packs_install.bat**

If you want to load the content packs individually, use the steps described in this section.

---

1 On a Gateway Server, log onto BSM and open the Content Manager: **Admin** > **Platform** > **Content Manager**.

2 In the Content Pack Definitions toolbar, click **Import a Content Pack**.

3 From the Import Content Pack dialog, browse to the location of the content packs (default location on the Gateway Server: **<HPBSM_install_dir>\conf\opr\content\en_US**

4 Select a content pack (for example, MM-INF.xml) and click **Open**.

5 To import the content pack, select an appropriate option and click **Import**.

The Information dialog window appears showing you the number of artifacts (for example, health indicator definition artifacts) that you have imported.

6 Click **OK** to close the Information dialog.

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

⚓ How to Validate Event Synchronization

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

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

Verify Message Forwarding from HPOM to Operations Management

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

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

1 Make sure the BSM servers are running.

2 Make sure at least one open message interface policy is deployed on your HPOM system. For instructions and details, see the *HP Operations Manager* documentation.

3 On the HPOM system, open a command or a shell prompt and create a new message by executing the following command:

Windows:

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

UNIX:

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

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

Note: If the message is sent multiple times, no new message is generated by HPOM. These messages are regarded as duplicates and only the message duplicate count is increased.

To generate a new message, modify the message text for example as follows:

UNIX:

/opt/OV/bin/OpC/opcmsg a=App o=Obj msg_text="Hello_002"

Windows:

opcmsg a=App o=Obj msg_text="Hello_002"

Synchronize Operations Management Events with HPOM Messages

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

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

1 Make sure the BSM platform is running.

2 Log on to the BSM platform management console.

3 Select **Applications** > **Operations Management**.

4 In the Event Browser, select the event for which you want to change the severity. Choose an event that has been synchronized in HPOM and in BSM earlier and change its severity, for example, from minor to major.

5 In the General tab of the Event Details pane, click **Edit**.

6 From the Severity drop-down list, choose another severity (for example, major) and click **Save** to change it to the selected severity.

7 In HPOM event browser, verify the severity of this event and make sure it has been set to the new severity value.

🔧 How to Manage a BSM Host System with HPOM for UNIX or Linux

To install an HPOM Agent installation on a system where BSM is installed:

1 Exchange certificates between the HPOM and BSM host systems. For details, see How to Establish a Trust Relationship between BSM and External Servers.

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

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

---

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

opcnode -add_node <BSM Server>

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

opcnode -chg_id node_name=<BSM Server> id=<core ID of BSM Server>

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

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

6 Validate the agent installation with the command:

opcragt -status <BSM Server hostname>

The following information should be displayed:

Control Agent /opt/OV/bin/OpC/opcctla (7052) is running
Message Agent /opt/OV/bin/OpC/opcmsga (7059) is running
BBC Local Location Broker /opt/OV/bin/llbserver (7060) is running
Subagent 12:
Performance Agent /opt/OV/bin/coda -redirect (7062) is running

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

🔨 How to Manage a BSM Host System with HPOM for Windows

To install an HPOM Agent installation on a system where BSM is installed:

1 Exchange certificates between the HPOM and BSM host systems. For details, see How to Establish a Trust Relationship between BSM and External Servers.

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

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

---

3 Synchronize packages on the BSM node.

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

All Tasks > **Synchronize inventory** > **Packages**

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

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

opcragt -status <BSM_Server>

The output should indicate that the agent is running.

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

9

Generate Events in HP Operations Manager when BSM Alert is Triggered

This chapter includes:

Concepts

➤ Generating Events in HP Operations Manager when BSM Alert is Triggered Overview on page 348

Tasks

➤ How to Configure BSM Alerts to Forward an Event When the Alert is Triggered on page 349

Concepts

⚙ Generating Events in HP Operations Manager when BSM Alert is Triggered Overview

You can configure specific CI Status alerts, SLA alerts, or EUM alerts to automatically forward a corresponding event through the Event Channel to HP Operations Manager or Operations Management or to other applications to proactively alert the operator about a problem in the system. The alerts are mapped to the events using the Event Template.

For general details about the integration of BSM with other applications, see "Business Service Management Integration with Other Applications Overview" on page 294.

For task details, see "How to Configure BSM Alerts to Forward an Event When the Alert is Triggered" on page 349.

Tasks

🔧 How to Configure BSM Alerts to Forward an Event When the Alert is Triggered

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

For concept details, see "Generating Events in HP Operations Manager when BSM Alert is Triggered Overview" on page 348.

This task includes the following steps:

➤ "Enable a CI Status Alert to be Sent as an Event" on page 349

➤ "Enable an SLA Alert to be Sent as an Event" on page 350

➤ "Enable an EUM Alert to be Sent as an Event" on page 350

Enable a CI Status Alert to be Sent as an Event

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

1 Select **Admin > Service Health > View Management > CI Status Alerts**, select a view and a CI and click **New Alert** or select an existing alert and click **Edit**.

2 In the Actions page, click the **New Event Generation** link in the **Generate Events** section.

3 In the **CI Alert Template Repository** dialog box that opens, select the template you want to use to map the alert to an event and click **Select**. The template you selected is now listed in the Generate Events section. For user interface details, see "CI Status Template Repository Dialog Box" in *Using Service Health*.

Enable an SLA Alert to be Sent as an Event

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

1 Select **Admin > Service Level Management > SLA Alerts**, click **New Alert** or select an existing alert and click **Edit**.

2 In the Actions page, click the **New Event Generation** link in the **Generate Events** section.

3 In the **SLA Template Repository** dialog box that opens, select the template you want to use to map the alert to an event and click **Select**. The template you selected is now listed in the **Generate Events** section. For details, see "Event Template for SLA Alerts" in *Using Service Level Management*.

Enable an EUM Alert to be Sent as an Event

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

1 Select **Admin > End User Management > Monitoring**, select the view and the CI in the left pane, click the **Alerts** tab, and click the **Press to create new alert** 🔆 button, or select one of the alerts, and click the **Press to edit alert** 🖉 button.

2 In the Actions page, select the **Generate Event** option. For user interface details, see "Actions Tab" in *Using End User Management*.

3 In the Definition Details area, in the Actions section, click the first link in the **Generate events with** <template name> **template and** <value> **values Event Type Indicator**, to select or modify the default template that maps the alert to the event in the Template Repository dialog box. For user interface details, see "Template Repository Dialog Box" in *Using End User Management*.

4 Click the second link to open the Event Type Indicator dialog box, where you specify the ETI that corresponds to the alert. For user interface details, see "Event Type Indicator Dialog Box" in *Using End User Management*.

10

How to Integrate HP Service Manager with Business Service Management Components

This chapter redirects you to the **HP Service Manager Integration with BSM Components** document that is only available online because of the interactive nature of the document.

To access the document, open the main page of the BSM online documentation library (available from the BSM application), locate the Solutions and Integration column (on the right) and click the HP Service Manager Integration link. The interactive document is also available from the documentation update site located at http://h20230.www2.hp.com/selfsolve/manuals.

11

Integrate Network Node Manager i (NNMi) with BSM

This chapter includes:

Concepts

➤ Integrate NNMi with BSM – Overview on page 354

Tasks

➤ How to Integrate NNMi with BSM on page 355

Concepts

✿ Integrate NNMi with BSM – Overview

You can integrate Network Node Manager i with BSM to provide the following capabilities:

➤ The display of NNMi events in the Event Browser in Operations Management.

➤ NNMi events have corresponding out-of-the-box health indicators, the health indicators affect the status of the Network CIs in applications such as Service Health and Service Level Management. The integration also provides the relevant out-of-the-box KPIs for Network CIs.

➤ The populating of the BSM Run-time Service Model (RTSM) with the NNMi topology. BSM stores each device in the NNMi topology as a Configuration Item (CI).

➤ The capability to drill down from various EUM reports, MyBSM, and other locations, to NNMi where you can display trace route information between the client and the destination machine.

➤ The capability to connect to the NNMi Management server and further analyze incoming events in NNMi.

For details, see "Network Node Manager i (NNMi)" on page 295.

Tasks

🔧 How to Integrate NNMi with BSM

This task describes how to integrate NNMi with BSM.

Note: Before performing this integration, read the information located in the HP NNMi – HP BSM Topology Integration Best Practices PDF.

This task includes the following steps:

➤ "Prerequisite" on page 355
➤ "Perform the integration in NNMi" on page 356
➤ "Configure LW-SSO in both BSM and NNMi" on page 356
➤ "Connect NNMi to another BSM instance" on page 356
➤ "Configure BSM to display NNMi data" on page 357
➤ "Results" on page 357

1 Prerequisite

Make sure you have the BSM and NNMi licenses installed. For details, see "License Management Overview" in *Platform Administration*.

2 **Perform the integration in NNMi**

a Connect to the RTSM. For details, see "HP Business Service Management Topology" in the *NNMi Deployment Reference* available in the NNMi documentation library or at http://h20230.www2.hp.com/ selfsolve/manuals.

b Perform the steps needed to integrate NNMi with BSM in the NNMi application. For details, see "HP BSM Operations Management" in the *NNMi Deployment Reference* available in the NNMi documentation library or at http://h20230.www2.hp.com/selfsolve/manuals.

3 **Configure LW-SSO in both BSM and NNMi**

Make sure that LW-SSO is configured in both BSM and NNMi with the same init key. For details on how to configure the init key in BSM, see "Authentication Wizard" in *Platform Administration*. For details on how to configure the init key in NNMi, see "Using Single Sign-On with NNMi" in the *NNMi Deployment Reference* available in the NNMi documentation library or at http://h20230.www2.hp.com/selfsolve/manuals.

4 **Connect NNMi to another BSM instance**

As NNMi stores the RTSM IDs after the first run of the topology integration, the reconciliation works only partially on the RTSM, and the NNMi log files still include several reconciliation errors, which are caused by the non-existing RTSM IDs. To fix the problem, perform the following steps:

a Change the Integration to the new BSM system.

b Log on to the NNMi JMX console http://<**NNMi_fqdn_and_port**>/ **jmx-console** using the system account and password.

c Go to **mbean NnmBsmModule**.

d Run **java.lang.String resetNnmBsmIds()**.

You should see a list of devices from which the RTSM ID has been removed.

e Disable and enable the topology Integration to get the CIs into RTSM.

5 Configure BSM to display NNMi data

To display NNMi data in BSM and to access the NNMi components in MyBSM, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

a Select **Foundation**.

b Select **Integration with other applications**.

c In the **Integrations with other applications - HP NNM** table, locate and modify the following parameters:

➤ **HP NNM Integration URL.** The NNMi host and port number (protocol://host:port/nnm).

➤ **HP NNM User name.** The user name that is used for log on to NNMi.

➤ **HP NNM User password.** The user password that is used for log on to NNMi.

6 Results

If the NNMi events have corresponding health indicators, the health indicators affect the status of the relevant CIs in applications such as Service Health and Service Level Management.

12

HP Operations Orchestration Integration

This chapter includes:

Concepts

➤ HP Operations Orchestration Integration Overview on page 360

Tasks

➤ How to Integrate BSM and OO on page 361

➤ How to Integrate BSM and HP Operations Orchestration – Use-Case Scenarios on page 369

Reference

➤ Predefined Mappings on page 371

➤ HP Operations Orchestration Integration User Interface on page 372

Concepts

🎱 HP Operations Orchestration Integration Overview

HP Operations Orchestration (OO) provides a simple way for customers to run scripts for automatic actions. The integration with Business Service Management (BSM) uses the OO capabilities for building investigation tools or service remediation scripts, providing the operators with a simple way to validate a problem, investigate it, or automatically correct it. A run book can be executed manually.

For general details about the integration of BSM with other applications, see "Business Service Management Integration with Other Applications Overview" on page 294.

OO run books can be launched from the Service Health, and the Event Browser applications.

The integration of BSM and OO provides the capability of mapping CI types to OO run books.

After you create such mappings, you can run the mapped OO run books:

➤ On CIs using the right-click menu option in Service Health. For details, see "Invoke Run Books" in *Using Service Health*. The OO run book parameters are populated using the map to the CI attributes defined in the "Run Book Mapping Configuration Wizard" on page 374.

➤ At the event level in Operations Management. Operations Management opens an event and checks if the CI for this event has a run book assigned to it and if the run book is set to run automatically. The OO run book parameters are populated using the map to the CI or event attributes defined in the "Run Book Mapping Configuration Wizard" on page 374.

BSM provides a number of predefined mappings between CIs and OO run books. For details on this topic, see "Predefined Mappings" on page 371.

Tasks

🔨 How to Integrate BSM and OO

This task describes the working order required to integrate BSM and OO.

This task includes the following steps:

➤ "Prerequisites" on page 362

➤ "Configure the link between BSM and OO" on page 362

➤ "Configure Lightweight Single Sign-On (LW-SSO) authentication" on page 363

➤ "In Windows - export OO server certificates to BSM" on page 364

➤ "In Windows - import OO server certificates to BSM" on page 365

➤ "In Linux - export OO server certificates to BSM" on page 366

➤ "In Linux - import OO server certificates to BSM" on page 367

➤ "Grant permissions" on page 368

➤ "Map run books to CI Types" on page 369

➤ "Use OO functionality from BSM applications" on page 369

Note: Consult the relevant BSM_<version_number>_Release_Notes.pdf for details about the supported versions.

---

1 Prerequisites

Details about the supported versions of BSM and HP Operations Orchestration are provided in the BSM_<version_number>_Release_Notes.pdf document.

2 Configure the link between BSM and OO

To configure the integration between BSM and OO, in BSM select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Foundations**.

➤ Select **Integrations with other applications**.

➤ In the **HP Operation Orchestration** table, locate **Operation Orchestration application URL**. Modify the setting to the URL used to access the OO application. For example, https://<fully qualified server name>:8443.

➤ In the same table, locate **User Name.** Enter the OO log on user name and password used when invoking run books in an automatic way. The user must be defined in OO as an internal user. For example: bsm_oo_int_user.

3 Configure Lightweight Single Sign-On (LW-SSO) authentication

Configure Lightweight Single Sign-On (LW-SSO) authentication between BSM and OO. You must configure LW-SSO in both BSM and OO.

To configure LW-SSO:

a In BSM, select **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**, and copy the **Token Creation Key** (the initString) to OO, and replace, in OO, all the initStrings in the **lwssofmconf.xml** file located in the **<OO installation directory>\Program Files\Hewlett-Packard\Operations Orchestration\Central\conf** directory.

b In OO, in the **web.xml** and **applicationContext.xml** files located in the **<OO installation directory>\Program Files\Hewlett-Packard\ Operations Orchestration\Central\WEB-INF** directory, enable all filters and mappings between **LWSSO_SECTION_BEGIN** and **LWSSO_SECTION_END**.

c In OO, in the **<OO installation directory>\jetty\resources\log4j.properties** file, uncomment the linethat appears under the LWSSO comment.

d Restart the following OO services: **RSCentral**, **RSJRAS**, and **RSScheduler**.

e If OO and BSM are in different domains in the Windows operating system, you must make sure that the **Trusted Hosts/Domains** parameter is the same in OO and BSM. To set the parameter in BSM, select **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**, and configure the **Trusted Hosts/Domains** parameter.

For details on configuring LW-SSO in BSM, see "Authentication Strategy Page" in *Platform Administration*.

4 **In Windows - export OO server certificates to BSM**

To export server certificates from OO and import them into BSM in a Windows environment, you use the **keytool** utility, which is included in Sun JRE, to export and import certificates.

a **Export the OO Server Certificate.** To export the OO server certificate, on the OO server enter:
C:\> "%JAVA_HOME%\jre\bin\keytool" -keystore "%ICONCLUDE_HOME%\Central\conf\rc_keystore" -export -alias pas -file "C:\ <Operations Orchestration server fully qualified host name>.cer"

b When prompted for passwords enter: bran507025.

Tip: If your **%JAVA_HOME%** environment variable points to the JRE directory instead of the JDK directory, remove **jre** from the keystore path (C:\> "%JAVA_HOME%\bin\keytool" -keystore) in the command.

---

5 In Windows - import OO server certificates to BSM

Import the server certificate from the OO server to the BSM Gateway
Server so that the two systems can communicate with each other securely.

Tip: If your **%JAVA_HOME%** environment variable points to the JRE
directory instead of the JDK directory, remove **jre** from the keystore path
(C:\> **"%JAVA_HOME%\bin\keytool" -keystore**) in the commands.

---

a **Import the Server Certificate to BSM.** To import the server certificate
you exported from OO to the BSM cacerts keystores, on the BSM
Gateway Server enter:

➤ **C:\> "%JAVA_HOME%\jre\bin\keytool" -keystore
"%TOPAZ_HOME%\JRE\lib\security\cacerts" -import -alias
"<Operations Orchestration fully qualified host name>" -file
"<Operations Orchestration fully qualified host name>.cer"**

➤ **C:\> "%JAVA_HOME%\jre\bin\keytool" -keystore
"%TOPAZ_HOME%\JRE64\lib\security\cacerts" -import -alias
"<Operations Orchestration fully qualified host name>" -file
"<Operations Orchestration fully qualified host name>.cer"**

b When prompted for password enter: changeit.

Note: If JAVA_HOME is not set, use TOPAZ_HOME.

---

c In order to prevent a certificate error, place this certificate into the
Trusted Root Certificate Authorities on any browser that will be
accessing BSM as follows:

➤ Click the **Install certificate** button to start the wizard.

➤ Click **Next**.

➤ Select the **Place all certificates in the following store** radio button.

➤ Click **Browse.**

➤ Select **Trusted root certification authorities**.

➤ Click **Next**.

➤ Click **Finish**.

d Restart BSM on the Gateway server.

6 **In Linux - export OO server certificates to BSM**

To export server certificates from HP Operations Orchestration (OO) and import them into BSM in a Solaris environment, you use the **keytool** utility, which is included in the Sun Solaris **opt/HP/BSM/JRE64/bin/ keytool** directory, to export and import certificates.

a To export the OO server certificate, on the OO server enter:
Keytool -keystore "$ICONCLUDE_HOME/Central/conf/rc_keystore" -export -alias pas -file "<Operations Orchestration fully qualified host name>.cer"

b When prompted for passwords enter: bran507025.

7 In Linux - import OO server certificates to BSM

Import the server certificate from the OO server to the BSM Gateway Server so that the two systems can communicate with each other securely.

a **Import the Server Certificate to BSM.** To import the server certificate you exported from OO to the BSM cacerts keystores, on the BSM Gateway Server, go to **$TOPAZ_HOME/jre/bin** and enter the following commands:

Note: If TOPAZ_HOME is not set, use the following script: **/opt/HP/BSM/scripts/topaz_env.sh**

➤ **keytool -keystore "$TOPAZ_HOME/JRE/lib/security/cacerts" -import -alias "<Operations Orchestration fully qualified host name>" -file "<Operations Orchestration fully qualified host name>.cer"**

➤ **keytool -keystore "$TOPAZ_HOME/JRE64/lib/security/cacerts" -import -alias "<Operations Orchestration fully qualified host name>" -file "<Operations Orchestration fully qualified host name>.cer"**

b When prompted for password enter: changeit.

c In order to prevent a certificate error, place this certificate into the Trusted Root Certificate Authorities on any browser that will be accessing BSM as follows:

➤ Click the **Install certificate** button to start the wizard.

➤ Click **Next**.

➤ Select the **Place all certificates in the following store** radio button.

➤ Click **Browse.**

➤ Select **Trusted root certification authorities**.

➤ Click **Next**.

➤ Click **Finish**.

d Restart BSM on the Gateway server.

8 **Grant permissions**

Grant administrator permissions so that users can create, view, and modify the mapping between BSM CI types and OO run books, and invoke OO run books from BSM.

To integrate with OO, you must set up users with specific permissions. Select **Admin** > **Platform** > **Users and Permissions**, select the user or create a new user and select the **Operations Orchestration Integration** context. For details on this topic, see "Permissions Overview" in *Platform Administration*.

➤ To enable a BSM user to start runbooks, the operator, for example, Bob, must have the same user name in BSM and in OO.

➤ If the user is only used in BSM and does not need to automatically launch OO flows, the user must be defined in OO as **external**. If the BSM user also needs to automatically launch OO flows, it must be defined in OO as **internal**.

➤ Both **internal** and **external** users must have the following capabilities in OO: AUTHOR, SCHEDULE, RUN_REPORTS, and HEADLESS_FLOWS. You can either add the users to groups with these capabilities (for example, the administrator group has these capabilities) or you can create such a group.

➤ In BSM, the user must have the Execution right in the Operations Orchestration context

➤ To enable a BSM user to configure runbook-CI type mappings, you have to setup the following:

    ➤ In BSM, give the user the Administration right in the Operations Orchestration context.

    ➤ Setup the same integration user in OO (for example, BSMOO_integr_user) and in the RTSM.

9 Map run books to CI Types

You can map OO run book parameters to:

➤ CI type attributes. For details on the user interface, see "Run Books Configuration Page" on page 372.

The child CIs of a CI, for which you configure a run book, are also assigned that run book.

➤ The Operations Management event attributes are pre-defined in Operations Management. For details, see Operations Management documentation.

10 Use OO functionality from BSM applications

You can trigger a run book from:

➤ HPOM. For details, see HPOM documentation.

➤ From Service Health using the **Invoke Run Books** context menu option. For details, see "Service Health Menu Options" in *Using Service Health*.

➤ From Event browser using the context menu or from the Action panel.

🦮 How to Integrate BSM and HP Operations Orchestration – Use-Case Scenarios

This section describes two possible scenarios to integrate BSM and HP Operations Orchestration (OO).

Use-Case Scenario in Service Health

In OO, the Restart a Node run book is associated with a Node CI Type. The parameters of the run book are mapped to the relevant CI attributes of the Node CI.

In Service Health, the operator detects that a host has a system problem. The operator right-clicks the CI to get a list of the run books relevant to the CI. One of the run books is Restart a Node. The run book can execute automatically because the values of the parameters, such as host name/IP are automatically populated by data taken from the CI context.

Use-Case Scenario in Operations Management

In the Operations Management Event Browser, the operator is going through his assigned events. The operator detects an event related to a lack of disk space that causes a database performance issue. From the event context the operator can get a list of relevant run books. The operator can launch the appropriate run book, manually. The run-book continue running without further input from the operator as all run book parameters are extracted from the event or related CI.

Reference

🔧 Predefined Mappings

BSM provides a number of predefined mappings between CI types and HP Operations Orchestration (OO) run books. The following table lists the CI types and the OO run books that are mapped to them:

BSM CI Type	HP Operations Orchestration Run Books
IIS	Soft Reset IIS
Weblogic AS	Restart Server
Websphere AS	Restart Server
Windows	Restart Windows Server, Restart Windows Server with Wait, Start Automatic Services

Tip: In the predefined mapping, the Restart Server run book runs successfully only for Weblogic and Websphere applications that are discovered by Data Flow Management. For Weblogic and Websphere applications discovered by SiteScope, application credentials are not reported and the run book is unable to run successfully, unless you manually configure the credentials as default parameters in the Run Book Mapping Configuration wizard, manually change them for a specific invocation of a run book, or enter them when prompted during a run book invocation. For details on the Run Book Mapping Configuration wizard user interface, see "Configure Parameters Page" on page 377.

🔖 HP Operations Orchestration Integration User Interface

This section describes:

➤ Run Books Configuration Page on page 372

➤ Run Book Mapping Configuration Wizard on page 374

➤ Select Topology Dialog Box on page 379

🔖 Run Books Configuration Page

This page displays the mappings between BSM CI types and HP Operations Orchestration (OO) run books, and enables you to create new mappings or edit existing ones.

To access	Admin > Integrations > Operations Orchestration tab
Important information	➤ To work with OO from BSM, the two systems must be integrated. For details on how to perform this task, see "How to Integrate BSM and HP Operations Orchestration – Use-Case Scenarios" on page 369. ➤ Click a row in the table to select an existing mapping for editing or deletion. ➤ BSM provides a number of predefined mappings between CIs and OO run books. For details on this topic, see "Predefined Mappings" on page 371.
Relevant tasks	"How to Integrate BSM and HP Operations Orchestration – Use-Case Scenarios" on page 369

User interface elements are described below:

UI Element (A-Z)	Description
✳	**New.** Opens the **Run Book Mapping Configuration** wizard, where you configure the mapping between a CI type and OO run books. For details on the user interface, see "Run Book Mapping Configuration Wizard" on page 374.
✏	**Edit.** Opens the **Select CI Type** page of the **Run Book Mapping Configuration** wizard where you can edit the selected mapping. For details on the user interface, see "Select CI Type Page" on page 375.
✖	**Delete.** Delete the selected mapping.
CI Type	Displays the CI types to which OO run books are already mapped.
Operation Orchestration Flows	Displays the OO run books that are mapped to each CI type.

🔍 **Run Book Mapping Configuration Wizard**

This wizard enables you to create mappings of CI Type attributes, event attributes, or both and HP Operations Orchestration (OO) run book parameters.

To access	Use one of the following: ➤ To create a new mapping, select **Admin** > **Integrations** > **Operations Orchestration** tab, and click the **New** 🌟 button. ➤ To edit an existing mapping, select **Admin** > **Integrations** > **Operations Orchestration** tab, select the existing mapping, and click the **Edit** 🖊 button.

Important information	➤ The child CIs of a CI, for which you configure a run book, are also assigned that run book.
	➤ When using the Run Book Mapping Configuration wizard to edit a previously configured mapping:
	  ➤ The Welcome and Summary pages of the wizard are not displayed.
	  ➤ You do not have to access the wizard pages in a specific order. Click a wizard page name on the left to go directly to that page.
	  ➤ From any of the wizard pages, click the **OK** button to save the mapping configuration and exit the wizard.
	➤ The Welcome and Summary pages are displayed only when you create a new run book mapping.

Relevant tasks	"How to Integrate BSM and HP Operations Orchestration – Use-Case Scenarios" on page 369
Wizard map	The Run Book Mapping Configuration Wizard contains: Welcome Page > Select CI Type Page > Select Run Books Page > Configure Parameters Page > Summary Page

🔍 Select CI Type Page

This page enables you to select a CI type to which to map HP Operations Orchestration (OO) run books.

Important Information	General information about the wizard is available at "Run Book Mapping Configuration Wizard" on page 374.
Wizard map	The Run Book Mapping Configuration Wizard contains:
	Welcome Page > **Select CI Type Page** > Select Run Books Page > Configure Parameters Page > Summary Page

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<CI type tree>	Displays a list of CI types from which you select the required CI type to which to map OO run books. Click a CI type to select it.
	Note:
	➤ CI types that already have run books mapped to them appear in the tree, but are disabled.
	➤ When you edit an existing mapping, only the configured CI type is displayed and you cannot edit it.
<Search string>	You can search for CI types with names containing a specific string that you enter in this field. Click the **Search** button to run the search. Only matching results are displayed in the tree.
	Note:
	➤ The search is not case sensitive.
	➤ You can use the asterisk (*****) wildcard in your string to match one or more words of text.
Clear	Click to clear the current search string and display all CI types.
Search	Click to display only CI types that match the search string.

🔍 Select Run Books Page

This page enables you to select the HP Operations Orchestration (OO) run books to map to the selected CI type.

Important information	General information about the wizard is available at "Run Book Mapping Configuration Wizard" on page 374.
Wizard map	The Run Book Mapping Configuration Wizard contains: Welcome Page > Select CI Type Page > **Select Run Books Page** > Configure Parameters Page > Summary Page

User interface elements are described below:

UI Element (A-Z)	Description
▷	**Select run book to map.** Adds the run book you selected in the Flow Library area to the list in the Selected Run Books area.
◁	**Remove run book from mapping.** Removes the run book you selected in the Selected Run Books area from the list and moves it back to the Flow Library area.
Flow Library	Displays a tree of the available run books in the OO flow library. Click a run book to select it.
Run Book Description	Displays the description of a selected run book.
Selected Run Books	Displays the run books you select for mapping to the CI type and their path in the OO flow library. Click a run book to select it for removal from the list. **Note:** ➤ A run book that is included in an existing mapping, but that is not found in OO, is denoted by the ⊗ icon. Remove the run book from the mapping. ➤ A run book included in an existing mapping that contains different parameters than those defined in the mapping (that is, additional or deleted parameters), is denoted by the ⓘ icon.

🔍 Configure Parameters Page

This page enables you to configure the settings and default values of the parameters used by the selected HP Operations Orchestration (OO) run books.

Important information	General information about the wizard is available at "Run Book Mapping Configuration Wizard" on page 374.
Wizard map	The Run Book Mapping Configuration Wizard contains:
	Welcome Page > Select CI Type Page > Select Run Books Page > **Configure Parameters Page** > Summary Page

User interface elements are described below:

UI Element (A-Z)	Description
CI	The default CI from the selected CI type topology to use as the source for the required run book parameter. Click the arrow to open a drop-down list of all the CIs included in the CI type topology. Select a different CI if required.
	Note: If there is no configured topology for the selected CI type, the CI corresponding to the selected CI type itself is the only available option.
CI Attribute	The default CI attribute, of the selected CI, to use as the source for the required run book parameter. Click the arrow to open a drop-down list of all the attributes for the selected CI. Select a different attribute if required.
Default Value	A default value to be used for the CI attribute, if required.
Enable to run automatically	Select the option when you want to automatically run the run book.
	Note: The run book runs automatically only when all the parameters listed in the Configure Parameters page have been assigned a value, and the run book runs without user intervention.

UI Element (A-Z)	Description
Event Attribute	The default event attributes for events that correspond to the selected CI type. The field automatically lists all the default event attributes and custom attributes that were defined in Operations Management. You can select one of the listed default event attributes or add your own.
	For details about the attributes, see Operations Management Online Help documentation.
Run Book/Parameter Name	A hierarchical list of the selected run books and the parameters they require.
	Note:
	➤ Only parameters that are configured as flow input parameters for run books are included. For example, a parameter that is included in an operation configured in a run book is not displayed and cannot be mapped.
	➤ Mandatory parameters for which settings are required are denoted by a red asterisk.
	➤ A parameter included in an existing mapping, but that is not found in a run book, is denoted by the icon.
	➤ A parameter found in a run book, but not included in an existing mapping, is denoted by the icon.
	➤ Additional and deleted parameters are automatically added to, or removed from the mapping when you click the **OK** button on the wizard page.
To choose an attribute that is not part of the selected CI click here	Click the link to open the **Select Topology** dialog box, where you can select a CI from a related CI topology to use as the source for the required run book parameter. For details on the user interface, see "Select Topology Dialog Box" on page 379.

🔦 Summary Page

This page summarizes the configuration of the mapping of the parameters used by the selected HP Operations Orchestration (OO) run books to the CI attributes or to the event attributes as well as the default values of the attributes.

Important information	General information about the wizard is available at "Run Book Mapping Configuration Wizard" on page 374.
	This page is displayed only when you create a new run book mapping.
Wizard map	The Run Book Mapping Configuration Wizard contains:
	Welcome Page > Select CI Type Page > Select Run Books Page > Configure Parameters Page > **Summary Page**

🔦 Select Topology Dialog Box

This dialog box enables you to select a different CI type or node CI from a topology related to the CI type selected in the **Run Book Mapping Configuration** wizard. This CI is used as the source for a required run book parameter for the CI type selected in the wizard.

To access	Click the **Select Related CIs** link in the **Configure Parameters** page in the **Run Book Mapping Configuration** wizard. For details on the user interface, see "Configure Parameters Page" on page 377.
See also	"Run Book Mapping Configuration Wizard" on page 374

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Topology map>	Displays a map of the selected CI topology.
Select the node to which the run books are mapped	Select a specific node from the selected topology to use as the source for a required run book parameter for the CI type selected in the **Run Book Mapping Configuration** wizard. Available nodes are those applicable for the CI type selected in the wizard, and their descendants.
Select topology	Select a topology from the drop-down list of topologies that are related to the CI type selected in the **Run Book Mapping Configuration** wizard. Related topologies are those topologies in the Run Book folder in Modeling Studio that include a node for the CI type selected in the wizard.
	Note:
	➤ Topology names in the Run Book folder in Modeling Studio cannot contain spaces.
	➤ You can create topologies using Query Manager (**Admin** > **RTSM Administration** > **Modeling** > **Modeling Studio**). For details on the user interface, see "Modeling Studio Page" in the *Modeling Guide*.

13

HP Diagnostics and HP Business Service Management Integration

This chapter includes:

Concepts

Tasks

Concepts

⚙ HP Diagnostics and HP Business Service Management Integration Overview

HP Diagnostics is a composite application triage and diagnostics solution that is designed to help you improve the performance of your J2EE, .NET, and ERP/CRM enterprise applications throughout the application lifecycle.

HP Diagnostics is integrated with BSM, enabling you to monitor the availability and performance of your production enterprise application. This integration enables you to significantly reduce the Mean Time To Resolution of problems and thus increase the availability and value of the business applications.

From within BSM, you can track the performance status of your applications that are being monitored by HP Diagnostics.

The Diagnostics integration with BSM enables you to drill down to Diagnostics data from specific BSM configuration items and reports. You can also generate high level reports in BSM about the performance of applications and Business Process Monitor (BPM) transactions that are monitored by Diagnostics.

For additional details about the integration, see "HP Diagnostics" on page 316.

Tasks

🔧 How to View HP Diagnostics Data in HP Business Service Management

To view HP Diagnostics data in HP Business Service Management, you must register the HP Diagnostics server machine in HP Business Service Management.

This task includes the following steps:

➤ "Register HP Diagnostics" on page 383

➤ "Set up BSM to work with Diagnostics" on page 384

➤ "View HP Diagnostics data in BSM" on page 384

➤ "Access HP Diagnostics from BSM" on page 384

1 Register HP Diagnostics

In BSM, select **Admin > Diagnostics**, to open the HP Diagnostics Server Details page. Enter the details of the server as follows:

➤ **Diagnostics server host name**. Enter the HP Diagnostics Server name.

Even when the Diagnostics Server is installed on the same system as BSM you must enter the actual name of the host in the box. Do not enter **localhost**.

➤ **Diagnostics server port number.** Accept the default port number (**2006**) or enter the port number through which HP Diagnostics listens to server traffic.

➤ **Diagnostics server protocol.** Select the communication protocol (HTTP or HTTPS) through which HP Business Service Management connects to HP Diagnostics.

If you select HTTPS, additional configuration steps are required. For details, see the *HP Diagnostics Installation and Configuration Guide*.

Click **Submit** to register the server with HP Business Service Management. The Diagnostics Server details are saved in BSM and BSM server details are automatically registered on the HP Diagnostics machine.

If the server name is incorrect or the server is unavailable, an error message is displayed.

If the user name with which you logged in does not have permissions for making changes on the HP Diagnostics server, a message is displayed instead of the HP Diagnostics page.

2 Set up BSM to work with Diagnostics

For help with the remainder of this procedure for registering the server, see the *HP Diagnostics Installation and Configuration Guide* (select **Help > Diagnostics HP Diagnostics Installation and Configuration Guide**).

3 View HP Diagnostics data in BSM

To view relevant Diagnostics information, select **Application > Service Health**, select the Diagnostics View in Model Explorer and click the appropriate tab.

For information about the HP Diagnostics data displayed in HP Business Service Management, see the *HP Diagnostics User's Guide* (select **Help > Diagnostics Help > HP Diagnostics User's Guide**).

4 Access HP Diagnostics from BSM

You can access HP Diagnostics from BSM using right-click options in views and drilldowns from some reports.

🔧 How to Access Online Help for HP Diagnostics in HP Business Service Management

Click **Help > Diagnostics Help** to access the online HP Diagnostics Documentation Library, for the Diagnostics application or for Diagnostics administration in BSM.

🔍 Troubleshooting and Limitations

This section describes troubleshooting and limitations for the integration of HP Diagnostics and BSM.

After connecting BSM to the HP Diagnostics server, a message is displayed: "Session does not exist."

Check that Internet Explorer is set up to enable the browser to submit cookies to the HP Diagnostics server:

1 In Internet Explorer (version 6.0), select **Tools** > **Internet Options** > **Privacy**.

2 In the Web Sites section, click the **Edit** button.

3 In the Per Site Privacy Actions dialog box, enter the HP Diagnostics server DNS domain name.

4 Click **Allow**, **OK**, and **OK**.

14

Best Practices for Integrating Third-Party Data

This chapter includes:

Concepts

➤ Third-Party Integration Overview on page 388

Reference

➤ Out-of-the Box Integrations on page 391

➤ Recommended Integration Points and Data Collectors on page 394

➤ Integration Options and Details on page 395

➤ Coexistence Procedure for SiteScope and the Integration Adapter on page 404

Concepts

⚙ Third-Party Integration Overview

Third-party data can be integrated with Business Service Management (BSM) for use with BSM applications. This section contains details of the prerequisites and best practices for integrating third-party data with BSM applications.

Before setting up the integration, you need to decide:

➤ The type of data to be collected. You can integrate events, metrics, and topology data in BSM.

➤ Where you want the data to be used. For a list of BSM applications that use third-party data, see "BSM Applications That Use Third-Party Data" on page 389.

There are various options to collect and use third-party data. You can use one of the out-of-the box integrations listed in "Out-of-the Box Integrations" on page 391. Alternatively, if you do not find the integration that you are looking for, you can choose the integration option according to the type of data to be collected and your integration needs.

The following integration tools are available, depending on your selection:

➤ Integration Adapter, using one of the policies: **XML** or **SNMP.**

➤ SiteScope using one of the generic Integration Monitors: **Database**, **Log**, **SNMP Trap**, **Web Service**.

➤ Both Integration Adapter policy and a SiteScope Integration Monitor.

The integration type depends on the method through which data can be acquired from a third-party system.

➤ **Remote Integration.** In remote integrations, installation of HP software on a third-party system is not required. A data collector (SiteScope with Integration Monitors or Integration Adapter) can be installed near the third-party system, for example in the same subnet, and behind the firewall if one is present.

➤ **Local Integration.** You install SiteScope or the Integration Adapter directly on the third-party domain manager or application system.

All data collectors specified as remote may also be applied locally, but those specified as local cannot be applied remotely.

BSM Applications That Use Third-Party Data

You can view the information collected from a third-party domain manager or application system in the following BSM applications:

➤ **Operations Management:** Correlates and manages events from third-party systems. You can view events in the Operations Management Event Browser (if you have an Event Management Foundation license). For details, see *Using Operations Management*.

➤ **Run-time Service Model (RTSM):** Integrates topology monitored by third-party domain managers or custom applications. You can then manage and work with these discovered configuration items (CIs) in views that provide a subset of the components in which your business functions. For details, see the *RTSM Administration Guide*.

➤ **Service Health:** Integrates monitoring metrics or events from third-party systems into health indicators (HIs), impacting the overall CI status. For details, see *Using Service Health*.

➤ **Service Level Management:** Integrates third-party data into SLM HIs, impacting SLA status. For details, see *Using Service Level Management.*

➤ **Reports:** Integrates monitoring metrics from third-party systems into System Availability Management reports. For details, see "SAM Reports" in *Using System Availability Management.*

Integration Prerequisites For BSM 9.10

The following are required to enable the integration of third-party data with BSM 9.10 applications when using SiteScope Integration Monitors or the Integration Adapter:

Product	Required Licenses
BSM 9.10	To use the SiteScope Integration Monitors, you need to have a System Availability Management license. For details, see "SAM Administration Overview" in *Using System Availability Management.* To use the Integration Adapter, you need to have a Target Connector licence. For details, see "Introduction and Overview" > "Licensing" in *Using Operations Management.*
SiteScope 11.11 or later	No license required
Integration Adapter 9.10	No license required

Reference

🔖 Out-of-the Box Integrations

You can use the following out-of-the box integrations with the Integration Adapter tool:

➤ "Third-Party Integrations" on page 392

➤ "HP Product Integrations" on page 393

Third-Party Integrations

Integration Source	Integration Type	Applicable to BSM Applications	Integration Point	Documentation
Microsoft System Center Operations Manager (SCOM)	➤ Events ➤ Topology	➤ Operations Management ➤ Run-time Service Model ➤ Service Health ➤ Service Level Management	Integration Adapter	Integration Adapter SCOM integration documentation, available from the HP Live Network (https://www.www2.hp.com): ➤ *HP BSM Connector for SCOM Installation Guide* ➤ *HP BSM Connector for SCOM User Guide* ➤ *HP BSM Connector for SCOM Release Notes*
Nagios	➤ Events ➤ Topology	➤ Operations Management ➤ Run-time Service Model ➤ Service Health ➤ Service Level Management	Integration Adapter	Integration Adapter Nagios integration documentation, available from the HP Live Network (https://www.www2.hp.com): ➤ *HP BSM Connector for Nagios Installation Guide* ➤ *HP BSM Connector for Nagios Release Notes* ➤ *HP BSM Connector for Nagios Open Source and Third Party Licenses*

HP Product Integrations

Integration Source	Integration Type	Applicable to BSM Applications	Integration Point	Documentation
HP Network Node Manager i	➤ Events ➤ Topology	➤ Operations Management ➤ Run-time Service Model ➤ Service Health ➤ Service Level Management	Integration Adapter	"Integrations with NNMi" in *HP NNMi Deployment Reference*, available from the HP Software Support Product Manuals site (http://support.openview.hp.com/selfsolve/manuals).
HP ArcSight	Events	Operations Management	Integration Adapter	*SmartConnector Configuration Guide for ArcSight Forwarding Connector* available from the ArcSight support website (https://software.arcsight.com/documentation).

Recommended Integration Points and Data Collectors

This tables displays the options to collect and use third-party data based on the source type and integration type, when not using an out-of-the box integration.

For more details on each integration option, see the section for the relevant data type being collected in "Integration Options and Details" on page 395.

Data Source	Event	Metrics	Topology	Event & Topology	Metrics & Topology	Event & Metrics
Log	SiteScope[1]	SiteScope[1]	SiteScope[1]	SiteScope[1]	SiteScope[1]	SiteScope[1]
Database	SiteScope[2]	SiteScope[2]	SiteScope[2]	SiteScope[2]	SiteScope[2]	SiteScope[2]
Web Service	SiteScope[3]	SiteScope[3]	SiteScope[3]	SiteScope[3]	SiteScope[3]	SiteScope[3]
SNMP Trap	SiteScope[4] or Integration Adapter SNMP policy	SiteScope[4]	SiteScope[4]	SiteScope[4] or Integration Adapter SNMP policy + one SiteScope integration monitor	SiteScope[4]	SiteScope[4] or Integration Adapter SNMP policy + one SiteScope integration monitor
Local: XML	Integration Adapter XML policy			Integration Adapter XML policy + one SiteScope integration monitor		Integration Adapter XML policy + one SiteScope integration monitor
Using the following SiteScope Technology Integration monitor: [1] Technology Log File Integration Monitor [2] Technology Database Integration Monitor [3] Technology Web Service Integration Monitor [4] Technology SNMP Trap Integration Monitor						

🔍 Integration Options and Details

This section includes:

Events Integration

This describes the method if you want to integrate third-party events only into BSM. The data is consumed by the following applications:

➤ Operations Management

➤ Service Health

➤ Service Level Management

Integration Type	Integration Tool	For more information, see
Remote or Local	SiteScope Integration Monitors	In *Documentation Updates for SiteScope 11.11*: ➤ "Event Integration for Technology Integration Monitors" In *Using SiteScope* in the SiteScope Help: ➤ "Integration Monitor Field Mapping" In *Monitor Reference* in the SiteScope Help: ➤ "Technology Log File Integration Monitor" ➤ "Technology Database Integration Monitor" ➤ "Technology SNMP Trap Integration Monitor" ➤ "Technology Web Service Integration Monitor"
	Integration Adapter Policy - SNMP	In *HP BSM Integration Adapter User Guide* PDF: ➤ "Developing SNMP interceptor policies"
Local Only	Integration Adapter Policy - XML	In *HP BSM Integration Adapter User Guide* PDF: ➤ "Developing XML interceptor policies"

Metrics Integration

This describes the method if you want to integrate third-party metrics only into BSM. The data is consumed by the following applications:

➤ Service Health

➤ Service Level Management

➤ System Availability Management reports

Integration Type	Integration Tool	For more information, see
Remote or Local	SiteScope Integration Monitors	In *Documentation Updates for SiteScope 11.11*: ➤ "SiteScope Integration Monitor Metrics Flow With Custom Topology - Best Practices" ➤ "SiteScope Integration Monitor Metrics Flow With Computer/Monitor Topology - Best Practices" ➤ "SiteScope Integration Monitor Metrics Flow With No Topology - Best Practices" In *Using SiteScope* in the SiteScope Help: ➤ "Integration Monitor Field Mapping" In *Monitor Reference* in the SiteScope Help: ➤ "Technology Log File Integration Monitor" ➤ "Technology Database Integration Monitor" ➤ "Technology SNMP Trap Integration Monitor" ➤ "Technology Web Service Integration Monitor"

Topology Integration

This describes the method if you want to integrate third-party topology data only into BSM. The data is consumed by the following applications:

➤ Operations Management

➤ Run-time Service Model

➤ Service Health

➤ Service Level Management

Integration Type	Integration Tool	For more information, see
Remote or Local	SiteScope Integration Monitors	In *Documentation Updates for SiteScope 11.11*: ➤ "Reporting Topology Without Data for Technology Integration Monitors" In *Using SiteScope* in the SiteScope Help: ➤ "Topology Settings for Technology Integration Monitors" In *Monitor Reference* in the SiteScope Help: ➤ "Technology Log File Integration Monitor" ➤ "Technology Database Integration Monitor" ➤ "Technology SNMP Trap Integration Monitor" ➤ "Technology Web Service Integration Monitor"

Metrics and Topology Integration

This describes the method if you want to integrate third-party metrics and topology data into BSM. The data is consumed by the following applications:

➤ Run-time Service Model

➤ Service Health

➤ Service Level Management

➤ System Availability Management reports

Integration Type	Integration Tool	For more information, see
Remote or Local	SiteScope Integration Monitors	In *Documentation Updates for SiteScope 11.11*: ➤ "SiteScope Integration Monitor Metrics Flow With Custom Topology - Best Practices" and ➤ "SiteScope Integration Monitor Metrics Flow With Computer/Monitor Topology - Best Practices" In *Using SiteScope* in the SiteScope Help: ➤ "Topology Settings for Technology Integration Monitors" In *Monitor Reference* in the SiteScope Help: ➤ "Technology Log File Integration Monitor" ➤ "Technology Database Integration Monitor" ➤ "Technology SNMP Trap Integration Monitor" ➤ "Technology Web Service Integration Monitor"

Events and Topology Integration

This describes the method if you want to integrate third-party events and topology data into BSM. The data is consumed by the following applications:

➤ Operations Management

➤ Run-time Service Model

➤ Service Health

➤ Service Level Management

You can use the following integration tools:

➤ SiteScope Integration Monitors for both events and topology, or

➤ The Integration Adapter policy for events, and one of the SiteScope Integration Monitors with the **Report topology without data** option for topology.

Note: When using the Integration Adapter and a SiteScope Integration Monitor, follow the procedure described in "Coexistence Procedure for SiteScope and the Integration Adapter" on page 404.

Integration Type	Integration Tool	For more information, see
Remote or Local	SiteScope Integration Monitors	In *Documentation Updates for SiteScope 11.11*: ➤ "SiteScope Integration Monitor Metrics Flow With Custom Topology - Best Practices" and ➤ "SiteScope Integration Monitor Metrics Flow With Computer/Monitor Topology - Best Practices" In *Using SiteScope* in the SiteScope Help: ➤ "Integration Monitor Field Mapping" In *Monitor Reference* in the SiteScope Help: ➤ "Technology Log File Integration Monitor" ➤ "Technology Database Integration Monitor" ➤ "Technology SNMP Trap Integration Monitor" ➤ "Technology Web Service Integration Monitor"
	Integration Adapter Policy - SNMP	In *HP BSM Integration Adapter User Guide* PDF: ➤ "Developing SNMP interceptor policies"
Local Only	Integration Adapter Policy - XML	In *HP BSM Integration Adapter User Guide* PDF: ➤ "Developing XML interceptor policies"

Events and Metrics Integration

This describes the method if you want to integrate third-party events and metrics data into BSM. The data is consumed by the following applications:

➤ Operations Management

➤ Service Health

➤ Service Level Management

➤ System Availability Management reports

You can use the following integration tools:

➤ SiteScope Integration Monitors for both events and metrics, or

➤ The Integration Adapter policy for events, and one of the SiteScope Integration Monitors with the **Report topology without data** option for metrics.

Note: When using the Integration Adapter and a SiteScope Integration Monitor, follow the procedure described in "Coexistence Procedure for SiteScope and the Integration Adapter" on page 404.

Integration Type	Integration Tool	For more information, see
Remote or Local	SiteScope Integration Monitors	In *Documentation Updates for SiteScope 11.11*: ➤ "SiteScope Integration Monitor Metrics Flow With Custom Topology - Best Practices", ➤ "SiteScope Integration Monitor Metrics Flow With Computer/Monitor Topology - Best Practices", and ➤ "SiteScope Integration Monitor Metrics Flow With No Topology - Best Practices" In *Using SiteScope* in the SiteScope Help: ➤ "Integration Monitor Field Mapping" In *Monitor Reference* in the SiteScope Help: ➤ "Technology Log File Integration Monitor" ➤ "Technology Database Integration Monitor" ➤ "Technology SNMP Trap Integration Monitor" ➤ "Technology Web Service Integration Monitor"
	Integration Adapter Policy - SNMP	In *HP BSM Integration Adapter User Guide* PDF: ➤ "Developing SNMP interceptor policies"
Local Only	Integration Adapter Policy - XML	In *HP BSM Integration Adapter User Guide* PDF: ➤ "Developing XML interceptor policies"

🔍 Coexistence Procedure for SiteScope and the Integration Adapter

1 **Install the Integration Adapter together with the HP Operations agent.**

   For details, see the *HP BSM Integration Adapter Installation and Upgrade guide*.

2 **Install SiteScope without the HP Operations agent.**

   If you have not yet installed SiteScope, select **Do not install HP Operations agent** in the Configuration wizard during SiteScope installation.

   If you have already installed SiteScope, the Integration Adapter agent installation may upgrade the agent installed on the SiteScope server.

3 **Use different port ranges for SiteScope and the Integration Adapter.**

   Note: This step is not required if you did not perform any port customization for SiteScope or the Integration Adapter.

   If you have changed the ports, make sure you use different port ranges for SiteScope and the Integration Adapter.

   ➤ In SiteScope, use the Configuration Tool to review or change ports used by SiteScope. For details, see "Using the SiteScope Configuration Tool" in the *HP SiteScope Deployment Guide* PDF.

   ➤ In the Integration Adapter, use the configuration program (**%OvDataDir%\installation\HPOprIA\ia-config.bat**). For details, see "Configure HP BSM Integration Adapter" in the *HP BSM Integration Adapter Installation and Upgrade guide*.

4 **If you intend to use the SiteScope Integration Monitor common event flow, perform the following steps:**

   ➤ In SiteScope, select **Preferences** > **Integration Preferences**, and click **HP Operations Manager Integration** to create a new Operations Manager integration.

   ➤ Expand the HP Operations Manager Integration Main Settings panel, and in Connection Settings, specify the address of your Operations Manager/BSM server in the **HP Operations Manager/BSM server** box.

➤ Skip the **Connect** step, and complete the **Install policies** step only.

For details, see "How to Enable SiteScope to Send Events to HPOM or BSM" in *Using System Availability Management.*

15

HP BSM Integration Adapter

This chapter includes:

Concepts

Tasks

Concepts

🌀 HP BSM Integration Adapter Overview

Note: Before performing integrations with third-party products, review the information in "Best Practices for Integrating Third-Party Data" on page 387.

HP BSM Integration Adapter enables you to monitor event sources, and, if certain conditions apply, to forward the detected events as HP Business Service Management (BSM) events directly to BSM Operations Management. BSM tries to associate the events that it receives with configuration items (CIs) using CI resolution and with indicators using ETI (event type indicator) resolution. This is only possible if the computer on which the event occurs is set up as a CI in the BSM Run-time Service Model (RTSM). Discovery policies automatically populate the RTSM with topology data based on discovery scripts executed within the BSM Integration Adapter environment.

For more information about integrating events and topology data into BSM, see "How to Integrate Events and Topology Data with HP BSM Integration Adapter" on page 418.

For more information about BSM Integration Adapter, see the *HP BSM Integration Adapter User Guide* PDF.

HP BSM Integration Adapter Environment

The BSM Integration Adapter environment typically includes the source manager that provides the input events and topology data, as well as the BSM deployment where the events and topology data are received.

You typically install BSM Integration Adapter on the computer that provides the input events and topology data. For example, to integrate Network Node Manager i (NNMi) events into BSM, install BSM Integration Adapter on the NNMi management server.

BSM Integration Adapter includes the HP Operations Agent. The HP Operations Agent collects and monitors data on the event source, enriches these events with information that is meaningful to BSM users, and sends the events to BSM where they are displayed in the Operations Management Event Browser. The HP Operations Agent can also run discovery scripts or programs, store and compare the CI details obtained in each discovery cycle, and send the discovery data to the RTSM.

The BSM Integration Adapter uses monitor and discovery policies to configure the agent. For each monitor policy, you decide what kinds of events to monitor, how often to monitor, what to look for in the events, and what to do if certain events are detected. For each discovery policy, you decide which discovery script to run and how often to run.

For more information about the HP Operations Agent, see the documentation that HP Operations Agent provides.

Note: If you have the Event Management Foundation license, BSM Operations Management can receive events and topology data from HP Operations Manager (HPOM), or directly from BSM Integration Adapter. BSM Integration Adapter is the preferred method for sending events and topology data to Operations Management in the following situations:

➤ If you are developing *new* integrations for sending events and topology data to BSM Operations Management.

➤ If there is no need to use the HPOM event processing and discovery capabilities or console.

➤ If HPOM is not part of the BSM deployment.

For more information about deploying BSM, see the the *HP Business Service Management Deployment Guide* PDF.

You can integrate BSM Integration Adapter into Operations Management so that administrators can launch the BSM Integration Adapter user interface in the Connected Servers manager or in the context of an event. Single sign-on authentication enables BSM users to log into BSM once and gain access to BSM Integration Adapter without being prompted to log in again.

BSM also enables operators to start the user interface of the source manager in the context of an event in the Operations Management Event Browser.

Event Integration

For BSM Integration Adapter to be able to convert source events to BSM events, the event sources must make their data available as SNMP traps or in XML-formatted files:

➤ **SNMP traps**

SNMP event sources can range from simple hardware devices that send SNMP traps to sophisticated network management solutions such as Network Node Manager i (NNMi).

NNMi provides an out-of-the-box integration with BSM Integration Adapter, which converts NNMi incidents to SNMPv2c traps and forwards these SNMPv2c traps as BSM events to the BSM Operations Management Event Browser. For more information about this integration, see the *NNMi Deployment Reference*.

➤ **XML files**

BSM Integration Adapter can also monitor XML-formatted files. Because BSM Integration Adapter is agnostic to the content and syntax of the XML files, you can monitor any XML file.

If the application that you want to monitor does not log its events in XML format, consider writing a program or script that diverts and converts the application's output to XML-formatted files.

Tip: Monitoring XML files is a convenient way to forward events from other source managers to BSM Operations Management. In the context of BSM, a source manager is an HP or third-party software solution that monitors and manages performance, systems, services, or networks in the IT environment. Examples include NNMi, Microsoft System Center Operations Manager (SCOM), or IBM Tivoli solutions.

After Operations Management receives an event, you can keep it up to date on the source by configuring BSM and BSM Integration Adapter to synchronize event lifecycle changes (to the state closed) back to the source manager that generated the original event. For example, if a BSM Operations Management operator closes an event, a notification can be automatically sent to NNMi.

Topology Data

Accurate and up-to-date CI topology data in the RTSM is essential for CI and ETI (event type indicator) resolution, TBEC (Topology-based Event Correlation), and context-specific tools. BSM Integration Adapter uses discovery policies to automatically discover IT infrastructure resources and their interdependencies.

Discovery policies execute a discovery script that you create and that must write details of each discovered CI and its relationships in XML to STDOUT (standard output stream). BSM Integration Adapter processes the XML data and publishes details of new, changed, and removed CIs and CI relationships to the discovery server on the BSM gateway servers, according to a schedule that you specify for each policy.

Before topology data is written to the RTSM, topology synchronization rules manipulate the data by applying mapping rules and scripts. Mapping rules and scripts transform the discovered topology data into CI and CI relations in the RTSM. For more information about topology synchronization, see the OMi *Extensibility Guide* PDF.

Tip: You can also create the CIs and CI relationships using the discovery features of the RTSM and HP Data Flow Management (DFM), using topology synchronization from HPOM, or manually. It is recommended to use BSM Integration Adapter discovery if you already use BSM Integration Adapter to forward events to the BSM Operations Management Event Browser. You can create CIs manually if the CIs you want to create are limited in number, and are stable in nature, so are unlikely to change.

HP BSM Integration Adapter User Interface and Authentication

The BSM Integration Adapter user interface is web based; you can therefore access it from anywhere using a supported web browser.

The BSM Integration Adapter user interface is as follows:

BSM Integration Adapter supports the following user authentication strategies:

➤ **Single Sign-On (SSO) for BSM applications (recommended)**

The default single sign-on authentication strategy for BSM is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in BSM and does not require an external computer for authentication.

LW-SSO enables a user to log into BSM once and gain access to all BSM applications without being prompted to log in again. The applications inside BSM trust the authentication, and you do not need further authentication when moving from one application to another. For example, if you configure BSM Integration Adapter to use LW-SSO, BSM users can launch the BSM Integration Adapter user interface without having to provide additional credentials.

Tip: BSM enables you to group users to make managing user permissions more efficient. For example, you could add all BSM Integration Adapter users to a dedicated group (IA_ADMINS, for example) and assign permissions to access BSM Integration Adapter to the group.

For more information about LW-SSO, see the BSM Platform Administration guide.

➤ **Local user authentication**

Each BSM Integration Adapter instance maintains a local user store. These users can access the local BSM Integration Adapter instance only and cannot gain access to other BSM applications. When BSM users launch the BSM Integration Adapter user interface, they have to provide the credentials of a local BSM Integration Adapter user.

🔩 Policies

Policies are collections of configuration information used to configure HP Operations Agent on the BSM Integration Adapter server to perform monitoring or discovery tasks. When you develop monitor policies, you decide what kinds of events to monitor, how often to monitor, what to look for in the events, and what to do if certain events are detected. Discovery policies automatically populate the BSM RTSM with topology data based on discovery scripts executed within the BSM Integration Adapter environment.

BSM Integration Adapter enables you to create and edit policies to discover CIs and CI relationships, to capture SNMP events, and to monitor XML files. You can import policies developed on other servers, for example, HP Operations Manager (HPOM) management servers, Network Node Manager i (NNMi) management servers, or other BSM Integration Adapter servers.

Note: NNMi provides an SNMP interceptor policy that you can import into the BSM Integration Adapter policy repository. The policy includes an SNMPv2c trap definition for each of the management events and SNMP traps in the current NNMi configuration. For more information about the BSM Integration Adapter–NNMi integration, see the *NNMi Deployment Reference*.

Integrating Events with XML Interceptor Policies

XML interceptor policies are especially suited for integrating events from other source managers. XML interceptor policies process XML files and send events to the Operations Management event browser when certain conditions apply. You can define the attributes of the BSM event based on information in the XML file. This enables you to process events generated by the applications and to convert them to BSM events.

XML interceptor policies process exactly the XML elements and attributes that you define. The XML syntax is not important to the policy, as long as the event information is embedded in XML elements and attributes.

If the source manager does not store its events in XML files, you may need to write a program or script that extracts the events from wherever they are stored, formats the data using XML syntax, and generates an XML file with the events. If you have control over the XML elements that are used in the XML file, choose XML elements and attributes that map to event attributes and values. This will simplify the policy.

XML interceptor policies facilitate event integration tasks by offering the following special features:

➤ **Pattern matching.** The pattern-matching language enables you to very accurately specify the character string that you want a rule to match. Selected, dynamic parts of text-based events can be extracted, assigned to variables, and used as parameters to build the event description or to set other attributes.

➤ **Mapping defaults.** Mapping defaults enable you to map XML elements and attributes to custom variables. You can then use the custom variables in the policy to dynamically replace a specific value in the XML source file with a default value in the event.

➤ **Drag and drop.** XML policy editors enable you to drag and drop data quickly and easily create defaults and rules.

➤ **Sample data.** You can load a sample of the XML log file that you want to monitor. BSM Integration Adapter makes the XML elements and values of the sample file available so that you can insert them by dragging and dropping.

The XML interceptor policy editor is as follows:

Tasks

🔖 How to Integrate Events and Topology Data with HP BSM Integration Adapter

This section describes how to integrate events and topology data into BSM using BSM Integration Adapter. For more information about each task, refer to the corresponding documentation.

This task includes the following steps:

➤ "Install and configure BSM Integration Adapter" on page 419

➤ "Create new discovery, SNMP, or XML interceptor policies in BSM Integration Adapter" on page 419

➤ "Configure event synchronization - optional" on page 420

➤ "Configure drilldown - optional" on page 420

➤ "Activate the policies in BSM Integration Adapter" on page 420

1 Install and configure BSM Integration Adapter

Use the *HP BSM Integration Adapter Installation and Upgrade Guide* to install and configure BSM Integration Adapter on the computer that serves as event and topology source. During the configuration process you establish the connection between BSM Integration Adapter and BSM.

2 Create new discovery, SNMP, or XML interceptor policies in BSM Integration Adapter

BSM Integration Adapter enables you to create and edit policies of the type discovery, SNMP interceptor, and XML interceptor.

Tip: If your event source does not provide data in XML file format, you may need to write a program or script that converts the event data to XML format. See also "Integrating Events with XML Interceptor Policies" on page 416.

Alternatively, you can import policies developed on other servers, for example, HP Operations Manager (HPOM) management servers, Network Node Manager i (NNMi) management servers, or other BSM Integration Adapter servers. For more information about importing policies, see the *HP BSM Integration Adapter User Guide* PDF.

3 Configure event synchronization - optional

After Operations Management receives an event, you can keep it up to date on the event source by configuring BSM and BSM Integration Adapter to synchronize event lifecycle changes (to the state closed) back to the source manager that generated the original event. For example, if a BSM Operations Management operator closes an event, a notification can be automatically sent to NNMi. For more information about configuring event synchronization, see the *HP BSM Integration Adapter User Guide* PDF.

4 Configure drilldown - optional

You can integrate BSM Integration Adapter into Operations Management so that administrators can launch the BSM Integration Adapter user interface in the Connected Servers manager or in the context of an event. BSM also enables operators to start the user interface of the source manager in the context of an event in the Operations Management Event Browser. For more information about configuring drilldown, see the *HP BSM Integration Adapter User Guide* PDF.

5 Activate the policies in BSM Integration Adapter

When you create a new policy or import a policy, the policy exists in the BSM Integration Adapter policy repository but does not function yet. You must first activate the policy for it to start monitoring the corresponding event source. For more information, see the *HP BSM Integration Adapter User Guide* PDF.

16

EMS Integration Administration

This chapter includes:

Concepts

Tasks

Reference

Concepts

🔩 Integration Administration Application Overview

Note: Before performing integrations with third-party products, review the information in "Best Practices for Integrating Third-Party Data" on page 387.

BSM has the ability to integrate with existing Enterprise Management Systems (EMS) software and provides the capability to build new integrations (that report predefined or custom topologies for example, Node, Tickets, or Node - Running Software), or use out-of-the-box integrations (for example: HP Service Manager or NetScout nGenius).

Features of the Application

The EMS Integrations application provides the following features:

➤ **CIT relationships map.** You can sketch a CIT relationship map of the integration you are creating to help you formulate the data assignments that are described below. This feature is for illustration only.

➤ **SiteScope Integration Monitors.** SiteScope Integration Monitors integrate measurements, open incidents, alerts, and events generated by Enterprise Management Systems software into BSM. For details about the SiteScope integration monitors, see "Working with SiteScope Integration Monitors" in *Using System Availability Management*.

You access the System Availability Management Administration through a window in the EMS Integrations application. Using the window, you can access SiteScopes and create integration monitors to collect performance and availability data from your EMS system.

➤ **Assignments.** You can configure assignments for EMS Monitor CI type that you added to the CIT relationship map you sketched previously. A health indicator or a KPI assignment rule includes a condition and a task. The condition describes, where relevant, specific characteristics of a CI. The task describes the shortcut menus, health indicators, KPIs, rules, rule parameters, and selectors that are to be assigned automatically to the CI when the condition occurs, if the assignment is running. Out-of-the-box integrations and new assignments with predefined topology already include the relevant assignments. For details on the assignment mechanism, see "Assignment Mechanism" in *Using Service Health*.

➤ **Integration View Results.** Out-of-the-box integrations already include predefined views. In addition, a new view is automatically created for a new integration The name of the view is the same as the name of the integration data source. The view includes the relevant CIs. You can display the view contents and the status of the view's CIs in Service Health.

Understanding Node, Tickets, or Node - Running Software Integration Types

This section describes the main concepts of Node, Tickets, and Node - Running Software default integration types.

The out-of-the-box Node, Tickets, and Node - Running Software integration types use out-of-the-box topology scripts to create the appropriate topology.

KPIs and health indicators assigned to an EMS Monitor CI, as shown below, are automatically propagated to the parent CI.

Node

When an **EMS Monitor** CI is added to the RTSM, the following happens:

➤ In Service Health:

   ➤ The **System EMS Monitor** health indicator is assigned to the **EMS Monitor** CI with the **SiteScope EMS Monitor Multiple Events** rule.

   ➤ The **Legacy System** KPI is assigned to the **EMS Monitor** CI with the **Worst Status** rule and the **EMS Measurement** menu.

➤ In Service Level Management:

   ➤ The **Software Performance EMS Monitor** health indicator is assigned to the **EMS Monitor** CI with the **Application Quality** rule.

   ➤ The **System EMS Monitor** health indicator is added to the **EMS Monitor** CI with the **System Quality** rule.

   ➤ The **Legacy System** KPI is assigned to the **EMS Monitor** CI with the **Group Average Value** rule.

   ➤ The **Software Performance** KPI is assigned to the **EMS Monitor** CI with the **Group Average Value** rule.

For concept details about assignments, see "Assignments" in *Using Service Health*.

Tickets

When an **EMS Monitor** CI is added to the RTSM, the following happens:

➤ In Service Health:

   ➤ The **Ticketing EMS Monitor** health indicator is assigned to the **EMS Monitor** CI with the **Number of Open Incidents** rule.

   ➤ The **Number of Open Incidents** KPI is assigned to the **EMS Monitor** CI with the **Worst Status** rule.

➤ In Service Level Management:

  ➤ The **Software Performance EMS Monitor** health indicator is assigned to the **EMS Monitor** CI with the **Application Quality** rule.

  ➤ The **System EMS Monitor** health indicator is added to the **EMS Monitor** CI with the **System Quality** rule.

  ➤ The **Legacy System** KPI is assigned to the **EMS Monitor** CI with the **Group Average Value** rule.

  ➤ The **Software Performance** KPI is assigned to the **EMS Monitor** CI with the **Group Average Value** rule.

For concept details about assignments, see "Assignments" in *Using Service Health*.

Node - **Running Software**

When an **EMS Monitor** CI is added to the RTSM, the following happens:

➤ In Service Health:

  ➤ The **System EMS Monitor** health indicator is assigned to the **EMS Monitor** CI with the **SiteScope EMS Multiple Events** rule if the value of the **Monitored CI Type** field on the **EMS Monitor** CI is **Node**.

  ➤ The **System EMS Monitor** health indicator is assigned to the **EMS Monitor** CI with the **SiteScope EMS Multiple Events** rule if the value of the **Monitored CI Type** field on the **EMS Monitor** CI is **Running Software**.

  ➤ The **Legacy System** KPI is assigned to the **EMS Monitor** CI with the **Worst Status** rule and the **EMS Measurement** menu is assigned to the **EMS Monitor** CI.

  ➤ The **Legacy System** KPI is assigned to the **EMS Monitor** CI with the **Worst Status** rule and the **EMS Measurement** menu is assigned to the **EMS Monitor** CI.

➤ In Service Level Management:

➤ The **Software Performance EMS Monitor** health indicator is assigned to the **EMS Monitor** CI with the **Application Quality** rule if the value of the **Monitored CI Type** field on the **EMS Monitor** CI is **Node**.

➤ The **System EMS Monitor** health indicator is added to the **EMS Monitor** CI with the **System Quality** rule on the **EMS Monitor** CI is **Node**.

➤ The **Legacy System** KPI is assigned to the **EMS Monitor** CI with the **Group Average Value** rule.

➤ The **Software Performance** KPI is assigned to the **EMS Monitor** CI with the **Group Average Value** rule.

For concept details about assignments, see "Assignments" in *Using Service Health*.

Tasks

🔧 How to Integrate Data from Third-Party Sources (EMS Data) into HP Business Service Management

---

Note: Before performing integrations with third-party products, review the information in "Best Practices for Integrating Third-Party Data" on page 387.

This section describes the processes for integrating data from third-party sources (EMS data) into BSM.

The process uses SiteScope integration monitors to integrate the data from that application, into BSM, using EMS.

This task includes the following steps:

➤ "Prerequisite" on page 427

➤ "Plan EMS strategy" on page 428

➤ "Create an EMS integration (for Metric Samples)" on page 428

➤ "Create an EMS integration (for Event or Ticket Samples)" on page 429

➤ "View status in Service Health and Service Level Management" on page 433

➤ "View data in the Event Log (for monitor configured with event or ticket samples)" on page 433

➤ "Assign group permissions (for monitor configured with metrics samples that reports SiteScope monitors in the topology)" on page 434

1 Prerequisite

You must integrate SiteScope and BSM. For details, see "How to Configure the Integration Between SiteScope and BSM" in *Using System Availability Management*.

2 **Plan EMS strategy**

Review the Integration Monitor types. Consider the type of information you want to see in HP Business Service Management from your EMS system. Determine whether one of the specific Integration Monitors meets your organization's needs or whether a generic Integration Monitor (Technology Log File, Database, SNMP Trap, Web Service) is required.

Review the Event, Ticket, and Metrics samples and fields to understand how the incoming EMS data maps to HP Business Service Management data.

For more information, see "Working with SiteScope Integration Monitors" in *Using SiteScope* in the SiteScope help.

3 **Create an EMS integration (for Metric Samples)**

a **Configure the integration monitors:**
You can either:

➤ In **System Availability Management Admin,** select the SiteScope server from which you want to create the integration monitor. For user interface details, see "System Availability Management Administration Page" in *Using System Availability Management.*

➤ In **SiteScope**, configure the SiteScope integration monitors in SiteScope. For more information, see "Working with SiteScope Integration Monitors" in *Using SiteScope* in the SiteScope help.

b If you want to create a new technology monitor, you must also configure the field mapping according to the metric sample type, and the topology script as follows:

➤ **SiteScope Topology** to send the basic SiteScope topology with Sitescope Monitor and Computer CIs

➤ **No topology** to create only data, and no topology

➤ **Custom** to create the CIs according to the topology described in user-written topology script

c **Create or customize a data assignment:**
For **No topology** or **Custom** scripts, you might have to create or customize a data assignment for the reported CIs.

You can either create/change the assignments or change existing Health Indicators attached to specific CIs:

➤ In Service Health: To change/create assignments, go to **Admin > Service Health** > **Assignments** > **KPI/Health Indicator Assignments**. To apply the change on existing CIs, select the assignment and click **Synchronize CI Type**. For details, see "Edit Integration Dialog Box" on page 444.

➤ In Service Level Management: You can either create/change the assignments or change existing Health Indicators attached to specific CIs. To change/create assignments, go to **Admin > Service Level Management** > **Assignments** > **KPI/Health Indicator Assignments**. To apply the change on existing CIs, select the assignment and click **Synchronize CI Type**. For details, see "Edit Integration Dialog Box" on page 444.

4 Create an EMS integration (for Event or Ticket Samples)

In BSM, select **Admin > Integrations > EMS Integrations Admin**, click the **New Integration** button to create a new integration (see "Add Integration Dialog Box" on page 441) and proceed as follows:

a Sketch a CIT Relationship map:
In BSM, select **Admin > Integrations > EMS Integrations Admin**, and sketch a CIT relationship map of the integration you are creating to help you formulate the data assignments that are described below and to understand which topology to create. This feature is for illustration only.

b Configure the integration monitors:
You can either:

➤ **In EMS.** Open the System Availability Management Administration window where you can access a SiteScope and create integration monitors to collect performance and availability data from your EMS system. For details, see "Working with SiteScope Integration Monitors" in *Using SiteScope* in the SiteScope help.

➤ **In System Availability Management Admin.** select the SiteScope server from which you want to create the integration monitor. For user interface details, see "System Availability Management Administration Page" in *Using System Availability Management*.

➤ **In SiteScope.** Configure the SiteScope integration monitors in SiteScope. For more information, see "Working with SiteScope Integration Monitors" in *Using SiteScope* in the SiteScope help.

If you want to create a new technology monitor, you must also configure:

➤ The field mapping according to the sample type which can be event, ticket, or measurement.

➤ The topology script depending on the sample type described in the following table:

Event Sample Script	Tickets sample script
Select one of the following options: ➤ **Node** to create the Node and EMS Monitor CIs ➤ **Node-Running Software** to create the Node, Running Software, and EMS Monitor CIs ➤ **Custom** to create the CIs according to the topology user-written topology script	Select one of the following options: ➤ **Ticket** to create the Business Service and EMS Monitor CIs ➤ **Custom** to create the CIs according to the topology user-written topology script

c Create or customize a data assignment:
Create or customize a data assignment for each integration CI type in the CIT relationship map you sketched previously. Out-of-the-box EMS integrations or custom integrations that are based on predefined topology type (Node, Node-Running Software, or Custom) already include the relevant data assignments. For user interface details, see "Edit Integration Dialog Box" on page 444.

Depending on the type of data you want to integrate, select the following EMS integration type:

Events	Tickets
Select one of the following EMS integration types: ➤ **Nodes** ➤ **Nodes-Running Software** ➤ **Custom**	Select one of the following EMS integration types: ➤ **Ticket**s ➤ **Custom**

Limitations: For event and ticket samples, the monitor_id of the reported EMS monitor is built in the following way:

➤ For Tickets samples and Tickets topology, the monitor id is:
   <data_source>_<target_name>

➤ For Events samples and Node topology, the monitor id is:
   < target_name>

➤ For Events samples and Node- Running Software topology (where subject is not equal to **system**), the monitor id is:
   <subject (running software name)>

➤ For Events samples and Node- Running Software topology (where subject equals **system**), the monitor id is:
   < target_name>

Note: Do not use xml special characters (",',<,>,&) in the fields used to compose the monitor_id. Using these characters will cause problems in treating the samples in BSM.

You can either create/change the assignments or change existing Health Indicators attached to specific CIs:

➤ In Service Health: To change/create assignments, go to **Admin > Service Health** > **Assignments** > **KPI/Health Indicator Assignments**. To apply the change on existing CIs, select the assignment and click **Synchronize CI Type**. For details, see "Edit Integration Dialog Box" on page 444.

➤ In Service Level Management: You can either create/change the assignments or change existing Health Indicators attached to specific CIs. To change/create assignments, go to **Admin > Service Level Management** > **Assignments** > **KPI/Health Indicator Assignments**. To apply the change on existing CIs, select the assignment and click **Synchronize CI Type**. For details, see "Edit Integration Dialog Box" on page 444.

d Display the view:
A predefined view already exists for the out-of-box integrations.

A new view is automatically created whem creating a custom integration. The name of the view is the same as the name of the data source used in the integration.

The view displays the following:

➤ EMS Monitor CIs that were created by the EMS integration.

➤ CIs that were created by the EMS integration and that have a relationship to the above EMS Monitor CIs.

➤ All hosts with a relationship to either of the CIs mentioned above.

Tip: Do not edit or change the view – parts of the view are hidden in RTSM. To view the integration topology in a different way, create another view.

The HP OM (Legacy), Service Manager, and NetScout integrations are out-of-the-box integrations that enable the user to view HP OM (Legacy), HP Service Manager, and NetScout data in BSM. For details about the NetScout integration, see "NetScout nGenius Integration" on page 455.

For examples, see "How to Create a Node - Running Software Integration – Use-Case Scenario" on page 435.

5 View status in Service Health and Service Level Management

For event and ticket samples, you can view the data and statuses in the views created by the integration.

You can see the statuses corresponding to metric samples mapped with SiteScope Topology scripts, in the System Monitors view and System Hardware Monitoring views in Service Health and Service Level Management. You can also use the System Monitors view to view statuses, if you do not use SiteScope topology but report SiteScope monitors instead.

You must create a view that includes the relevant CIs, to view the statuses corresponding to metrics samples mapped with Custom or No topology scripts.

6 View data in the Event Log (for monitor configured with event or ticket samples)

After you defined monitors in System Availability Management Administration, you can see data in the Event Log and in Service Health.

For details about the Event Log, see "Event Log Overview" in *Using System Availability Management*.

For details about Service Health, see "Monitoring your Environment Using the Service Health Application" in *Using Service Health*.

7 Assign group permissions (for monitor configured with metrics samples that reports SiteScope monitors in the topology)

If you configure a generic integration monitor with a Metrics field mapping, you must assign for each defined user, permissions to view SiteScope groups and their subgroups in System Availability Management reports and custom reports. For more information, see "Permissions Overview" in *Platform Administration*.

How to Add CITs and Relationships to a Relationship Map

This section explains how to sketch the relationships map to help you when you define the assignment in the **HI and KPI Assignments** area. You sketch the map by adding CI Types (CITs) and relationships to the map.

To add CITs and relationships to a relationship map:

1 Select **Admin** > **Integrations** > **EMS Integrations**, and select an existing integration or create a new one.

2 In the Edit Integration dialog box, click **CI Relationships Map**.

3 In the CIT Relationships Map dialog box, you can:

   a Add a CIT to the map, by selecting the required CI Type from the tree in the left pane and dragging it to the right pane or by clicking the **Add selected CITs to Query** button in the toolbar of the CI Types tree in the left pane.

   b Add a relationship between two CITs, by selecting two CITs in the right pane and right-clicking to display a list of the available relationships, or by clicking the **Create Relationship** icon and drawing a line between the required CITs. The Select Relationship Type dialog box opens. Select the required relationship type. For details, see "Select Relationship Type Dialog Box" in *Modeling Guide*. For details about the different relationships, see "Shortcut Menu Options" in the *Modeling Guide*.

4 Click **OK**. The selected CITs are linked by the relationship you have selected.

For user interface details, see "CIT Relationships Map Dialog Box" on page 452.

🗡 How to Create a Node - Running Software Integration – Use-Case Scenario

To create a Node - Running Software integration:

1 Integrate BSM and the appropriate SiteScope. To specify the name of the host, select **Admin** > **System Availability Management**. Right-click **Summary** and select **New SiteScope**. In Main Settings, enter the name of the integration in the **Display Name** box and the name of the host in the **Host Name** box. Note that you might need other settings. For user interface details, see "New SiteScope Page" in *Using System Availability Management*.

2 Select **Admin** > **Integrations** > **EMS Integration Admin**, and click to open the Add Integration dialog box. Enter emsExample in the **Data Source** box and in the **Name** box, select Node - Running Software in the **Type** list, and enter a description in the **Description** box.

3 In the CI Relationships area, click **CI Relationships Map** to display the sketch of relationships for a typical Node - Running Software integration.

4 In the System Availability Management area, click **System Availability Management** to open the Summary page of System Availability Management in a new window. In that page, perform the following:

➤ Select the relevant SiteScope.

➤ Create a new group EMS.

➤ Under the new monitor, select the Technology Log File Integration monitor to open the New Technology Log File Integration monitor page. Enter the following values:

➤ In **Log file path name**: enter the location of the log file; c:\emsLog.txt.

➤ In **Content Match**, use the following example: /(.*),(.*),(.*),(.*),(.*),(.*)/

It should match the structure of the log file; for example:

```
8,event8,1,espresso,emsLog,app
8,event8,1,espresso,emsLog,app
```

➤ In **Fields mapping**, click **Load** and enter the relevant values:

```
###############################################################################
#          EMS Integrations event config file        #
# Use this file to send events to Business Service Management    #
#                                #
# Refer to "Integration Monitor Configuration Files" in SiteScope   #
#          documentation for more information.        #
###############################################################################

[$DEFAULT_PARAMETERS$]
##################################################
# NOTE: the following parameters are mandatory #
##################################################
# Time stamp in seconds since Jan 1st 1970 format.
# Use time() to get the sitescope host time or str_to_seconds() to read a value from the
input event
time_stamp:DOUBLE=time()
# Severity of event. Possible values are:
# SEVERITY_UNKNOWN, SEVERITY_INFORMATIONAL, SEVERITY_WARNING,
SEVERITY_MINOR, SEVERITY_MAJOR, SEVERITY_CRITICAL
severity:INT=$group2

# The name of the host / device that caused this event. If the name cannot be
determined an IP address can be used instead
target_name=$group3
# Event status or type (e.g "OPEN", "ASSIGNED", "CLOSED")
status="OPEN"

# Subject of event (for example, CPU, SAP application, Hard Disk ). Middle / High level
of hierarchy describing the event source
# The hierarchy describing an event is in the following format:
#   monitor_group (optional) --> object (optional) --> subject --> instance
# More levels can be added above monitor_group by using logical_group, and attr1 - 5
subject=$group4

# Instance of subject that generated the event (e.g "D:\\" ). The lowest level of hierarchy
describing the event source.
# See Subject explanation above.
instance=$group4
```

```
# Event description. Up to 2000 characters.
description=$group1

# Application / Software from which this event was collected
data_source="emsExample"
####################################################
# NOTE: The following parameters are optional.   #
# Remove comments from entries you want to use  #
####################################################
# IP of the host \ device that caused this event
#target_ip=
# Object of this event (for example, OS, Network, etc). optional level in the hierarchy
describing the event source

# See Subject explanation above.
#object=
# A unique identifier for this event
event_id=$group0
# For logical grouping
# See Subject explanation above.
#logical_group=
# Monitor group that reported this event. optional level in the hierarchy describing the
event source
# See Subject explanation above.
#monitor_group=

# Severity name in integrated system terminology
#orig_severity_name=
# Operator who acknowledged this event
#acknowledged_by=
# Operator who owns this event
#owner=
# Use with any numeric values you want to send to Business Service Management
#value:DOUBLE=

# Additional attributes 1..5
attr1=$group5
#attr2=
#attr3=
#attr4=
# For long string values up to 2000 use attr5
#attr5=
[allRecords]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
```

➤ In **Topology Settings**, select the Node - Running Software topology and click **Load**.

➤ Click **Save**.

➤ Test the script to view the expected results of the monitor. To activate, click **Test Script** in the Field Mapping or Topology Settings panes.

For additional information about the monitor, see "Technology Log File Integration Monitor" in *Monitor Reference* in the SiteScope help.

5 In the **Health Indicator and KPI Assignments** area, click the **Health Indicator Assignments** tab, and make sure the assignments are all running. Do the same with the KPI assignments in the **KPI Assignments** tab.

6 In the View Results area, click **Integration Results**, to display the topology of the default view named after the name you gave in the **Data Source** box in the steps above.

The integration is complete.

7 Select **Applications > Service Health**, in the 360° tab, select the emsExample view. The topology of the new view is displayed with data.

8 Select **Applications** > **Service Health**, in the Top View tab, select the emsExample view. The topology of the new view is displayed with data.

Reference

🔖 EMS Integration Administration User Interface

This section describes:

➤ Add Integration Dialog Box on page 441

➤ Edit Integration Dialog Box on page 444

➤ CIT Relationships Map Dialog Box on page 452

➤ EMS Integrations Admin Page on page 453

🔖 Add Integration Dialog Box

This dialog box enables you to create a new integration.

To access	**Admin** > **Integrations** > **EMS Integrations Admin**, and click the **New Integration** button.
	For user interface details, see "EMS Integrations Admin Page" on page 453.
Relevant tasks	"How to Integrate Data from Third-Party Sources (EMS Data) into HP Business Service Management" on page 427
See also	"Integration Administration Application Overview" on page 422

The initial dialog box includes the following elements:

UI Element (A-Z)	Description
Data Source	Enter the name of the integration data source when you create a custom integration.
	Note: The same data source must be used in the field mapping in the integration monitor. For details, see System Availability Management Area in "Edit Integration Dialog Box" on page 444.
Name	The name of the integration. The name of the integration is displayed in the EMS Integrations page.
Description	A description of the integration you are adding. The description of the integration is displayed in the EMS Integrations page.
OK	Opens the Edit Integration dialog box where you can enter the integration details.

UI Element (A-Z)	Description
Type	Select the type of integration you want to create. Select: ➤ **Node**. To create a node integration that adds nodes or reconciles the new nodes with existing nodes. For details, see "Understanding Node, Tickets, or Node - Running Software Integration Types" on page 423. ➤ **Node - Running Software.** To create a node and running software integration. For details, see "Understanding Node, Tickets, or Node - Running Software Integration Types" on page 423. ➤ **Tickets.** To create a business service connected to EMS monitor entities. For details, see "Understanding Node, Tickets, or Node - Running Software Integration Types" on page 423. ➤ **Custom Integration**. To create an integration with a topology created by a script the user defined in the monitor (not one of the predefined topologies created by predefined topology scripts like "Node"). This topology generally contains EMS Monitor CIs and other CIs the user wants to report. **Note:** When you select **Node**, **Tickets** or **Node - Running Software**, after you click the **OK** button, new KPI and Health Indicator assignments are automatically created in EMS. These assignments refer to the CI Type that is reported in the topology according to the integration type (for example, for the Node type, a Node CI).

🔍 **Edit Integration Dialog Box**

This dialog box enables you to edit an existing integration or to enter the details of a new integration.

To access	**Admin** > **Integrations** > **EMS Integrations Admin**, select an integration, and click the **Edit** 🖉 button.
Important information	➤ Complete each step of the procedure before starting on the next one.
	➤ Do not remove the data source when editing an integration.
	➤ It is recommended to work as much as possible with the out-of-the-box solutions:
	➤ HP ServiceCenter/HP Service Manager. For details, see "How to Integrate HP Service Manager with Business Service Management Components" on page 351.
	➤ HP OM. This integration is deprecated and is used for backward compatibility only. For details on the current way to perform the integration with BSM, see "HP Operations Manager" on page 298.
	➤ NetScout. For details, see "NetScout nGenius Integration" on page 455.
	➤ Node, Node - Running Software, and Tickets. For details, see "Understanding Node, Tickets, or Node - Running Software Integration Types" on page 423.
	Limitation: For details, see "Incident Ignored by EMS" in the document accessed by "How to Integrate HP Service Manager with Business Service Management Components" on page 351.
Relevant tasks	"How to Integrate Data from Third-Party Sources (EMS Data) into HP Business Service Management" on page 427
See also	"Integration Administration Application Overview" on page 422

Integration Main Settings

User interface elements are described below:

UI Element (A-Z)	Description
Data Source	The name of the integration data source.
Description	The description of the integration.
Name	The name of the integration.

HP OM Drilldown Settings

This section is displayed only when you select the HP OM integration (the HP Operations Manager integration). Note that this integration is deprecated and is used only for backward compatibility. For details on the current way to integrate HPOM and BSM see "HP Operations Manager" on page 298.

User interface elements are described below:

UI Element (A-Z)	Description

HP OM URL	**For HPOM integration only.**
	➤ The URL of the HP Operations Manager host.
	➤ This field is not mandatory.
	➤ This information is used to access the HP Operations Manager application using the OVO Drill Down shortcut menu option.
	➤ To enter the HP OM (Legacy) host automatically, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:
	    ➤ Select **Foundations**.
	    ➤ Select **Integrations with other application**.
	    ➤ In the Integrations with other applications - HP OM (Legacy) table, locate **The OVO host**. Modify as required.
	Limitation: For details about the menu option and the limitations, see "Operation Manager" in *Using Service Health*.

UI Element (A-Z)	Description

HP OM User Name	**For HPOM integration only.**
	
	➤ The name of the HPOM user.
	➤ This field is not mandatory.
	➤ This information is used to access the HP Operations Manager application using the OVO Drill Down shortcut menu option.
	➤ To enter the HPOM user name automatically, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:
	   ➤ Select **Foundations**.
	   ➤ Select **Integrations with other application**.
	   ➤ In the Integrations with other applications - HP OM (Legacy) table, locate **User of the OVO**. Modify as required.
	
	Limitation: For details about the menu option and the limitations, see "Operation Manager" in *Using Service Health*.

HP OM User Password	**For HPOM integration only.**
	
	➤ This field is not mandatory.
	➤ The password of the HP Operations Manager user.
	➤ This information is used to access the HP Operations Manager application using the OVO Drill Down shortcut menu option.
	➤ To enter the HP OM (Legacy) user password automatically, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integrations with other application**:
	   ➤ Select **Foundations**.
	   ➤ Select **Integrations with other application**.
	   ➤ In the Integrations with other applications - HP OM (Legacy) table, locate **User password of the OVO**. Modify as required.
	
	Limitation: For details about the menu option and the limitations, see "Operation Manager" in *Using Service Health*.

CI Relationship Area

Click the **CI Relationships Map** link to open the CIT relationship map dialog box where you can sketch the relationship map for the integration. This sketch is useful to help you draw which CI types are created and where the EMS monitors are located. This is only for illustration. For details, see "CIT Relationships Map Dialog Box" on page 452.

System Availability Management Area

Click the **System Availability Management** link to open the System Availability Management application where you can define the integration monitor for one of the out-of-box integrations or a new monitor for a new integration. The type of integration monitor is determined by the way the data is extracted or received (database, web service, log , SNMP). For details, see "Create an EMS integration (for Event or Ticket Samples)" on page 429 and see "Introduction to SAM Administration" in *Using System Availability Management*.

➤ To set up the HP OM Event Monitor, see "HP OM Event Monitor" in *Monitor Reference* in the SiteScope help.

➤ To set up the HP ServiceCenter Monitor, see "HP Service Manager Monitor" in *Monitor Reference* in the SiteScope help.

➤ To set up the NetScout Event Monitor, see "NetScout Event Monitor" in *Monitor Reference* in the SiteScope help.

➤ To set up the Technology SNMP Trap Integration monitor, see "Technology SNMP Trap Integration Monitor Overview" in *Monitor Reference* in the SiteScope help.

➤ To set up the Technology Database Integration Monitor, see "Technology Database Integration Monitor Overview" in *Monitor Reference* in the SiteScope help.

➤ To set up the Technology Log File Integration monitor, see "Technology Log File Integration Monitor Overview" in *Monitor Reference* in the SiteScope help.

➤ To set up the Technology Web Service Integration monitor, see "Technology Web Service Integration Monitor Overview" in *Monitor Reference* in the SiteScope help.

Limitation: If you have previously defined a SiteScope using this option and you reopen System Availability Management, the application does not display the SiteScope you have previously defined.

HI and KPI Assignments Area

This area enables you to specify the health indicator and KPI assignments defined for the current EMS integration.

CI Types Pane

This pane displays a hierarchy of CI types. You can select a CI type to view its assignments, edit an assignment, or add an assignment to the CI type.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
	Refresh. Click to refresh the CI Types pane and the Assignments pane display.
<CI Types>	Displays the hierarchy of the CI Types in the RTSM. You can select only System Monitor CI Types, or EMS Monitor CI Types.
Filter	This filter enables you to display, depending on your selection: ➤ **Show all assignments.** All assignments and propagation rules (default setting). ➤ **Show valid assignments only.** Only valid assignments. ➤ **Show invalid assignments only.** Only invalid assignments. If you want to resolve invalid assignments, open each assignment for editing. The dialog box that appears contains details on what needs to be fixed in the assignment definitions.

Assignments Pane

This pane displays details regarding the KPI and health indicator assignments for the CIT selected in the **CI Types** pane. Depending on the type of CIT, the assignment can be a Service Health assignment or an SLM assignment. Each type of assignment is displayed in its own table. Each table includes two tabs: **KPI Assignments**, and **Health Indicator Assignments**. Select a tab to display and configure the corresponding assignments. Within each table, each line represents one assignment on the selected CIT.

Important information	When you do not have a Service Level Management license, and you cannot create SLM assignments.

User interface elements are described below:

UI Element (A-Z)	Description
✳	**Add.** Click to create: ➤ In the Health Indicator Assignment tab, a health indicator assignment. For user interface details, see "Add/Edit Health Indicator Assignments for CI Type Dialog Box" in *Using Service Health*. ➤ In the KPI Assignments tab, a KPI Assignment. For user interface details, see "Add/Edit KPI Assignments for CI Type Dialog Box" in *Using Service Health*.
🗐	**Duplicate.** Click to copy a selected assignment, and open the copy for editing.
✏	**Edit**. Click to edit: ➤ In the Health Indicator Assignment tab, a new health indicator assignment. For user interface details, see "Add/Edit Health Indicator Assignments for CI Type Dialog Box" in *Using Service Health*. ➤ In the KPI Assignments tab, a new KPI Assignment. For user interface details, see "Add/Edit Health Indicator Assignments for CI Type Dialog Box" in *Using Service Health*.

UI Element (A-Z)	Description
✖	**Delete.** Click to delete one or more selected assignments. Assignments that are inherited from parent CITs cannot be deleted on the child CIT, but only on the parent CIT.
↺	**Restore to default.** Click to restore a selected overridden assignment to its original settings.
☑	**Select all.** Select all the assignments.
▢	**Clear Selection.** Clear the selection of assignments.
▷	**Start.** Click to start running a selected assignment on existing CIs, and on new CIs.
☐	**Stop.** Click to stop running a selected assignment.
⟳	**Synchronize CI Type.** Click to run assignments on the existing CIs of the selected CI Type. If you are working with the KPI Assignments tab the KPI assignments are run; if you are working with the Health Indicator Assignments tab the health indicator assignments are run. For details, see "Integration Administration Application Overview" on page 422.
⟳	**Refresh.** Click to refresh the Assignments pane display.
▥	**Change visible columns.** Click to open the Choose Columns to Display dialog box where you can select the columns you want to display in the table.
Assignment Name	The name of the assignment.
Description	The description of the assignment.
Health Indicators	Within the Health Indicator Assignments tab, contains a list of the health indicators that are assigned to CIs of the selected CIT, based on the assignment.

UI Element (A-Z)	Description
KPIs	Within the KPI Assignments tab, contains a list of the KPIs that are assigned to CIs of the selected CIT, based on the assignment.
Monitored By	List of values of the **Monitored By** attribute within the RTSM; the assignment is only applicable if the CI contains one of the listed values as its **Monitored By** attribute.
Status	The assignment status: ➤ **Running.** The assignment has been started and is running on the appropriate CIs. ➤ **Stopped.** The assignment has been stopped and is not running.

View Results Area

Click the **Integration Results** link to open the View Results page that displays the view corresponding to the integration you have created. The view includes all the CIs that were created by the integration.

❧ CIT Relationships Map Dialog Box

This dialog box enables you to add elements and relationships to the CIT relationships map.

To access	Click **Define the CIT relationships map** in the Add Integration Dialog Box.
Important information	Sketch the relationships map to help you when you define the assignment in the **HI and KPI Assignments** area.
	For details on how to work with the relationships map, see "How to Add CITs and Relationships to a Relationship Map" on page 434.
	For details about the toolbar, see "Toolbar Options" in the *Modeling Guide*.
	For details about the right-click options, see "Shortcut Menu Options" in the *Modeling Guide*.

🔍 EMS Integrations Admin Page

This page lists existing EMS integrations, and enables you to define new integrations or edit existing ones. In addition, the page can also display legacy integrations of type Host-Application.

To access	**Admin** > **Integrations** > **EMS Integrations Admin**
Important information	This page also enables you to access the HP Operations Manager, HP Service Manager, and NetScout predefined SiteScope monitor definitions and assignments used in the integrations of Business Service Management with those products. For more information about the integration with: ➤ HP Operations Manager. Legacy integration. For details, see "HP Operations Manager" on page 298. ➤ HP Service Manager, see "How to Integrate HP Service Manager with Business Service Management Components" on page 351. ➤ NetScout, see "How to Display NetScout Data in BSM" on page 459. Legacy Host-Application integrations are displayed in this page for backward compatibility with legacy EMS integrations. Note that you cannot create new integrations of that type.
Relevant tasks	"How to Integrate Data from Third-Party Sources (EMS Data) into HP Business Service Management" on page 427

User interface elements are described below:

UI Element (A-Z)	Description
	New. Opens the Add Integration dialog box opens where you can create a new integration. For user interface details, see "Add Integration Dialog Box" on page 441.
	Edit. Opens the Edit Integration dialog box where you can edit the selected integration. For user interface details, see "Edit Integration Dialog Box" on page 444.
	Delete. Deletes the selected integration. When you delete the integration, the assignments, view and TQLs created for it are automatically deleted as well. **Note:** You cannot delete out-of-the-box integrations.
Description	The description of the integration.
Name	The name of the integration.

17

NetScout nGenius Integration

This chapter includes:

Concepts

➤ NetScout Integration Overview on page 456

Tasks

➤ How to Display NetScout Data in BSM on page 459

Concepts

🔩 NetScout Integration Overview

This section provides an overview of NetScout and describes the main concepts of the NetScout integration.

This section includes the following topics:

➤ "Overview of NetScout" on page 456

➤ "NetScout EMS Integration" on page 456

➤ "NetScout View and Topology" on page 457

Overview of NetScout

NetScout nGenius monitors network traffic and reports performance metrics about applications routing through that network. NetScout integration shows NetScout alarms in BSM Service Health. NetScout sends SNMP traps containing information about the alerting instances that could map to existing CI types in the RTSM (Run-time Service Model).

NetScout EMS Integration

The assignment of the NetScout EMS integration enriches the monitor-level Application Monitor CIs with the appropriate KPIs, rules, and shortcut menus that are to be assigned automatically to the CIs when the condition occurs, and the assignment is running.

Note: The Application Monitor CIs assignment is used only when the machine, on which NetScout nGenius is installed, is monitored using SiteScope version 10.0 or earlier.

NetScout View and Topology

NetScout analyzes packets that include information about the applications running through specific routers or switches. When there is a problem, the packets can send in alarms with information about the problematic application.

The application alarms SNMP trap reports about problems discovered in an application using information analyzed from packets. The application information is not linked to the router information as the routing path is not constant and may vary depending on network traffic decisions.

The NetScout integration creates the NetScout view. The NetScout view includes CIs that represent the application alarms.

The NetScout view includes the Application CI, the EMS Monitor CI, and their relationship.

For details on integrating NetScout data in BSM, see "How to Display NetScout Data in BSM" on page 459.

All the sample information sent by NetScout is displayed by the **Application** KPIs attached to the **Application Monitor** CIs. The **SiteScope EMS Multiple Events Rule** calculates the statuses of those KPIs based on data obtained from NetScout samples.

The **SiteScope EMS Rule** tooltip corresponding to the **SiteScope EMS Multiple Events Rule** is preconfigured to provide the appropriate infrastructure to work with the NetScout-related CIs in Service Health. For details on the Application KPI, see "Software Performance" in *Using Service Health*.

For details on:

➤ The **SiteScope EMS Multiple Events Rule**, see "SiteScope EMS Multiple Events Rule" in *Using Service Health*.

➤ The **SiteScope EMS Rule** tooltip, see "Example of a SiteScope EMS Rule Tooltip" in *Using Service Health*.

Tasks

⚒ How to Display NetScout Data in BSM

NetScout data can be displayed in BSM using the EMS Integration tool.

For additional information about EMS integration, see "Integration Administration Application Overview" on page 422.

This task includes the following steps:

➤ "Prerequisite" on page 459

➤ "Configure the integration" on page 459

➤ "Customize the integration – optional" on page 460

➤ "View NetScout data in the NetScout View and enrich the view" on page 461

1 Prerequisite

In the NetScout nGenius server, select **Device** > **Global settings**, and enter, in the Server IP Addresses box, the SiteScope Server IP address of the SiteScope that reports to BSM.

2 Configure the integration

The NetScout integration is predefined. The integration retrieves the samples provided by the NetScout nGenius system, creates the appropriate topology in BSM (application CIs), creates a view, assigns the appropriate KPIs, rules, shortcut menus, shortcut menu items, and tooltips depending on the type of sample and displays the information using the created view.

To configure the NetScout integration, select **Admin > Integrations > EMS Integration Admin**, select NetScout and click **Edit**. In the Edit Integration dialog box:

a Add the NetScout Event Monitor to a SiteScope monitor group created for this monitor and other Integration Monitor types in **Step 2. Retrieve data from EMS system using System Availability Management**. The monitor is used to retrieve data from the NetScout server using System Availability Management Administration. It is recommended that you configure Integrations Monitors only after a connection between the SiteScope and HP Business Service Management is established. For concept details, see "How to Integrate Data From a NetScout System" in *Monitor Reference* in the SiteScope documentation library.

b Activate the Application Monitor CIs data assignment rule in **Step 3. Define the data assignments rules**. The data assignment rule is automatically deactivated, by default. The data assignment rule includes the assignment rules to create the topology for the Application Monitor CIs.

For details on the assignment rules, see "Edit Integration Dialog Box" on page 444.

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.

---

3 Customize the integration – optional

You can use the EMS Integrations application to customize a NetScout integration. The integration forwards the retrieved data captured from the NetScout system by the SiteScope NetScout Event Monitor to BSM, and creates the appropriate topology (Application CIs). For details on the available customization, see "Edit Integration Dialog Box" on page 444.

4 View NetScout data in the NetScout View and enrich the view

You can view NetScout application alarms in the NetScout view. For details, see "NetScout View and Topology" on page 457.

To enrich the view, attach IT Universe CIs to the appropriate Application Monitor CIs. For details on attaching CIs, see "Insert Relationship Dialog Box" in the *Modeling Guide*.

Index