HP Service Health Reporter

Software Version: 9.40
Windows ® and Linux operating systems

Administration Guide

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2010 - 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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

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

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

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

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

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

Support

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

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

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

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

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

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

To find more information about access levels, go to:

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

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

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Administration Guide

This guide provides an overview of the Administration Console and guides you through the step-by-step tasks that you have to perform using the Administration Console.

This guide is organized into the following sections based on the tasks you must perform on the Administration Console:

Getting Started

This section guides you through the essential administrative tasks that you must perform immediately after installing SHR. It includes performing the post-install configuration tasks, configuring topology collection, and configuring data collection from the various data sources.

Monitoring SHR

This section introduces you to the various monitoring tasks that you can perform through the Administration Console. It explains how to monitor the database content, the data processes, the database, error logs, and the application server platform.

Administering SHR

This section explains the various administrative tasks that you can perform through the Administration Console. It explains how to view the database credentials and licensing information, configure security access and data retention of the database, control the data processes, manage user accounts and services, and configure the time shifts.

Administration Console Screens

This section provides an overview of each screen that is available on the Administration Console.

Role of the Administrator

As an administrator, you must perform the following tasks after you install the SHR software. Here is the priority listing of the required tasks:

- Configuration tasks—These tasks are performed immediately after installing the SHR. You must perform these tasks to ensure that SHR is up and running and data collection operations take place according to your requirements. Configuration tasks include:

- Performing various post-install configuration tasks.

- Selecting and installing the required Content Packs[1].

- Configuring your data sources to provide topology information[2] to SHR for data collection.

- Configuring the different data collectors to collect fact data based on the collection policies defined in the Content Packs.

- Monitoring tasks—These tasks help you monitor the performance of SHR and identify and troubleshoot any problems with the application and the database. Monitoring tasks include:
  - Monitoring the data that is loaded in the SHR database for each installed Content Pack.

  - Monitoring and troubleshooting the data processes.

  - Monitoring the performance and availability of the SHR database and the host platform.

  - Tracking the errors reported by SHR.

  - Monitoring the SHR, SAP BOBJ, and database services.

- Administrative tasks—These tasks help you ensure that the SHR's data and database are useful, usable, available, and accurate at all times. Administrative tasks include:
  - Setting up database access and security.

  - Managing the product license.

  - Controlling the execution of data processes.

  - Defining data retention policies for each Content Pack.

Accessing the Administration Console

1. Click **Start > Programs > HP Software > Service Health Reporter> Administration**.
   The Administration Console Login page appears.

   You can also access the Administration Console using the following links:

   - Type the SHR host system address in a web browser. The default address is **http://<server name>:21411/BSMRApp/logon.jsp** where *server name* refers to the name of the host

---

[1]SHR provides out-of-the-box business intelligent solutions called Content Packs that define the data collection and data warehousing policies. The Content Packs also contain the required information to display reports.
[2]The relationship between Configuration Items (CIs), such as applications, servers, and system resources in your IT environment.

system on which you have installed SHR. In addition, you can use this URL to remotely access the Administration Console from any other system.

- Click Administration Console on the Administration Console on the SHR landing page **http://<servername>:<port>/MySHR/index.html**, where *server name* is name of the host system on which SHR is installed.

For information about web browser requirements to access the Administration Console, see the *HP Service Health Reporter Support Matrix*.

2. Type:

Field	Description
Login Name	Name of the SHR administrator.
	Note: For first-time access, use the default login name and password. The default login name is Administrator. There is no password. The default user, Administrator, has complete administrative privileges.
	Important: You should change the default login name and password after the first access to prevent unauthorized use. For the steps, see Access SAP BusinessObjects Central Management Console.
Password	Password of the SHR administrator.

3. Click **Log In**.
   The Administration Console opens.

Administration Console page

After you complete the post-install configuration task, the Home page of the Administration Console appears. The Home page includes:

Name	Description
Task pane	SHR collection configuration, administration, and monitoring options: • Home • Topology Source • Collection Configuration • Administration • Internal Monitoring • Help
License details	Summary of the SHR license information.
Time zone	Time zone information.
User	Name of the current SHR user.
Logout	Option to log out of the Administration Console.
Help	Option to launch the *Online Help for Administrators*.
View pane	View the administration, configuration, and monitoring options and attributes.

Logging out of the Administration Console

To prevent unauthorized access, log out of the Administration Console after use.

From the Administration Console, click **Logout** to log out of the Administration Console. The `You are successfully logged out` message appears, after which the web browser window automatically closes.

SHR log files

SHR uses the log4j API for most of it logging purposes. It maintains a log file for each of the its modules, such as collector, loader, metadata repository, internal monitoring, Administration Console, package manager, and data processing. These log files are placed in the `%PMDB_HOME%\log` folder. SHR also maintains an application-wide log file that contains error messages from all the modules. These log file can be used for troubleshooting purposes.

The log files available in SHR are as follows:

Log File	Module	Description
aggregate.log	Aggregate	Contains log messages related to the loading of data from the rate tables to the hourly, daily, and forecast tables, and from the hourly tables to the daily tables.
aggrgen.log	Aggregate	Contains log messages related to aggregate procedure generation. `Appender:aggrgenAppender`
audit.log	Aggregate, trendproc, trendtimer	Records the start time, end time, and duration of back-end processes. When a process begins, the file assigns a Process Identification (PID) that also records when the process ends, showing that the PID for the process was terminated.
backend.log	Aggregate, trendproc, trendtimer	Contains log information for all steps in the data processing job. `Appender: backendLogAppender`
BOEInstall_0.log BusinessObjects.12.7.log	Business Objects	SAP BusinessObjects installation log files.
BSMRApp.log	NA	Application-wide log file that contains error messages from all the SHR modules, except data processing. `Appender: bsmrappender`
BSMRCollectionService.log	Collector	Log file for the PMDB Platform Collection Service.
BSMRDBLoggerService.log	Logger	Log file for the PMDB Platform DB Logger Service.

Log File	Module	Description
bsmrfrontend.log	Administration Console	Contains log messages related to the Administration Console UI web application. Appender: `BSMRFrontEndAppender`
bsmrim.log	Internal Monitoring	Contains log messages related to the internal monitoring of data processing job streams, Sybase IQ database, Performance Management database (PMDB) platform, and Content Packs. Appender: `BSMRIMAppender`
BSMRIMService.log	Internal Monitoring	Log file for the PMDB Platform IM Service.
catalina*.log	Administrator Console	Contains log messages about the Apache Tomcat server.
collections.log	Collector	Contains log messages related to the collection framework such as data sources configured collection, job scheduling, and maintenance. Appender: `collectionAppender`
collectStep.log	Collect	Contains log messages related to the collect step that moves data from the {PMDB_HOME}/collect directory to the {PMDB_HOME}/stage directory Appender: `collectAppender`
customer.log	Customer Enrichment	Contains log messages on customer enrichment.

Log File	Module	Description
customgroup.log	Custom Group	Contains log messages related to importing of custom groups defined in an XML file. Appender: `customgroupAppender`
dbcollector.log	Collector	Contains log messages related to database collection. Appender: `dbCollectorAppender`
downtime.log	Downtime	Contains log messages related to configuring downtime and enriching the performance data with configured downtime information. Appender: `downtimeAppender`
dw_abclauncher.log	Data processing	Contains log messages related to job streams. Log messages specific to a process can be seen in the process-specific log file. For example, loader.log for the loader process. Appender: `abclauncher-RollinglogFileAppender`
enrich.log	Location Enrichment	Contains log messages on generic enrichments.
hpacollector.log	Collector	Contains log messages related to HP Performance Agent collection. Appender: `hpaCollectorAppender`
IAEngine.log	Internal Alerting	Contains log messages related to Internal Alerts.
IAEvent.log	Internal Alerting	Contains log messages related to Internal Alerts.

Log File	Module	Description
License.log	License	Contain messages for license-related tasks. `Appender: licenseAppender`
loader.log	Loader	Contains log messages related to data loading from the stage area to the data store.
loadgen.log	Loader	Contains log messages related to data load procedure generation. `Appender :loadgenAppender`
localhost*.log	Administration Console	Contains log messages related to Server Access.
location.log	Location Enrichment	Contains log messages from location enrichment.
mapperStep.log	Mapper	Contains log messages related to transformation of collected data. Transformation includes pivot transform, rows filtering, and so on. `Appender: mapperAppender`
metadata.log	Metadata Repository	Contains log messages related to metadata repository persistence, access, and modification. `Appender: MetadataRepositoryAppender`
mybsm.log	MyBSM Integration	Contains log messages related to launching of SHR reports from the MyBSM console.

Log File	Module	Description
OvInstallerLog.txt	Installer	This folder also stores log files for each component of SHR such as LCore components, OVPerl, and so on.
packagemanager.log	Package Manager	Appender: `pkgmgrAppender`
pmdb.iqmsg	Sybase IQ	Sybase IQ log file information
pollerDataProcessor.log	Collector	Contains logs related to data download from remote collectors to SHR server.
Postgresql-<date and time>.log	PostgreSQL	PostgreSQL log file information
postinstallconfig.log	Post Install	Details on database schema creation on Sybase IQ, details on SHR Management database schema creation on Postgresql. Appender: `postinstallAppender`
reconcilStep.log	Reconciliation	Contains log messages related to reconciliation of collected data. Appender: `reconcileAppender`
remotepoller.log	Remote Collector	Contains log messages related to configuration and metadata synchronization and data transfer between SHR server and the different collectors configured.
runProc.log	Run Proc	Contains log messages related to execution of database procedures and functions associated with each content pack.
reloadAppender	Reload	Log file for the contrib utility (reload.exe) that handles reload of failed data.

Log File	Module	Description
shiftmaint.log	Shift Management	Contains log messages related to populating the shift fact tables based on shift configured in Administration Console. Appender: `shiftMaintAppender`
sis_aggregate.log	Aggregate	Contains logs from the SiteScope aggregate process that runs as part of collection service
siscollector.log	SiteScope Collector	Contains logs from the SiteScope collector (for both GDI and DA)
stage.log	Stage	Contains log messages related to data staging, and purging of staging area. Appender: `stageAppender`
stderr*.log	Administrator Console	Contains messages logged to standard error by the Tomcat server.
stdout*.log	Administrator Console	Contains messages logged to standard output by the Tomcat server.
topologycollector.log	Collector	Contains log messages related to topology collection. Appender: `topologyCollectorAppender`
trend.log	Aggregate, trendproc, trendtimer	Contains messages for all back-end processes of SHR. Each message specifies the start and end time for the logged process.
TrendTimerService.log	Trend Timer	Contains log messages related to the SHR timer service.
VC_collector/collector.log	VC Collector	`VC Collector logfiles` Appender: `vcAppender`

Log File	Module	Description
(Only on Linux) <hostname>.0001.srvlog<hostname>.0001.st derr	SybaseIQ	`Sybase database log file.`

SHR service log files

All SHR services have a log file associated with it. These log files contain console error messages. These log files are not controlled through log4j API and are overwritten during service startup.

Log file	Service
BSMRService.log	Log file for the Performance Management Database (PMDB)[1] Platform Administrator Service.
BSMRCollectionService.log	Log file for the PMDB Platform Collection Service.
BSMRDBLoggerService.log	Log file for the PMDB Platform DB Logger Service.
BSMRIMService.log	Log file for the PMDB Platform IM Service.
SybaseService.log	Log file for the PMDB Platform Sybase IQ Service.
Trend.log	Log file for PMDB Platform Timer service
Postgresql-<date and time>.log	Log file for the SHR PostgreSQL service.

Log file message format

All entries in the log files have the following format

Format	Description
Timestamp	The timestamp field represents the time the log entry occurred. It uses a 24-hour clock with the YYYY-MM-DD hh:mm:ss,nnn format.
Severity	The severity field is the severity level for the log entry. The severity levels are DEBUG, INFO, WARN, ERROR, FATAL.

[1]A common repository of the health, performance, and availability data of the IT elements in your environment. The platform data store contains performance data that is processed, transformed, and aggregated in the data store, based on the metadata specifications in the content packs.

Format	Description
Class_name	The fully qualified class name of the caller issuing the logging request.
Method_name	The method name where the logging request was issued.
Message	The application-supplied message associated with the logging event.

Getting started

After you install the SHR application, you must perform the following configuration tasks to ensure that SHR is operational and can start collecting data from the various data sources:

Task 1: Perform the post-install configuration tasks

You must perform the post-install configurations tasks immediately after installing the SHR application. These tasks help you set up the SHR database user account details and define the database schema. This guide provides a brief overview of the post-install configuration tasks. For the step-by-step procedure to perform these tasks, see the *HP Service Health Reporter Configuration Guide*

Task 2: Configure the topology source

You must configure the topology sources from where SHR can retrieve the topology information about your environment. For more information, see Managing the enterprise topology.

Task 3: Install the Content Pack components

Select and install the required Content Pack components from the **Administration Console > Administration > Deployment Manager** page . The selection of the Content Pack components depends on the type of your SHR deployment environment. For the step-by-step procedure for installing the Content Packs, see the *HP Service Health Reporter Configuration Guide* .

Task 4: Configure the data sources

After you finish configuring the topology sources, you can configure the data sources from where SHR data collectors can collect fact data for the various installed Content Pack components. For more information, see Configuring and managing data collection.

Configuring SHR

The Post-Install Wizard is a web-based user interface (UI) to perform the mandatory SHR post-installation configuration tasks. The wizard sequentially takes you through the steps for configuring the SHR database, creating the database schema, and configuring the management database.

The Post-Install Wizard appears when you launch the SHR Administration Console for the first time. You can access the Administration Console only after you successfully complete the SHR post-installation configuration tasks.

Using the Post-Install Wizard, you can perform the following configuration tasks:

- Configure the time zone for SHR.

- Create the database for SHR and configure an administrator user account to access the database.

- Create the database schema by specifying the data collection volume.

- Manage the user account for the management database, which is a repository used by SHR to store run-time data such as data processing[1] stream status, changed table status, and node information.

- Configure the topology source for the data collection.

SHR Configuration Wizard

The SHR Configuration Wizard opens when you run the Administration Console for the first time after installing SHR. This wizard takes you through a series of pages where you must configure the SHR database before you can start using SHR to collect data and generate reports.

The SHR Configuration Wizard includes the following pages:

Configure SHR Parameter/s

On the Configure SHR Parameter/s page, select the time zone, that is, **GMT** or **Local**, under which you want SHR to operate.

Configure Database Connection page

SHR uses the Sybase IQ[2] database engine to create the database. On the Configure Database Connection page, you must provide the details of the database server where you want to create a database for SHR.

The Configure Database Connection page includes:

Field	Description
Database Type	Type of database that you want to configure for SHR. SHR only supports Sybase IQ.
Remote Database	Select this option if you have performed a remote Sybase IQ installation.

[1]Data processing refers to a set of best practices in the context of data storage. They have been developed by HP to improve the quality and control during the loading of data into data stores.
[2]Sybase IQ is a column-oriented relational database used for business intelligence and data ware-housing. As a column-oriented database management system (DBMS), Sybase IQ stores data tables as sections of columns of data rather than as rows of data.

Field	Description
Host name	Name or IP address of the host where the Sybase IQ database server is running.
Port	Port number to query the database; the default port is 21424.
Server name	Name of the Sybase IQ server. **Important**: The server name displayed in this field is only for informational purposes. You must not change the server name at any time.
User name	Name of the Sybase IQ database user; the user must have database administrator (DBA) privileges.
Password	Password of the Sybase IQ database user.
Admin Password	Password for the SHR database administrator. The SHR Configuration Wizard uses this password to create the SHR database administrator account.
Confirm Admin Password	Retype the same password for confirmation purposes.

Create Database Schema page

On the Create Database Schema page, you must specify the deployment size of the Sybase IQ database to plan your data collection and retention. The deployment size or data volume indicates the number of nodes from where SHR will collect data. Nodes include both directly managed nodes, such as in the case of HP Operations agent, where SHR directly collect the data from the HP Operations agent data source, and indirectly managed nodes, such as those managed by HP Business Service Management, HP OMi, and HPOM. For these nodes, SHR collects the data from the Profile database, HP OMi, and HPOM data sources. Based on your selection, SHR calculates and displays the recommended database size.

The Create Database Schema page includes:

Field	Description
Select Deployment Size	The total number of managed nodes from which SHR will collect the required data: ● Low Volume—This option enables SHR to support data collection from less than 500 nodes. ● Medium Volume—This option enables SHR to support data collection from 500 to 5000 nodes.
IQ Main Cache(MB)	The recommended size of the main buffer cache for the Sybase IQ main store. The value displayed in this field changes based on the type of deployment size you select.

Field	Description
IQ Temporary Cache (MB)	The recommended size of the temporary buffer size for the Sybase IQ temporary store. The value displayed in this field changes based on the type of deployment size you select.
IQ DBSpace Size(MB)	The recommended size for the IQ_System_Main dbspace, which stores the main database files. You can modify this size.
IQ Temporary DBSpace Size(MB)	The recommended size for the IQ_System_Temp dbspace, which stores the temporary database files. You can modify this size.
Choose Database File Location	The location where the database files will be stored.

Note: You can reconfigure the deployment size of the database later by using the Database Administration Utilities, which will override your current selection.

Create Management Database page

The SHR management database refers to the online transaction processing (OLTP) store used by SHR to store its run-time data such as job stream status, changed tables status, and node information. On the Create Management Database page, you can change the password of the administrator account for accessing the management database.

The Create Management Database page includes:

Field	Description
User name	Name of the PostgreSQL database administrator.
Password	Password of the PostgreSQL database administrator. The default value is **PMDB92_admin@hp**.
User name	Name of the SHR management database user. This field is disabled by default.
New Password	New password of the SHR management database user.
Confirm New Password	Retype the password for confirmation purpose.

Configure Topology Source

You can configure the topology source on the Configure Topology Source page.

The Configure Topology Source page includes:

Field	Description
Service Definition Source	Option to select RTSM or HPOM or VMware vCenter as the source of the service definition (topology) data. **Note:** You must select the topology source during post-install configuration of SHR. You cannot switch among the topology sources (RTSM, HPOM, and VMware vCenter) after wards.
Host name	IP address or fully-qualified name (FQDN) of the service definition host system.
Connection Status	Status of the service definition source connection. • ✅ Indicates that the SHR host system is connected to the data source. • ❌ Indicates that the SHR host system is not connected to the data source.
Configuration	Modify an existing service definition source connection.
Test Connection	Test a service definition source connection.
Create New	Create a new service definition source connection.
Save	Save a specific service definition source configuration attribute.

For information on how to configure a topology source connection, see Managing the enterprise topology.

Summary page

You can review the details of the database connection and the management database on the Summary page.

The Summary page includes:

Field	Description
Database Connection	Details of the database connection. Details include: • Host name • Port
Management Database	Details of the SHR management database. Details include: • Host name • Port

Note: The HP Service Health Reporter Configuration Wizard supports session state persistence, which enables you to resume and continue a halted or previously-interrupted configuration session.

Managing the enterprise topology

Before SHR can start collecting domain-specific data, such as fact data related to applications, databases, and system resources, from the nodes or Configuration Items (CIs), it must first identify and collect the topology information[1] about the managed environment, your business services, and the underlying IT components. Using this information, SHR can align and reconcile the collected fact data for long-term storage, analytics, and cross-domain reporting.

Enterprise topology source

The enterprise topology includes IT components such as applications, servers, databases, and system resources, which are monitored by HP business service-oriented product, such as Run-time Service Model (RTSM) or HPOM. These monitored components are called Configuration Items (CIs). Identifying the enterprise topology helps you understand how each of your business services is linked to the underlying CIs. It provides a map of the dependencies of the business services to the IT infrastructure. It helps you track configuration changes.

SHR supports the collection of topology-related data from the following data sources:

- RTSM—is the central repository for the configuration information, which stores and handles the topology and configuration data that is collected and updated through data collectors by the Discovery[2] process. The information concerning the discovered CIs and their relationships are used to generate a topology model of all the components that constitute your IT environment on which your business functions.

- HPOM/OMi10—is a distributed, client-server software solution designed to help system administrators detect, solve, and prevent problems that occur in networks, systems, and applications in any enterprise. HPOM collects data that enable you to maximize IT system performance, reduce downtime, delegate tasks to operators, and reduce costs. HPOM constantly monitors thousands of events[3] that occur on all your managed nodes[4] and presents just the information you want to know just when you need it. HPOM uses a component called Service Navigator (SN) to create the topology service tree for the managed nodes and builds the relationship between the nodes and the applications in your environment.

The collection of the topology data from these data sources depends on the type of scenario in which SHR is deployed. SHR currently supports three types of deployment scenarios:

[1]The relationship between Configuration Items (CIs), such as applications, servers, databases, and system resources in your IT environment.
[2]The mechanism that enables you to collect data about your system by discovering the IT infra-structure resources and their interdependencies. Discovery can discover such resources as applic-ations, databases, network devices, different types of servers, and so on. Each discovered IT resource is stored in the RTSM, where it is represented as a managed CI.
[3]A particular fault or incident within the computing environment that occurs on an object.
[4]Managed nodes are computers that are controlled and monitored by HPOM.

- BSM Service and Operations Bridge (SaOB)

- Application Performance Management (APM)

- HPOM

If SHR is deployed within the BSM SaOB or the APM environment, you must configure the data collector to collect topology data from RTSM. If SHR is deployed in the HPOM environment, the HPOM database becomes the source of the topology information for SHR.

For more information about deployment scenarios, see the *HP Service Health Reporter Concepts Guide*.

Managing the data collection

SHR uses various out-of-the-box collectors to collect topology data:

- RTSM collector—Collects topology information and data about the various CI types in your environment from the RTSM database. The data to be collected is defined by the RTSM view provided with each Content Pack.

- HPOM collector—Collects topology information and data about the various CI types in your environment from the HPOM database. The information collected by the HPOM collector is limited to node list and node groups.

These data collectors collect the required data from the RTSM or HPOM service definition sources, which you must configure in SHR. You can create and configure RTSM or HPOM service definition source connections on the Service Definition page of the Administration Console. In addition, you can schedule SHR to collect data from the data repositories at specific intervals. You can also add new data source connections or modify the existing connections.

Using the Service Definition page, you can perform the following RTSM or HPOM topology data collection tasks:

- Select a service definition source

- Create a service definition source connection

- Modify a service definition source connection

- Enable or disable a service definition data collection

- Schedule a service definition synchronization

- Test the service definition source connection

- View a service definition source connection status

- View a service definition data collection status

Select a service definition source

Before you can configure the topology definition data connections, you must first select the source from where SHR should retrieve the topology information. This topology source depends on the type of deployment scenario used for SHR. You can view the topology source on the Service Definition page of the Administration Console.

To select the service definition source:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Under **Service Definition Source**, perform one of the following steps:
   - Select **RTSM** if you want to configure RTSM as the topology source for SHR.

   - Select **HP OM** if you want to configure HPOM as the topology source for SHR.

   - Select **VMware vCenter** if you want to configure VMware vCenter as the topology source for SHR

You cannot change the topology source after it has been configured on the Service Definition page. All the other tasks that you can perform on this page, such as creating a new data source connection, enabling collection, scheduling the frequency, and testing the connections, is available only for the selected source.

Create a service definition source connection

To create an RTSM service definition connection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Ensure that the required service definition source is selected under **Service Definition Source**.

3. Click **Create New**.
   The Connection Parameters dialog box opens.

4. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the Business Service Management (BSM) server. If your BSM deployment is distributed, type the name of the gateway server in this field. **Note:** In a distributed BSM deployment with multiple gateway servers and load balancer configured, type the virtual IP address of the load balancer in this field.
Port	Port number to query the RTSM web service. The port number is 80.
User name	Name of the RTSM web service user. The default user name is admin.
Password	Password of the RTSM web service user. The default password is admin.
Collection Station	This option is used for a collector installed on a remote system.

5. Click **OK**.

6. Click **Save**.

7. In the message box, click **Yes**.
   A `Saved Successfully` message appears in the Information message panel.

Note: You can create a single RTSM data source connection. The Create New button is disabled by default at the data source connection is created.

To create an HPOM service definition connection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Click **Create New**.
   The **Connection Parameters** dialog box opens.
   Note: If you are using the database method of authentication to connect to the HPOM database server, you must provide the user details that have the select and connect permissions for the "openview" database here.

3. Type:

Field	Description
Datasource Type	Select the type of HPOM that is configured in your environment. The options include: ■ HPOM for Windows ■ HPOM for UNIX ■ HPOM for LINUX ■ HPOM for Solaris
Database Type	Depending on the data source type that you select, the database type is automatically selected for you. For the HPOM for Windows data source type, the database type is MSSQL. For the HPOM for UNIX, HPOM for LINUX, or HPOM for Solaris, the database type is Oracle.
Database in Oracle RAC	Option to enable HPOM database on Oracle RAC. This option is not displayed when HPOM for Windows is selected.
Service Name	Specify the name by which SHR connects to the Oracle instance. This option appears only if Database in Oracle RAC is selected.
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the SHR system. This option appears only if OM on Oracle RAC is selected.
Host name	IP address or fully-qualified domain name (FQDN)of the HPOM database server. If the HPOM database is configured on a remote system, the machine name of the remote system must be provided here. Host name is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Database instance	System identifier (SID) of the database instance. The default database instance is OVOPS. Database instance is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected.
Database name	Name of the HPOM database. This field only appears if HPOM for Windows is selected as the data source type. The name of the database is openview.

Field	Description
Port	Port number to query the HPOM database server. Port number is not displayed when the database type is Oracle and Management DB on Oracle RAC is selected. To find the port number, see the *Configuration Guide*.
Windows Authentication	Option to enable Windows authentication for accessing the HPOM database. The user can use the same credentials to access HPOM as that of the Windows system hosting the database. This option only appears if HPOM for Windows is selected as the data source type.
User name	Name of the HPOM database user. **Note**: For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.
Password	Password of the HPOM database user. **Note**: For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.

6. In the message box, click **Yes**.
   A Saved Successfully message appears in the Information message panel.

Note: The default SQL Server Express that is installed with HPOM for Windows does not accept remote connections.

Data collection for the newly created service definition data source is enabled by default. In addition, the collection frequency is scheduled for every 24 hours.

Note: When you create a data source connection for HPOM on the Service Definition page, the same data source connection appears on the Operation Manager page as well. However, updating the data source connection on the Service Definition page does not update the connection details on the Operation Manager page.

To create a VMware vCenter service definition connection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Click **Create New**.
   The **Connection Parameters** dialog box opens.

3. Type:

Field	Description
Host name	IP address or FQDN of the VMware vCenter server.
User name	Name of the VMware vCenter user.
Password	Password of the VMware vCenter user.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.

6. In the message box, click **Yes**.
   A `Saved Successfully` message appears in the Information message panel.

Modify a service definition source connection

To modify an RTSM service definition connection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. For a specific host, click **Configure**.
   The Connection Parameters dialog box appears.

3. In the **Connection Parameters** dialog box, type the following connection parameters:

Field	Description
Host name	IP address or FQDN of the Business Service Management server. You cannot modify the host name after it has been specified during the creation process. This field is disabled by default.
Port	Port number to query the RTSM web service. The default port is 0.

Field	Description
User name	Name of the RTSM web service user. The default user name is admin.
Password	Password of the RTSM web service user. The default password is admin.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

To modify an HPOM service definition connection:

1. From the Administration Console, select **Topology Source > Service Definition**.
   The Service Definition page opens.

2. For a specific host, click **Configure**.
   The Connection Parameters dialog box appears.
   Note: If you are using the database method of authentication to connect to the HPOM database server, you must provide the user details that have the select and connect permissions for the "openview" database here.

3. In the **Connection Parameters** dialog box, type the following connection parameters:

Field	Description
Datasource Type	Select the type of HPOM that is configured in your environment. The options include: ■ HPOM for Windows ■ HPOM for UNIX ■ HPOM for LINUX ■ HPOM for Solaris You cannot modify the data source type after it has been selected during the creation process. This field is disabled by default.

Field	Description
Database Type	Depending on the data source type that you select, the database type is automatically selected for you. For the HPOM for Windows data source type, the database type is MSSQL. The database type is Oracle for the HPOM for UNIX, LINUX, and Solaris. You cannot modify the database type after it has been selected during the creation process. This field is disabled by default.
Database in Oracle RAC	Option to enable HPOM database on Oracle RAC. This option is not displayed when HPOM for Windows is selected.
Service Name	Specify the name by which SHR connects to the Oracle instance. This option appears only if Database in Oracle RAC is selected.
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the SHR system. This option appears only if OM on Oracle RAC is selected.
Host name	Address (IP or FQDN) of the HPOM database server. You cannot modify the host name after it has been specified during the creation process. This field is disabled by default
Database instance	System identifier (SID) of the database instance. The default database instance is OVOPS.
Database name	Name of the HPOM database. This field only appears if HPOM for Windows is selected as the data source type. The name of the database is openview.
Port	Port number to query the HPOM database server. To find the port number, see the *Configuration Guide*.
Windows Authentication	Option to enable Windows authentication for accessing the HPOM database. The user can use the same credentials to access HPOM as that of the Windows system hosting the database. This option only appears if HPOM for Windows is selected as the data source type.
User name	Name of the HPOM database user. **Note**: For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.

Field	Description
Password	Password of the HPOM database user. **Note**: For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

To modify a VMware vCenter service definition connection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. For a specific host, click **Configure**.
   The Connection Parameters dialog box appears.

3. In the **Connection Parameters** dialog box, type the following connection parameters:

Field	Description
Host name	IP address or FQDN of the VMware vCenter server.
User name	Name of the VMware vCenter user.
Password	Password of the VMware vCenter user.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.

6. In the message box, click **Yes**.
   A `Saved Successfully` message appears in the Information message panel.

Enable or disable a service definition data collection

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. For a specific host, perform any one of the followings steps:
   - Select the check box in the **Enable Collection** column to enable data collection.

   - Clear the check box in the **Enable Collection** column to disable data collection.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Schedule a service definition collection

To schedule an RTSM service definition collection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. For one or more hosts, specify a synchronization time between 1 and 24 hours in the **Hrs** box in the **Schedule Frequency** column.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

To schedule an HPOM service definition collection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. For one or more hosts, specify a synchronization time between 1 and 24 hours in the **Hrs** box under **Schedule HP OM Synchronization**, and then click **Apply**.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

To schedule a VMware vCenter service definition collection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. For one or more hosts, specify a synchronization time between 1 and 24 hours in the **Mins** box under **Schedule VMware vCenter Synchronization**, and then click **Apply**

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Test the service definition source connection

To test the RTSM service definition source connection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Click **Test Connection**.
   A `Test Connection Successful` message appears in the Information message panel if the connection exists.

   Note: The test connection to RTSM topology source will be successful only if Oracle view exist in the RTSM.

To test the HPOM service definition source connection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Select the check box in the first column for the HPOM data source connection that you want to test, and then click **Test Connection**.
   Note: You cannot test more than one HPOM connection at a time.
   A `Test Connection Successful` message appears in the Information message panel if the connection exists.

To test the VMware Vcenter service definition source connection:

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Select the check box in the first column for the VMware vCenter data source connection that you want to test, and then click **Test Connection**.
   Note: You cannot test more than one VMware vCenter connection at a time.
   A `Test Connection Successful` message appears in the Information message panel if the connection exists.

View service definition source connection status

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Check the connection status indicator in the **Status Connection** column:

   - ✔ indicates that the host system is connected to the data source.

   - ✖ indicates that the host system is not connected to the data source.

View service definition data collection status

1. In the Administration Console, click **Topology Source > Service Definition**.
   The Service Definition page opens.

2. Check the collection status indicator in the **Status Collection** column:

Status of the collection showing the date and local time of the latest collection attempt and the current status:

- ⬆ indicates that the data collection is in progress.

- ✅ indicates that the data collection completed successfully in the previous attempt.

- ❌ indicates that the data collection failed in the previous attempt.

- ⏸ indicates that the data collection was never started.

Note: Status collection column is not displayed when VMware vCenter is the service definition source.

Configuring and managing data collection

In SHR, data collection involves collecting domain-specific data from the various product center repositories such as HP Operations Manager i (OMi), HP Business Service Management Profile database, and HP Operations agent. The collected data is stored in the SHR database, which is then used for long-term, cross-domain performance analysis and reporting.

Data collection

SHR provides an open and flexible data collection framework that can be used to collect data from heterogeneous data sources. SHR uses various data collectors to collect the required data:

- HP Operations agent collector—Collects system performance metrics for the System Management Content Pack and application metrics for domain-specific applications. The data is collected by the HP Operations agents that are installed on the host systems.

- Database collector—Collects events, messages, availability, and performance Key Performance Indicators (KPIs) from the databases of the data source such as Profile database, Management database, HPOM database, HP OMi database, and Network Performance Server (NPS). The database collector can also collect data from generic databases that use Sybase, Oracle, or SQL Server as the database system. This collector uses the database collector technology to collect the data.

These data collectors work internally within the SHR infrastructure to collect the data. Therefore, you cannot directly interface with these collectors. Instead, you can specify the data sources from where the collectors can collect the data through the Administration Console.

The Administration Console supports the configuration of these types of data source connections:

- Management and Profile databases

- HP Operations agent

- HP OMi

- HPOM

- BSM (RTSM)

- Generic databases

- VMware vCenter

The deployed Content Packs determine the fact data that are to be collected from the various data sources, and the interval at which the data is collected. Configuration of the data source connections for the installed Content Packs depends on the type of deployment scenario used. For more information about the data collection process and what Content Packs are supported for each deployment scenario, see the *HP Service Health Reporter Concepts Guide*.

You can use the Administration Console for:

- Managing the ManagementDB / ProfileDB data collection

- Managing the HP Operations agent data source data collection

- Managing the HP OMi data collection

- Managing the HPOM data collection

- Managing collection from generic databases

- "Managing the VMware vCenter data collection" on page 77

Managing the Management, Profile, and Operations Database data collection

You can configure SHR to collect data from the following HP Business Service Management data repositories:

- **Management database**: The Management database stores system-wide and management-related metadata for the HP Business Service Management environment.

- **Profile database**: The Profile database stores raw and aggregated measurement data obtained from the HP Business Service Management data collectors. The Profile database also stores measurements collected through HP OM, OMi, BPM, RUM, and Service Health.

- **Operations database**: The profile database stores data obtained from OMi10 data source.

SHR supports the configuration of and data collection from multiple Profile databases. You might have set up multiple Profile database in your HP Business Service Management environment for scaling purposes—one database might not be enough to store all the data—or for data separating—all critical data in one Profile database and all non-critical data in another. The information about the various Profile databases deployed in your environment is stored in the Management database.

For more information about the Management and Profile databases, see the *HP Business Service Management Database Guide*.

Managing the data collection

You can use the BSM/OMi page of the Administration Console to configure the data source connections. To configure the multiple Profile database connections, you only need to configure the Management database on the BSM/OMi page. After the Management database data source connection is configured, SHR discovers all the deployed Profile databases and lists them on the BSM/OMi page.

Using the BSM/OMi page, you can perform the following tasks:

- Create a new Management Database and Profile Database connection

- Modify a new Management Database and Profile Database connection

- Enable or disable Profile Database data collection

- Schedule Profile Database synchronization

- Test the Management Database and Profile Database connection

- View the Management Database and Profile Database connection status

- View the Management Database and Profile Database collection status

- Delete a Management Database connection

Create a new Management, Profile, and Operations Database connection

Create a new Management Database

1. In the Administration Console, click **Collection Configuration > BSM/OMi > Management Database**.

2. Under **Management Database**, click **Create New**.
   The Connection Parameters dialog box appears.

3. In the **Connection Parameters** dialog box, specify or type the connection parameters:

Field	Description
Host name	IP address or FQDN of the Management Database server. Not displayed when **Database in Oracle RAC** is selected.

Field	Description
Port	Port number to query the Management Database server. Not displayed when **Database in Oracle RAC** is selected.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle, MSSQL, or PostgreSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when **Database in Oracle RAC** is selected. **Note**: For information about the database host name, port number, and SID, contact your *HP Business Service Management* administrator.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
Database in Oracle RAC	This option appears only if you have selected Oracle as the database type.
Service name	Name of the service. This option appears only if **Database in Oracle RAC** is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if **Database in Oracle RAC** is selected.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. **Note**: If the Windows Authentication option is selected, this field is disabled.

4. Click **OK**.

5. Click **Test Connection** to test the connection.

6. Click **Discover Database** to automatically discover corresponding Profile database(s).

   > **Note:** If management database and profile database are on the same system, clicking **Discover Database** will automatically discover the corresponding Profile database. If the databases are on different systems, you have to manually configure the Profile database using the Profile Database tab.

   > **Note:** After you configure management database with **Database in Oracle RAC** option selected and the Test Connection is successful, clicking **Discovery Database** does not automatically discover the corresponding Profile database(s). You have to manually configure the profile database using the **Profile Database** tab.

7. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

After you save the newly created Management database connection, SHR retrieves the Profile database information from the Management database data source and lists all the available Profile database data sources under the Profile Database section.

To view details of the Profile database data source connection:

1. Under **Profile Database**, in the **Host name** column, click the icon.
   The pop-up box opens that displays details of the Profile database system.

2. View:

Field	Description
Host name	Name of the Profile database server.
Port	Port number to query the Profile database server.
Database instance	System Identifier (SID) of the Profile database instance.
DB type	The type of database engine that is used to create the Profile database. It can either be Oracle or MSSQL.
Database name	Name of the Profile database.
User name	Name of the Profile database user.

Note: Set up parameters for the profile management database, only if Profile DB on Oracle RAC is selected, or when both Management DB on Oracle RAC and Profile DB on Oracle RAC are selected. In such an instance, the Create New option under Profile Database is displayed.

Data collection for the Profile database data source is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Copy the `seed.properties` and `encryption.properties` files from the *%topaz_home%\Conf* folder on HP BSM Gateway Server to the *%PMDB_HOME%\config* folder on the HP SHR system to discover Profile Database. In case of Oracle RAC, copy the `bsm-tnsnames.ora` file to the *%PMDB_HOME%\config* folder.

If you have configured multiple management databases (both BSM and OMi topology), create multiple folders at *%PMDB_HOME%\config* (such as *%PMDB_HOME%\config\<Mgmt_DB_hostname>*) and copy the `seed.properties` and `encryption.properties` files into each folder. In case of Oracle RAC, copy the `bsm-tnsnames.ora` files to the *%PMDB_HOME%\config* folder and rename them to ensure they are unique.

The file name of the `bsm-tnsnames.ora` file must be specified when entering the database connection details for BSM in an Oracle RAC.

Create a new Profile Database

1. In the Administration Console, click **Collection Configuration > BSM/OMi > Profile Database**.

2. Under **Profile Database**, click **Create New**.
   The Connection Parameters dialog box appears.

3. In the **Connection Parameters** dialog box, specify or type the connection parameters:

Field	Description
Host name	IP address or FQDN of the Profile Database server. Not displayed when **Database in Oracle RAC** is selected.
Port	Port number to query the Profile Database server. Not displayed when **Database in Oracle RAC** is selected.
Database type	The type of database engine that is used to create the Profile Database. It can either be Oracle, MSSQL, or PostgreSQL.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.

Field	Description
Domains	Select the domains for which you want to enable data collection. **Note:** You must select the domains from which you want to enable data collection. If you have skipped topology configuration during post-install configuration and installed the content packs, you must return here to select from among the following domains to enable data collection. ■ HP Operations Manager ■ OMi ■ RUM ■ BPM ■ Service Health
Database instance	System Identifier (SID) of the Profile Database instance. Not displayed when **Database in Oracle RAC** is selected. **Note**: For information about the database host name, port number, and SID, contact your *HP Business Service Management* administrator.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
Database in Oracle RAC	This option appears only if you have selected Oracle as the database type.
Service name	Name of the service. This option appears only if **Database in Oracle RAC** is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if **Database in Oracle RAC** is selected.

Field	Description
User name	Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.

   A `Saved Successfully` message appears in the Information message panel.

Create a new Operations Database

a. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

b. Under **OMi**, click **Create New**.
   The Connection Parameters dialog box appears.

c. In the **Connection Parameters** dialog box, specify or type the connection parameters:

Field	Description
Data Source	Select your data source: Event or Operations.
Host name	IP address or FQDN of the Management Database server. Not displayed when **Database in Oracle RAC** is selected.
Port	Port number to query the Management Database server. Not displayed when **Database in Oracle RAC** is selected.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle, MSSQL, or PostgreSQL.

Field	Description
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when **Database in Oracle RAC** is selected. **Note**: For information about the database host name, port number, and SID, contact your *HP Business Service Management* administrator.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
Database in Oracle RAC	This option appears only if you have selected Oracle as the database type.
Service name	Name of the service. This option appears only if **Database in Oracle RAC** is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if **Database in Oracle RAC** is selected.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

    d.   Click **OK**.

e. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Modify a new Management, Profile, and Operations Database connection

You can only modify the Management database data source connection, not the Profile database data source connections.

To modify a Management database data source connection:

1. In the Administration Console, click **Collection Configuration > BSM/OMi > Management Database**.

2. Under **Management Database**, click **Configure**.
   The Connection Parameters dialog box appears.

3. In the **Connection Parameters** dialog box, specify or type the connection parameters:

Field	Description
Data source	Select your data source: BSM or OMi.
Host name	IP address or FQDN of the Management Database server. Not displayed when **Database in Oracle RAC** is selected.
Port	Port number to query the Management Database server. Not displayed when **Database in Oracle RAC** is selected.
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle, MSSQL, or PostgreSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when **Database in Oracle RAC** is selected. **Note**: For information about the database host name, port number, and SID, contact your *HP Business Service Management* administrator.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
Database in Oracle RAC	This option appears only if you have selected Oracle as the database type.
Service name	Name of the service. This option appears only if **Database in Oracle RAC** is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if **Database in Oracle RAC** is selected.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. **Note**: If the Windows Authentication option is selected, this field is disabled.

Field	Description
Password	Password of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. **Note**: If the Windows Authentication option is selected, this field is disabled.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Although you cannot configure the individual Profile database data source connections, you can retrieve the updated list of Profile database connections from the Management database. You can use the **Refresh** button to synchronize the databases and get the updated list of Profile database changes. Changes can include:

- New Profile database discovered from Management database.

- Existing Profile database deleted from Management database.

- Changes in configuration data for existing database.

To update the list of Profile database connections:

1. In the Administration Console, click **Collection Configuration > BSM/OMi**.
   The ManagementDB / ProfileDB page opens.

2. Under **Profile Database**, click **Refresh**.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

To update the list of Operations database connections:

1. In the Administration Console, click **Collection Configuration > BSM/OMi**.
   The ManagementDB / ProfileDB page opens.

2. Under **OMi**, click **Refresh**.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Enable or disable Profile Database data collection

1. In the Administration Console, click **Collection Configuration > BSM/OMi**.

2. For one or more hosts, under **Profile Database**, perform any one of the following steps:
   - Select the **Enable Collection** check box to enable data collection.

   - Clear the **Enable Collection** check box to disable data collection.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Schedule Profile Database synchronization

1. In the Administration Console, click **Collection Configuration > BSM/OMi**.

2. Under **Profile Database**, specify a synchronization time between 1 and 24 hours in the **Select Schedule** box and then click **Apply**.
   A `Please click on Save button to save the changes` message appears below the table.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Test the Management Database and Profile Database connection

To test the Management database data source connection:

1. In the Administration Console, click **Collection Configuration > BSM/OMi > Management Database**.

2. Click **Test Connection**.
   A `Test Connection Successful` message appears in the Information message panel if connection exists.

To test the Profile database data source connections:

1. In the Administration Console, click **Collection Configuration > BSM/OMi > Profile Database**.

2. Click **Test** in the **Test Connection** column for a specific Profile database data source connection.
   A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the Management Database and Profile Database connection status

To view the connection status of a Management database data source:

1. In the Administration Console, click **Collection Configuration > > BSM/OMi**.

2. Under **Management Database**, check the connection status indicator in the **Status Connection** column:

   - ⊘ indicates that the host system is connected to the data source.

   - ⊗ indicates that the host system is not connected to the data source.

To view the connection status of a Profile database data source:

1. In the Administration Console, click **Collection Configuration > BSM/OMi**.

2. Under **Profile Database**, for one or more Profile databases, check the connection status indicator in the **Status Connection** column:

   - ⊘ indicates that the host system is connected to the data source.

   - ⊗ indicates that the host system is not connected to the data source.

View the Management Database and Profile Database collection status

To view the collection status of a Management database data source:

1. In the Administration Console, click **Collection Configuration > BSM/OMi**.

2. Under **Management Database**, check the collection status indicator in the **Status Collection** column:

   Status of the collection showing the date and time of the latest collection attempt and the current status:

   - ⬆ indicates that the data collection is in progress.

   - ⊘ indicates that the data collection completed successfully in the previous attempt.

   - ⊗ indicates that the data collection failed in the previous attempt.

   - ⏸ indicates that the data collection was never started.

To view the collection status of Profile database data sources:

1. In the Administration Console, click **Collection Configuration > BSM/OMi**.

2. Under **Profile Database**, for one or more Profile databases, check the collection status indicator in the **Status Collection** column:

Status of the collection showing the date and time of the latest collection attempt and the current status:

- 🔼 indicates that the data collection is in progress.

- ✅ indicates that the data collection completed successfully in the previous attempt.

- ❌ indicates that the data collection failed in the previous attempt.

- ⏸ indicates that the data collection was never started.

Delete a Management Database connection

1. In the Administration Console, click **Collection Configuration > BSM/OMi**.

2. Under **Management Database**, click **Delete**.

3. In the message box, click **Yes**.
   A `Deleted Successfully` message appears in the Information message panel.

4. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Although you cannot delete individual Profile database data source connections, deleting the Management database data source connection automatically removes all the Profile database data source connections. However, deleting a Management database connection does not delete the collected data from the SHR database.

Managing the HP Operations Agent data source data collection

SHR reports on various facts collected from the HP Operations Agent managed nodes. The HP Operations Agent collects, summarizes, timestamp[1], and detects alarm conditions on current and historical resource data across your system. These agents provide performance, resource, and end-to-end transaction response time measurements, and support network and database measurement information.

HP Operations Agent data sources

SHR integrates with HP Operation Agent to collect historical system and application-performance data. Depending on the deployment scenario, RTSM or HPOM discovers the hosts on which the agent is installed and running. SHR uses an HP Operation Agent data collector to collect the fact data from the hosts. The list of metrics to be collected from each HP Operation Agent host is identified by the Content Packs.

For more information about HP Operation Agent, see the HP Operation Agent documentation.

[1]The process of recording timestamps that is the time at which an event occurred in the system. Timestamps are typically used for logging events.

Managing the data collection

You can use the HP Operations agent configuration page of the Administration Console to manage the HP Operations Agent data collection. You do not need to create new agent data source connections because, by default, SHR discovers all the nodes on which HP Operations agents are installed during the topology data collection phase. These discovered agent data sources or nodes are listed in the HP Operations agent Data Source page.

Using the HP Operations agent Data Source page, you can perform the following tasks:

- View the HP Operations agent data source details

- Enable or disable an HP Operations agent data source data collection

- Schedule an HP Operations agent data source synchronization

- Test the HP Operations agent data source connection

View the HP Operations Agent data source details

1. In the Administration Console, click **Collection Configuration > HP Operations agent**. The HP Operations agent page opens.

2. In the HP Operations Agent Data Source Summary table, view:

Field	Description
Domain name	A list of topology views that contain the specific CI attributes that the HP Operations agent collector uses to collect the relevant data. *All* indicates all the views. *Unassigned* indicates the HP Operations agent data sources that do not have any topology views assigned to it.
Hosts	The number of HP Operations agent data sources for that particular view.
Collection: Passed	The number of distinct HP Operations agent data sources from where the raw data was successfully collected.
Collection: Failed	The number of distinct HP Operations agent data sources from where data collection failed.
Collection: Never Collected	The number of distinct HP Operations agent data sources from where data was never collected.

Field	Description
Enabled/Disabled	The number of distinct HP Operations agent data sources that are enabled or disabled for data collection.

3. To view detailed information about the HP Operations agent data sources, click the view name or the number in the HP Operations Agent Data Source Summary table. You can:

   ▪ Click the view name to view the list of HP Operations agent data sources for that particular view.

   ▪ Click the number in the Hosts column to list details of all the HP Operations agent data sources.

   ▪ Click the number in the Passed column to view the details of the HP Operations agent data sources from where data collection was successful.

   ▪ Click the number in the Failed column to view the details of the HP Operations agent data sources from where data collection failed.

   ▪ Click the number in the Never Collection column to view the details of the HP Operations agent data sources from where data was never collected.

   ▪ Click the number in the Enabled/Disabled column to view the details of the HP Operations agent data sources were enabled or disabled for data collection.

   The HP Operations Agent Data Source Details *<view name>* table appears.

4. View:

Field	Description
Search: Host name	Search option that support pattern matching search. You can use this feature to search for a particular HP Operations agent data source or filter this displayed list of hosts.
Host name	Name of the HP Operations agent data source.
Enable Collection	Enable or disable data collection from the HP Operations agent data source. **Note**: Use the enable or disable option in the header to enable or disable data collection from all the HP Operations agent Data Sources in the list.
Schedule Polling Frequency	Time (in hours) to synchronize the SHR database with the HP Operations agent data source.

Field	Description
Remote Collector	List of remote collectors enabled for data collection configured in SHR.
Rule Type	List of rules you can apply on the remote collector.
Connection Status	Status of the HP Operations agent data source connection. ■ ✅ indicates that the host system is connected to the data source. ■ ❌ indicates that the host system is not connected to the data source.
Collection Status	Status of the data collection showing the date and local time of the latest collection attempt and the current status. ■ ✅ indicates that the data collection completed successfully. ■ ❌ indicates that the data collection failed. ■ ⏸ indicates that the data collection was never started.

Enable or disable a HP Operations agent data source data collection

1. In the Administration Console, click **Collection Configuration > HP Operations Agent**.
   The HP Operations agent Data Source page opens.

2. In the HP Operations Agent Data Source Summary table, click the view name or the number in the column to list the HP Operations agent data sources for which you want to enable or disable data collection. The HP Operations Agent Data Source Details table opens.

3. Type the host name in the **Host name** box and click **Search**, if you want to filter the list of HP Operations agent data sources.

4. You can enable or disable a HP Operations agent data source data collection in the following ways:
   - For one or more hosts, select the check box in the **Enable Collection** column.

   - To enable data collection for all the displayed HP Operations agent data sources, select the

check box in the **Enable Collection** header.

- To disable data collection, clear the **Enable Collection** check box.

5. Click **Save**.
A `Saved Successfully` message appears in the Information message panel.

Note: The collection for the HP Operations agent data source connections are enabled by default.

Schedule a HP Operations Agent data source data synchronization

By default, the data collection from the various HP Operations agent data sources is scheduled for every one hour. However, you can modify this according to your requirements.

To schedule a HP Operations agent data source polling frequency:

1. In the Administration Console, click **Collection Configuration > HP Operations agent**.
The HP Operations agent Data Source page opens.

2. In the HP Operations Agent Data Source Summary table, click the view name or the number in the column to list the HP Operations agent data sources for which you want to enable or disable data collection. The HP Operations Agent Data Source Details table opens.

3. For one or more hosts, specify a polling time between 1 and 24 hours in the **Hrs** box in the **Schedule polling frequency** column.
Note: Type the host name in the **Host name** box and click **Search**, if you want to filter the list of HP Operations agent data sources.

4. Click **Save**.
A `Saved Successfully` message appears in the Information message panel.

5. If you want to apply the collection schedule to all the lists hosts, click **Update All**.
The Apply schedule to group section appears.

Note: The Update All option does not appear for the **All** or **Unassigned** options in the View name column.

6. Specify a polling time between 1 and 24 hours in the **Hrs** box and then click **OK**.

7. Click **Save**.
A `Saved Successfully` message appears in the Information message panel.

Blacklisting of Nodes

Data collection from a host will not occur when the connection to the HP Operations agent is lost. If the node is unreachable for three consecutive data collection runs, the node is noted in the blacklisted category. Once a node is blacklisted, the interval of the data collection run is doubled with every three retries until the data collection interval reaches 24 hours. If the connection to the node is resumed, it is no longer considered a blacklisted node and the data collection interval resumes to the original value.

You can view the blacklisted hosts from the **Java Monitoring & Management Console**. Access this console from an SHR system through *<BO install dir>\javasdk\bin\jconsole.exe* and login with the <host name>;<port> credentials, where the port is 21409 for SHR.

To disable the blacklisting of nodes:

1. Browse to the following location:

   For Windows: %PMDB_HOME%\config\collection.properties

   For Linux: $PMDB_HOME/config/collection.properties

2. Open the .properties file in the edit mode and locate the property pa.collector.blacklist.mode parameter

3. Set the value to FALSE. The default value is TRUE.

Test the HP Operations agent data source connection

1. In the Administration Console, click **Collection Configuration > HP Operations agent**. The HP Operations Agent Data Source page opens.

2. In the HP Operations Agent Data Source Summary table, click the view name or the number in the column to list the HP Operations agent data sources for which you want to enable or disable data collection. The HP Operations Agent Data Source Details table opens.

3. Select the check box in the first column for a specific HP Operations agent data source connection.
   Note: Type the host name in the **Host name** box and click **Search**, if you want to filter the list of HP Operations agent data sources. You cannot test more than one HP Operations agent data source connection at a time.

4. Click **Test Connection**.
   A Test Connection Successful message appears in the Information message panel if the connection exists.

Assign View/Node Group based Rules for Data Collection

You can collect data from the HP Operations agent data source by grouping the views or nodes together.

1. In the Administration Console, click **Collection Configuration > HP Operations agent**.

2. Click the **Assignment** tab.

3. Select a **Collection Station** based on your environment.

4. For **Rule Type**, select **Pattern Based**.

5. In the **Rule** field, select as many rules as applicable and use the arrow to move it to the adjoining box.

6. Click **Save**.

Assign Pattern based Rules for Data Collection

You can collect data from the HP Operations agent data source by grouping the nodes together.

1. In the Administration Console, click **Collection Configuration > HP Operations agent**.

2. Click the **Assignment** tab.

3. Select a **Collection Station** based on your environment.

4. For **Rule Type**, select **View/Node Group Based**.

5. In the **Rule** field, enter a pattern for host names based on your choice and click the ✓ icon to add the rule.

6. Select as many rules as applicable and use the arrow to move it to the adjoining box.

7. Click **Save**.

Managing the HP OMi data collection

HP OMi combines business-service management and infrastructure management so that you can monitor and manage a wide variety of problems that occur in your IT environment from different but complimentary perspectives at the same time. HP OMi generates Health Indicators (HIs) for the CI types in your environment, which provide a detailed status of a CI type. These HIs are mapped with the events that are generated by other domain manager products in your environment such as Network Node Manager (NNM), HP SiteScope, and HPOM. The HIs are used to calculate the KPIs of a CI type, which displays the aggregated state of a CI type. The KPIs represent the high-level health of the CI types to the operator and shows the health and event summary of your business.

HP OMi data

SHR collects the historical HI and KPI values against RTSM instances from the HP Business Service Management Profile database over a period of time and displays the trend of these values through reports and dashboards. SHR uses the database collector to collect the historical HI and KPI values from the Profile database. The KPI names, HI dimension details, and value details are collected from the HP BSM Management database.

For more information about HP OMi, see the HP OMi documentation.

Prerequisite for Management Packs

To view reports for the following SHR content packs that gather data from the OMi10 data source, the corresponding Management Packs must be installed:

- Microsoft Active Directory

- Microsoft Exchange

- Microsoft SQL Server

- Oracle

- Oracle WebLogic

- IBM WebSphere

Installing these management packs is also mandatory to view SHR reports for Service Health and OMi.

Managing the data collection

Using BSM/OMi page from the SHR Administration Console, you can perform the following tasks:

- Create an HP OMi data source connection

- Modify an HP OMi data source connection

- Enable or disable an HP OMi data collection

- Schedule an HP OMi data collection

- Test the HP OMi data source connection

- View the HP OMi data source connection status

- View the HP OMi data collection status

- Delete an HP OMi data source connection

Create an HP OMi data source connection

Before you create a new HP OMi data source connection, make sure that a data source connection for the HP BSM Management database exists on the BSM/OMi page. This data connection is a prerequisite for the HP OMi connection because SHR collects the KPI metadata for HP OMi from the Management Database.

If you have one or more OMi setups in your environment, you must configure the OMi data source that belongs to the HP Business Service Management RTSM that was configured as the topology source.

To create a new HP OMi data source connection:

1. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

2. Click **Create New**.
   The Connection Parameters dialog box opens.

3. In the **Connection Parameters** dialog box, select the **Data Source** and type the following values:

Field	Description
Host name	IP address or FQDN of the HP OMi database server.
Port	Port number to query the HP OMi database server.
Database Instance	System Identifier (SID) of the HP OMi database instance. **Note**: For information about the database hostname, port number, and SID, contact your HP OMi database administrator.
Database type	The type of database engine that is used to create the HP OMi database. It can either be Oracle, MSSQL, or PostgreSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
User name	Name of the HP OMi database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the HP OMi database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Note: You can only create a single HP OMi data source connection. The Create New button is disabled after you create a new HP OMi data source connection or if a connection already exists.

Data collection for the newly created HP OMi data source connection is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Modify an HP OMi data source connection

1. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

2. For a specific host, click **Configure**.
   The Connection Parameters dialog box appears.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Data Source	Select the data source: Event or Operations.
Host name	IP address or FQDN of the HP OMi database server.
Port	Port number to query the HP OMi database server.
Database Instance	System Identifier (SID) of the HP OMi database instance. **Note**: For information about the database hostname, port number, and SID, contact your HP OMi database administrator.
Database type	The type of database engine that is used to create the HP OMi database. It can either be Oracle, MSSQL, or PostgreSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
OMi on Oracle RAC	Option to enable OMi database on Oracle RAC.
Service Name	Specify the name by which SHR connects to the Oracle instance. This option appears only if OMi on Oracle RAC is selected.
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the SHR system. This option appears only if OMi on Oracle RAC is selected.
User name	Name of the HP OMi database user. **Note**: If the Windows Authentication option is selected, this field is disabled.

Field	Description
Password	Password of the HP OMi database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Enable or disable an HP OMi data collection

1. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

2. Perform any one of the following steps:
   - Select the check box in the **Enable Collection** column to enable data collection.

   - Clear the check box in the **Enable Collection** column to disable data collection.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Schedule an HP OMi data collection

1. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

2. Specify a collection time between 1 and 24 hours in the **Hrs** box in the **Schedule Frequency** column.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Test the HP OMi data source connection

1. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

2. Click **Test Connection**.
   A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the HP OMi data source connection status

1. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

2. Check the connection status indicator in the **Status Connection** column:

   - ⊘ indicates that the host system is connected to the data source.

   - ⊗ indicates that the host system is not connected to the data source.

View the HP OMi data collection status

1. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

2. Check the collection status indicator in the **Status Collection** column:

   Status of the collection showing the date and time of the latest collection attempt and the current status:

   - ⊙ indicates that the data collection is in progress.

   - ⊘ indicates that the data collection completed successfully in the previous attempt.

   - ⊗ indicates that the data collection failed in the previous attempt.

   - ⊙ indicates that the data collection was never started.

Delete an HP OMi data source connection

1. In the Administration Console, click **Collection Configuration > BSM/OMi > OMi**.

2. Click **Delete**.
   A `Deleted Successfully` message appears in the Information message panel.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Managing the HPOM data collection

HPOM is a distributed server-client software solution that provides service-driven event and performance management of business-critical enterprise systems, applications, and services. HPOM centrally monitors performance and events by using agents that are installed on the managed nodes. An agent is a deployment package that helps you manage nodes by collecting data, discovering services, monitoring events, and running actions and commands that control the nodes.

SHR collects event statistics, severity statistics for each of those events, as well as operator statistics, such as how many events were handled by each operator, from the HPOM database.

Managing the data collection

Using the Operations Manager page, you can perform the following tasks:

- Create an HPOM data source connection

- Modify an HPOM data source connection

- Enable or disable an HPOM data collection

- Schedule an HPOM data collection

- Test the HPOM data source connection

- View the HPOM data source connection status

- View the HPOM data collection status

- Delete an HPOM data source connection

Create an HPOM data source connection

Note: When you create a data source connection for HPOM on the Service Definition page, the same data source connection appears on the Operation Manager page as well. However, updating the data source connection on the Service Definition page does not update the connection details on the Operation Manager page.

1. In the Administration Console, click **Collection Configuration > HP Operations Manager**. The Operations Manager page opens.

2. Click **Create New**.
   The Connection Parameters dialog box opens.
   Note: If you are using the database method of authentication to connect to the HPOM database server, you must provide the user details that have the select and connect permissions for the "openview" database here.

3.

Field	Description
OM on Oracle RAC	Option to enable HPOM database on Oracle RAC.
Service Name	Specify the name by which SHR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.

Field	Description
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the SHR system. This option appears only if OM on Oracle RAC is selected.
Host name	IP address or FQDN of the HPOM database server.
Port	Port number to query the HPOM database server. The default port is 1433 if SQL Server is the database type and 1521 if Oracle is the database type.
Database Instance	Specify the instance name of the HPOM database. The default database instance for HPOM for Windows is OVOPS; the default database instance for HPOM on UNIX/Linux is openview. For information about the database host name, port number, and instance name, contact your HPOM database administrator.
Database type	The type of database engine that is used to create the HPOM database. Select MSSQL if you want to create a connection for HPOM for Windows; select Oracle to create a connection for HPOM on UNIX/Linux.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
User name	Name of the HPOM database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the HPOM database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	The name of the system where the collector is installed.

4. Click **OK**.

5. Click **Save**.
   A Saved Successfully message appears in the Information message panel.

Data collection for the newly created HPOM data source is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Modify an HPOM data source connection

1. In the Administration Console, click **Collection Configuration > HP Operations Manager**. The Operations Manager page opens.

2. Click **Configure**.
   The Connection Parameters dialog box opens.
   Note: If you are using the database method of authentication to connect to the HPOM database server, you must provide the user details that have the select and connect permissions for the "openview" database here.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
OM on Oracle RAC	Option to enable HPOM database on Oracle RAC.
Service Name	Specify the name by which SHR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the SHR system. This option appears only if OM on Oracle RAC is selected.
Host name	Address (IP or name) of the HPOM database server.
Port	Port number to query the HPOM database server. The default port is 1433 if SQL Server is the database type and 1521 if Oracle is the database type.
Database Instance	System Identifier (SID) of the HPOM database instance. The default database instance is OVOPS. **Note**: For information about the database host name, port number, and SID, contact your HPOM database administrator.
Database type	The type of database engine that is used to create the HPOM database. It can either be Oracle or MSSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
User name	Name of the HPOM database user. **Note**: If the Windows Authentication option is selected, this field is disabled.

Field	Description
Password	Password of the HPOM database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	The name of the system where the collector is installed.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Enable or disable an HPOM data collection

1. In the Administration Console, click **Collection Configuration > HP Operations Manager**. The Operations Manager page opens.

2. For one or more hosts, perform any one of the following steps:
   - Select the check box in the **Enable Collection** column to enable data collection.

   - Clear the check box in the **Enable Collection** column to disable data collection.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Schedule an HPOM data collection

1. In the Administration Console, click **Collection Configuration > HP Operations Manager**. The Operations Manager page opens.

2. For one or more hosts, specify a collection time between 1 and 24 hours in the **Hrs** box in the **Schedule Frequency** column.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Test the HPOM data source connection

1. In the Administration Console, click **Collection Configuration > HP Operations Manager**. The Operations Manager page opens.

2. Select the check box in the first column for a specific HPOM connection.
   Note: You cannot test more than one HPOM connection at a time.

3. Click **Test Connection**.
   A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the HPOM data source connection status

1. In the Administration Console, click **Collection Configuration > HP Operations Manager**. The Operations Manager page opens.

2. For one or more hosts, check the connection status indicator in the **Status Connection** column:

   - indicates that the host system is connected to the data source.

   - indicates that the host system is not connected to the data source.

View the HPOM data collection status

1. In the Administration Console, click **Collection Configuration > HP Operations Manager**. The Operations Manager page opens.

2. For one or more hosts, check the connection status indicator in the **Status Collection** column:

   Status of the collection showing the date and time of the latest collection attempt and the current status:

   - indicates that the data collection is in progress.

   - indicates that the data collection completed successfully in the previous attempt.

   - indicates that the data collection failed in the previous attempt.

   - indicates that the data collection was never started.

Delete an HPOM data source connection

1. In the Administration Console, click **Collection Configuration > HP Operations Manager**. The Operations Manager page opens.

2. Select the check boxes in the first column to delete one or more HPOM data source connections.

3. Click **Delete**.
   A `Deleted Successfully` message appears in the Information message panel.

4. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Managing collection from generic databases

SHR enables you to configure data collection from any generic database source. Using the Generic Database page, you can configure SHR to connect to and collect data from any generic data source that use Sybase, Oracle, or Microsoft SQL Server as the database system.

This page is typically used to configure and collect network-related data from the Network Performance Server (NPS) for the Network reports in SHR. The Network Performance Server (NPS) provides the infrastructure that is used in conjunction with Network Node Manager i Software (NNMi) to monitor the operational performance of the network infrastructure. With the performance data collected by different NNMi Software Smart Plug-ins (iSPIs), the NPS builds data tables, runs queries in response to user selections, and displays query results in web-based reports that help you diagnose and troubleshoot problems in your network environment. The NPS enables you to effectively store, access, and track performance data.

Out-of-the-box, SHR supports configuration to generic data sources that use the above-mentioned database types. However, using this page, you can configure SHR to connect to and collect data from other generic database types as well such as MySQL, PostgreSQL, Sybase, and so on. For a particular database type, you can specify the domain for which you want SHR to collect data such as system data, network data, and so on. For more information on how to configure such data sources, contact HP Support.

Managing the data collection

Using the Generic Database page, you can perform the following tasks:

- Create a generic database connection

- Modify a generic database connection

- Enable or disable a generic database data collection

- Schedule a generic database data collection

- Test the generic database connection

- View the generic database connection status

- View the generic database collection status

- Delete a generic database connection

Create a generic database connection

1. In the Administration Console, click **Collection Configuration > Generic Database**.
   The Generic Database page opens.

2. Click **Create New**.
   The Connection Parameters dialog box opens.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the generic database server.
Port	Port number to query the database server.
Timezone	The time zone in which the data is stored into the source database.
Database type	The type of database engine that is used to create the database. It can be Sybase IQ, Sybase ASE, Oracle, or MSSQL.
Domain	Select the domain(s) for which you want SHR to collect data from the selected database type.

URL	The URL of the database instance. The syntax for the URL for each of the database types is:
	
	■ **Oracle**:
	`jdbc:bto:oracle://<server>:<port>;SID=<sid>`
	
	In an Oracle Real Application Cluster (RAC), copy the TNS ORA file to the SHR system and provide the absolute path in the following URL syntax:
	
	`jdbc:bto:oracle:TNSNamesFile=<absolute path of TNS ORA file>;TNSServerName=<Service name>`
	
	■ **MSSQL**: `jdbc:jtds:sqlserver://<server><port>/<database>;instance=<dbInstance>`
	
	■ **Sybase IQ**:
	`jdbc:sybase:Tds:<server>:<port>/<database>`
	
	■ **Sybase ASE**:
	`jdbc:sybase:Tds:<server>:<port>?ServiceName=<dbInstance>`
	
	■ **PostgreSQL**:
	`jdbc:postgresql://<server>:<port>/<database>`
	
	where *<server>*, *<port>*, *<sid>*, *<database>*, and *<dbInstance>* are replaceable variables that you must enter.

User name	Name of the generic database user.

Field	Description
Password	Password of the generic database user.
Collection Station	The name of the system where the collector is installed.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Data collection for the newly created data source is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Modify a generic database connection

1. In the Administration Console, click **Collection Configuration > Generic Database**.
   The Generic Database page opens.

2. Click **Configure**.
   The Connection Parameters dialog box opens.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	Address (IP or name) of the generic database server.
Port	Port number to query the database server.
TimeZone	The time zone under which the database instance is configured.
Database type	The type of database engine that is used to create the generic database. It can be Sybase IQ, Sybase ASE, Oracle, or MSSQL.
Domain	Select the domain(s) for which you want SHR to collect data from the selected database type.

Field	Description

URL	The URL of the database instance. The syntax for the URL for each of the database types is:
	
	■ **Oracle**:
	`jdbc:bto:oracle://<server>:<port>;SID=<sid>`
	
	In an Oracle Real Application Cluster (RAC), copy the TNS ORA file to the SHR system and provide the absolute path in the following URL syntax:
	
	`jdbc:bto:oracle:TNSNamesFile=<absolute path of TNS ORA file>;TNSServerName=<Service name>`
	
	■ **MSSQL**: `jdbc:jtds:sqlserver://<server> <port>/<database>;instance=<dbInstance>`
	
	■ **Sybase IQ**:
	`jdbc:sybase:Tds:<server>:<port>/<database>`
	
	■ **Sybase ASE**:
	`jdbc:sybase:Tds:< server>:<port>?ServiceName=<dbInstance>`
	
	■ **PostgreSQL**:
	`jdbc:postgresql://<server>:<port>/<database>`
	
	where *<server>*, *<port>*, *<sid>*, *<database>*, and *<dbInstance>* are replaceable variables that you must enter.

User name	Name of the generic database user.
Password	Password of the generic database user.
Collection Station	The name of the system where the collector is installed.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Enable or disable a generic database data collection

1. In the Administration Console, click **Collection Configuration > Generic Database**.
   The Generic Database page opens.

2. For one or more hosts, perform any one of the following steps:
   ■ Select the check box in the **Enable Collection** column to enable data collection.

- Clear the check box in the **Enable Collection** column to disable data collection.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Schedule a generic database data collection

1. In the Administration Console, click **Collection Configuration > Generic Database**.
   The Generic Database page opens.

2. For one or more hosts, specify a collection time between 1 and 24 hours in the **Hrs** box in the **Schedule Frequency** column.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Test the generic database connection

1. In the Administration Console, click **Collection Configuration > Generic Database**.
   The Generic Database page opens.

2. Select the check box in the first column for a specific database connection.
   Note: You cannot test more than one connection at a time.

3. Click **Test Connection**.
   A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the generic database connection status

1. In the Administration Console, click **Collection Configuration > Generic Database**.
   The Generic Database page opens.

2. For one or more hosts, check the connection status indicator in the **Status Connection** column:

   - indicates that the host system is connected to the data source.

   - indicates that the host system is not connected to the data source.

View the generic database collection status

1. In the Administration Console, click **Collection Configuration > Generic Database**.
   The Generic Database page opens.

2. For one or more hosts, check the connection status indicator in the **Status Collection** column:

Status of the collection showing the date and time of the latest collection attempt and the current status:

- ⬆ indicates that the data collection is in progress.

- ✅ indicates that the data collection completed successfully in the previous attempt.

- ❌ indicates that the data collection failed in the previous attempt.

- ⏸ indicates that the data collection was never started.

Delete a generic database connection

1. In the Administration Console, click **Collection Configuration > Generic Database**. The Generic Database page opens.

2. Select the check boxes in the first column to delete one or more database connections.

3. Click **Delete**.
   A `Deleted Successfully` message appears in the Information message panel.

4. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Managing the VMware vCenter data collection

VMware vCenter is a distributed server-client software solution that provides a central and a flexible platform for managing the virtual infrastructure in business-critical enterprise systems. VMware vCenter centrally monitors performance and events, and provides an enhanced level of visibility of the virtual environment, thus helping IT administrators to control the environment with ease.

SHR collects event statistics, severity statistics for each of those events, as well as operator statistics, such as how many events were handled by each operator, from the VMware vCenter database.

Managing the data collection

Using the VMware VCenter page, you can perform the following tasks:

- "Create VMware vCenter data source connection" on the next page

- "Modify a VMware vCenter data source connection" on the next page

- "Enable or disable a VMware vCenter data collection" on page 79

- "Schedule a VMware vCenter data collection" on page 79

- "Test the VMware vCenter data source connection" on the next page

- "View the VMware vCenter data source connection status" on page 80

Create VMware vCenter data source connection

Note: When you create a data source connection for VMware vCenter on the Service Definition page, the same data source connection appears on the VMware vCenter data collection page as well. You can create additional data sources from the VMware vCenter collection configuration page.

1. In the Administration Console, click **Collection Configuration > VMware vCenter**.
   The VMware vCenter page opens.

2. Click **Create New**.
   The Connection Parameters dialog box opens.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the VMware vCenter database server.
User name	Name of the VMware vCenter database user.
Password	Password of the VMware vCenter database user.
Collection Station	The name of the system where the collector is installed.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Data collection for the newly created VMware vCenter data source is enabled by default. In addition, the collection frequency is scheduled for every one hour.

Modify a VMware vCenter data source connection

1. In the Administration Console, click **Collection Configuration > VMware vCenter**.
   The VMware vCenter Data Source page opens.

2. Click **Configure**.
   The Connection Parameters dialog box opens.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the VMware vCenter database server.
User name	Name of the VMware vCenter database user.
Password	Password of the VMware vCenter database user.
Collection Station	The name of the system where the collector is installed.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Enable or disable a VMware vCenter data collection

1. In the Administration Console, click **Collection Configuration > VMware vCenter**.
   The VMware vCenter Data Source page opens.

2. For one or more hosts, perform any one of the following steps:
   - Select the check box in the **Enable Collection** column to enable data collection.

   - Clear the check box in the **Enable Collection** column to disable data collection.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Schedule a VMware vCenter data collection

1. In the Administration Console, click **Collection Configuration > VMware vCenter**.
   The VMware vCenter Data Source page opens.

2. For one or more hosts, specify a collection time between 5 and 60 minutes in the **Mins** box in the **Schedule Frequency** column.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Test the VMware vCenter data source connection

1. In the Administration Console, click **Collection Configuration > VMware vCenter**.
   The VMware vCenter page opens.

2. Select the check box in the first column for a specific VMware vCenter connection.
   Note: You cannot test more than one VMware vCenter connection at a time.

3. Click **Test Connection**.
    A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the VMware vCenter data source connection status

1. In the Administration Console, click **Collection Configuration > VMware vCenter**.
    The VMware vCenter Data Source page opens.

2. For one or more hosts, check the connection status indicator in the **Status Connection** column:

    - indicates that the host system is connected to the data source.

    - indicates that the host system is not connected to the data source.

Managing the SiteScope data collection

You can use the SiteScope page to configure a SiteScope data source, which collects data from several SiteScope monitors in your environment. Using this page, you can enable or disable data collection and add or delete the SiteScope application programming interface (API) collector according to your requirement.

Managing the data collection

Using the SiteScope page, you can perform the following tasks:

-   Create a SiteScope data source connection

-   Modify a SiteScope data source connection

-   Enable or disable SiteScope data collection

-   Test the SiteScope data source connection

-   View the SiteScope data source connection status

-   View the SiteScope data collection status

-   Delete a SiteScope data source connection

Create a SiteScope data source connection

To create a new SiteScope data source connection:

1. In the Administration Console, click **Collection Configuration > SiteScope**.
    The SiteScope page opens.

2. Click **Create New**.
   The Connection Parameters dialog box opens.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Connection Settings	
Host name	IP address or FQDN of the SiteScope server.
Port	Port number to query the SiteScope server.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
User name	Name of the SiteScope user.
Password	Password of the SiteScope user.
Init String	Shared key used to establish a connection to SiteScope server.
Collection Station	This option is used for a collector installed on a remote system.
General Data Integration Settings: These settings create a generic data integration between the SiteScope server and the SHR server. After the connection is successful, SiteScope servers push data to the SHR server. Also, you must create a tag in SHR that you must manually apply to the SiteScope monitors that you want to report on. For more information on applying the tag, see documentation for SiteScope.	
Integration name	Enter the name of the integration. **Note**: You cannot change it later.
Encoding	The encoding type for communication between SHR and SiteScope.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
Reporting interval (seconds)	User configurable; frequency at which SiteScope pushes data to SHR.
Request timeout (seconds)	User configurable; the time to wait before the connection times out. Value of zero (0) gives you infinite timeout period.
Connection timeout (seconds)	User configurable; timeout until connection is reestablished. Value of zero (0) means timeout is not used.

Field	Description
Number of retries	Number of retries that SiteScope server attempts during connection error with SHR.
Authentication when requested	Optional; if selected, authentication is performed using the Web server user name and password.
Authentication user name	If SHR is configured to use basic authentication, specify the user name to access the server.
Authentication password	If SHR is configured to use basic authentication, specify the password to access the server.
Proxy address	If proxy is enabled on SiteScope, enter the proxy address.
Proxy user name	Enter user name of the proxy server.
Proxy password	Enter password of the proxy server.
Create tag	Select it to create a tag for the SiteScope monitors that you must manually apply from the SiteScope server.
Tag name	User defined name of the tag.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Data collection for the newly created SiteScope data source connection is enabled by default. In addition, the collection frequency is scheduled for every 15 minutes.

Modify a SiteScope data source connection

1. In the Administration Console, click **Collection Configuration > SiteScope**.
   The SiteScope page opens.

2. For a specific host, click **Configure**.
   The Connection Parameters dialog box appears.

3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Connection Settings	

Field	Description
Host name	IP address or FQDN of the SiteScope server.
Port	Port number to query the SiteScope server.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
User name	Name of the SiteScope user.
Password	Password of the SiteScope user.
Init String	Shared key used to establish a connection to SiteScope server.
Collection Station	This option is used for a collector installed on a remote system.
General Data Integration Settings: These settings create a generic data integration between the SiteScope server and the SHR server. After the connection is successful, SiteScope servers push data to the SHR server. Also, you must create a tag in SHR that you must manually apply to the SiteScope monitors that you want to report on. For more information on applying the tag, see documentation for SiteScope.	
Integration name	Enter the name of the integration. **Note**: You cannot change it later.
Encoding	The encoding type for communication between SHR and SiteScope.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
Reporting interval (seconds)	User configurable; frequency at which SiteScope pushes data to SHR.
Request timeout (seconds)	User configurable; the time to wait before the connection times out. Value of zero (0) gives you infinite timeout period.
Connection timeout (seconds)	User configurable; timeout until connection is reestablished. Value of zero (0) means timeout is not used.
Number of retries	Number of retries that SiteScope server attempts during connection error with SHR.
Authentication when requested	Optional; if selected, authentication is performed using the Web server user name and password.

Field	Description
Authentication user name	If SHR is configured to use basic authentication, specify the user name to access the server.
Authentication password	If SHR is configured to use basic authentication, specify the password to access the server.
Proxy address	If proxy is enabled on SiteScope, enter the proxy address.
Proxy user name	Enter user name of the proxy server.
Proxy password	Enter password of the proxy server.
Create tag	Select it to create a tag for the SiteScope monitors that you must manually apply from the SiteScope server.
Tag name	User defined name of the tag.

4. Click **OK**.

5. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Enable or disable SiteScope data collection

1. In the Administration Console, click **Collection Configuration > SiteScope**.
   The SiteScope page opens.

2. Perform any one of the following steps:
   - Select the check box in the **Enable Collection** column to enable data collection.

   - Clear the check box in the **Enable Collection** column to disable data collection.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Test the SiteScope data source connection

1. In the Administration Console, click **Collection Configuration > SiteScope**.
   The SiteScope page opens.

2. Click **Test Connection**.
   A `Test Connection Successful` message appears in the Information message panel if connection exists.

View the SiteScope data source connection status

1. In the Administration Console, click **Collection Configuration > SiteScope**.
   The SiteScope page opens.

2. Check the connection status indicator in the **Status Connection** column:

   - ✓ indicates that the host system is connected to the data source.

   - ✗ indicates that the host system is not connected to the data source.

View the SiteScope data collection status

1. In the Administration Console, click **Collection Configuration > SiteScope**.
   The SiteScope page opens.

2. Check the collection status indicator in the **Status Collection** column:

   Status of the collection showing the date and time of the latest collection attempt and the current status:

   - ⬆ indicates that the data collection is in progress.

   - ✓ indicates that the data collection completed successfully in the previous attempt.

   - ✗ indicates that the data collection failed in the previous attempt.

   - ⏸ indicates that the data collection was never started.

Delete a SiteScope data source connection

1. In the Administration Console, click **Collection Configuration > SiteScope**.
   The SiteScope page opens.

2. Click **Delete**.
   A `Deleted Successfully` message appears in the Information message panel.

3. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel.

Monitoring SHR

After you perform the initial essential tasks to get SHR up and running, your next task is to monitor the SHR to ensure that it functions properly. The Administration Console provides an Internal Monitoring feature that you can use to monitor SHR.

You can use the Administration Console to perform the following monitoring tasks:

- View the status of SHR.

- Monitor the SHR content.

- Monitor the data processes.

- Monitor the SHR database.

- Monitor the application server platform.

Internal monitoring not only helps you identify the problematic processes or utilities that take a long time to run but also identify specific nodes where the data is stuck. If something goes wrong at the collection, reconciliation, or aggregation level, this feature helps you precisely identify the nodes where the problem occurred. You can also view the trend of usage of the database and the application server platform and a trend of the different data processes.

Using the Home page

SHR performs various self-monitoring tasks where it monitors the database system, its key services, the data collection, and the database loading operations. This information is displayed on the Home page of the Administration Console. The Home page gives you an overall status of the SHR components. You can directly troubleshoot performance issues with SHR by using this information. For additional information, you can drill down from this page by using the hyperlinks or open the relevant pages from the Task pane.

Monitoring SHR

Using the Home page, you can perform the following monitoring tasks:

- View the SHR status

- View details of the ABC alerts

View SHR status

The Home page displays information such as the status of the SHR services, the host system, and the database. You can view the number and status of active streams for the installed Content Pack components and the status of the data collection. You can also view the list of ABC and database alerts reported by SHR.

The Home page includes the following tables:

Group	Field	Description
Status Summary	Services Status	This table displays the status of the SHR database and SAP BOBJ Enterprise services. Status of the service: • ⬆ indicates that all the services are running successfully. • ⬇ indicates that one or all of the services are not running. The data displayed in this table is refreshed periodically. Click ↻ to update the table with the latest data.
	Connectivity Status	The table displays the status of SHR's connectivity to the following components: • Tomcat service (SAP BOBJ Tomcat Service) • SAP BusinessObjects Central Management Service (SAP BOBJ CMS) • SHR database (HP PMDB Platform Sybase)
	SHR Server System	This panel displays the host name, disk space, memory utilization (graph), and CPU utilization (graph) of the SHR system.
	IQ Server System	This panel displays the host name, disk space, memory utilization (graph), and CPU utilization (graph) of the SHR database system. If Sybase IQ is installed on a remote system and HP Operations agent is not installed on the same remote system, this panel displays "NA" to indicate that no data is available.
	BO Server System	This panel displays the host name, disk space, memory utilization (graph), and CPU utilization (graph) of the SAP BusinessObjects system of the SHR installation. If SAP BusinessObjects is installed on a remote system and HP Operations agent is not installed on the same remote system, this panel displays "NA" to indicate that no data is available.

Group	Field	Description
	Runtime File Distribution	Displays the data distribution of the SHR file system according to the size of the files in the following folders: • archive • collect • extract • stage • failed_to_* Before the data collected from the data sources are loaded into the appropriate Sybase IQ database tables, it is held in the SHR system for processing. Also, the data that failed to pass the data processing streams (*\stage\failed_to_** folder). are also stored on the SHR file system. Runtime file distribution shows the disk space used by these files.
	Content Health Summary	Displays the status of the data health in SHR fact tables for each installed content pack represented as follows: • **Success**: When data in SHR fact tables has been resolved. • **Failed**: When data in SHR fact tables could not be resolved and require attention. If a fact table encounters any of the following conditions, its health is marked 'Failed': • Data is not available for >10% of the dimensions. • Data is not available in hourly tables for the last 6 hours. • Data is not available in daily table for the last 1 day. • The table holds data for more than the configured period.

Group	Field	Description
ETL Status Summary	Content Pack Component Name	This table displays details of the Content Pack streams such as the total number of streams and the number of streams with errors. The total number of streams value indicates the number of streams that are currently running, or the number of streams that are loaded for execution, or the number of streams that completed in the last run. For additional information, you can drill down to the Data Processing page by clicking either the Content Pack component name or the stream number hyperlinks.
	Collection Status	Displays the number of data sources that are configured for each data collector. The status is represented in the following ways: • **Success**: When data collection from the data sources occurs without issues. • **Failed**: When data collection from the data sources has failed. • **Never Started**: When data collection from the data source has never occurred. The data displayed in this table is refreshed periodically. Click ⟷⟳ to retrieve the data from the memory to the database. Click ↻ to update the table with the latest data.
Alerts	ABC Alerts	This table list of all data processing job streams that have failed to complete along with their stream names, steps where the error occurred, messages, and dates. For more information, see View details of the ABC alerts.
	Health Alerts	This table displays the severity, message, and date of the all error, warning, and information alerts generated by SHR. The following icons are used to identify the types of alerts: • ⓘ indicates an information alert. No action is required for this type of alert. • ⚠ indicates a warning alert. You might need to resolve these types of alerts to ensure SHR functions properly. However, immediate action might not be required. • ✖ indicates an error alert. These are critical alerts and immediate action is required to resolve these issues.

View details of the ABC alerts

The SHR workflow framework creates an execution log file that stores the information of all the job steps. The ABC Alerts tab picks up and displays a list of the 10 latest active data processes that failed to complete successfully. You can use the information displayed on the ABC Alerts tab to troubleshoot data processing-related issues.

To view more information about the error:

1. Under the **Step Name** column, click a step name hyperlink.
   A dialog box opens.

2. View:

Field	Description
Status	Type of alert, which can be of two types: ■ Error—This status indicates that the job step failed to complete the execution process because of a serious error. The execution of the job stream cannot continue. ■ Maximum execution time exceeded—This status indicates that the job step failed to complete the execution process within the defined time frame.
Detail Message	Displays the execution log of the job step with detailed information on how the error was generated during the execution of the job step. An experienced user can also obtain all the necessary details related to the stream execution status by looking at the relevant dictionary and run-time tables.
Command	The command that was used to run the job stream when the error was generated. This field only appears for job steps with error states.
Max Retries	Maximum number of retries for the job step.
Remaining Retries	The number of remaining retries for the job step.
Max Execution Time (Mins)	Maximum execution time, in minutes, for the job step.
Start Time	Time when the execution of the job step started.
End Time	Time when the execution of the job step ended.

3. Click **OK**.

Monitoring the SHR content

In SHR, a fact table consists of the measurements or facts of a business process. It is often located at the center of a star schema or a snowflake schema, surrounded by dimension tables. The dimension tables contain attributes (or fields) used to constrain and group data when performing data processing queries. Fact tables are often defined by their grain. The grain of a fact table represents the smallest level by which the facts may be defined. For example, the grain of a CPU fact table might be stated as CPU utilization every five minute or CPU utilization every day. In the SHR database, the raw data or rate data that is collected is stored as unique records in fact tables called "As-polled" table or "5-minute" table. The workflow process then performs summary routines on these tables and converts it into hourly, daily, monthly, and yearly data. The converted data is stored in hourly, weekly, monthly, or yearly fact tables.

> **Note:** Monthly table and yearly table are not physical tables in the database for any out-of-the-box (OOTB) content packs.

SHR allows you to monitor the data throughput, that is, the volume of data that is stored in the database, for specific Content Pack component. Using the SHR Content page, you can monitor the growth of the fact tables for a specific Content Pack component.

Using this page, you can perform the following tasks:

- View the installed Content Pack components

- View the fact table details

View the installed Content Pack component

1. In the Administration Console, click **Internal Monitoring > Service Health Reporter Content**. The SHR Content page opens.

2. View:

Field	Description
Content Pack Component Name	Name of the Content Pack component.
Installation Date	Date and time of installation of the Content Pack component.
Version	Version number of the installed Content Pack component.
Detail	Option to view fact table details for the Content Pack component.

View the fact table details

1. In the Administration Console, click **Internal Monitoring > Content**.
   The Content page appears.

2. For a specific Content Pack component, click **Detail**.
   The Fact Details tab opens.

3. On the **Fact Details** tab, view:

Field	Description
Fact	The fact table alias.
	Clicking the Fact hyperlink opens the Fill Detail graph for the corresponding fact table. This graph displays the rate at the Fact table is growing based on the number of rows added at a point of time in the:
	■ Last 1 Day
	■ Last 7 Day
	The row count is checked at a six-hour interval and the graph is plotted accordingly.
Fact Row Count	Total number of rows currently in the fact table.
Dimension Instance	Total number of dimensions for the corresponding fact table. In the case of a star schema, this is the total number of primary dimensions.
Last Updated Row Count	The total number of rows that were updated during the last aggregation.
Last Updated	Time (in GMT) when the fact table was last updated.

Note: The fact table information displayed on this page is stored in the database for seven days, after which it is purged.

Monitoring the data processes

SHR provides a workflow framework that handles the tasks of taking raw data, running reconciliation and aggregation routines on it, and then loading the data into the data store. The Content Packs contains the predefined workflow job streams[1] that are loaded into the framework during the installation of the Content Pack. A job stream is made up of multiple job steps, which are processed in batches[2] by the workflow framework.

[1]A set of workflow execution tasks related through parent-child relationships. A child task can have zero, one, two, three, or more parent tasks.
[2]A run-time instance of a job stream is called a batch.

The workflow framework centrally organizes and manages the flow and the execution of the steps that each job stream based on metadata defined in the Content Packs.

The following figure illustrates the execution flow of a sample SHR job stream.

In this example, the job stream starts from data collection and ends with facts aggregation. All steps are dependent on the preceding steps; therefore, in the event of a failure on one of the steps, the workflow framework prevents the job stream from completing successfully. The workflow framework loads the next job stream for execution only after the current stream completes successfully.

Using the workflow framework, you can:

- Monitor the status of the execution of the workflow.

- Control the processes that move data into the data store.

Knowing how the workflow job streams perform becomes the most important task in monitoring the status of the SHR database operations.

Monitoring job stream details

SHR provides you with a way of monitoring the execution of the job streams of each installed Content Pack. The Data Processing page of the Administration Console displays stream information under the following three tabs:

- Stream Details—This tab displays information about the status of active streams that are currently running. You can also view the step-wise execution flow of the job stream.

- Historical Stream Overview—This tab displays number and status of the job streams that completed with errors or with warnings. Job streams that were aborted by the user because of it warning or error state, also appear on this tab.

- Historical Streams Details—This tab displays a graphical trend of the number of error and warning states encountered by a job stream during its execution over a period of time.

Using the Data Processing page, you can monitor the execution of the active job streams and troubleshoot any issues if the execution fails. In addition, you can perform a trend analysis for the

stream over a period of time to identify the cause of the failure. On this page, you can perform the following data stream monitoring tasks:

- View the data stream details

- View the historical stream details

- View the historical trend of the streams

View the job stream details
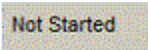
To view the number of job streams for a Content Pack component:

1. In the Administration Console, click **Internal Monitoring > Data Processing**.
   The Data Processing page opens.

2. On the **Stream Details** tab, view:

Field	Description
Content Pack Component name	Name of the Content Pack component.
Number of Streams	Total number of job streams. This value indicates the number of streams that are currently running, or the number of streams that are loaded for execution, or the number of streams that completed in the last run.
Stream Status Details	Status of the job stream which can be one among the following: ■ OK—The number of job streams that completed successfully. ■ Warning—The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream. ■ Error—The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved. ■ Total—The total number of streams that are running.

To view the details of the streams:

1. Click a number in the **Number of Streams** column to open the Stream Detail for Content Pack Component table.

2. View:

Field	Description
Stream Name	Name of the job stream.
Step Status (Completed/Total)	Status of the job stem in the stream. Completed indicates the number of steps in the job stream that have completed irrespective of whether it was successful or generated a warning or an error. Total indicates the total number of job steps in the stream.
Step Status	Status of the job step execution: Not Started indicates that the job stream has not started running but has been loaded for execution. SUCCESS indicates that all job steps in the stream completed successfully. WARNING indicates that some job steps completed with warnings. ERROR indicates that a job step in the stream failed to complete and generated an error.
Start Time	Local time when the execution of the job step started.

3. To view a diagrammatic representation of the job stream, in the **Start Time** column, click a specific Start Time hyperlink.
   The **Stream Details** diagram opens which displays the execution flow and status of the job steps.

4. Click a job step icon in the diagram to open a detailed message box about that job step.

5. View:

Field	Description
Step name	The name of the job step.
Process Id	The unique identifier for the job step.
State	The state of the job step. The options include: ▪ FINISHED—indicates that the job step finished running. ▪ WAITING—indicates that the job step is waiting to be run. ▪ RUNNING—indicates that the job step is currently running.

Field	Description
Status	Status of the job step. The options are: ■ SUCCESS—indicates that the job step execution was successful. ■ WARNING—indicates that the job step completed but generated a warning. ■ ERROR—indicates that the job step failed to complete and generated an error. ■ MAX_EXEC_TIME_EXCEEDED—indicates that the job step failed to complete within the defined execution timeframe. ■ WAITING—indicates that the job step in currently in the waiting state because the preceding job step is yet to complete.
Detail Message	Displays the execution log of the job step with detailed information on how the warning or error was generated during the execution of the job step.
Log File	The name of the log file where information about the job step process is logged.
Command	The command that was used to run the job step.
Max Retries	Maximum number of retries for the job step. This field only appears for job steps with error or warning states.
Remaining Retries	The number of remaining retries. This field only appears for job steps with error or warning states.
Max Execution Time (Mins)	Maximum execution time, in minutes, for the job step. This field only appears for job steps with error or warning states.
Start Time	Time when the execution of the job step started.
End Time	Time when the execution of the job step ended.
Audit Details	A summarized view of the data audit information for the job step. The information can include the number of files or rows that were processed, passed, and failed and the time taken for the audit step.

6. Click **OK**.

To understand the information displayed in the job stream diagram and relate it to the information in the tables, see Understanding the job stream status. To troubleshoot the stream alerts, see the *Troubleshooting Guide*.

Understanding the job stream status

To help you understand the information displayed on the Data Processing page and the relationship between the states and statuses of the job streams, three possible job stream scenarios are provided.

Scenario 1

Consider the following sample job stream.
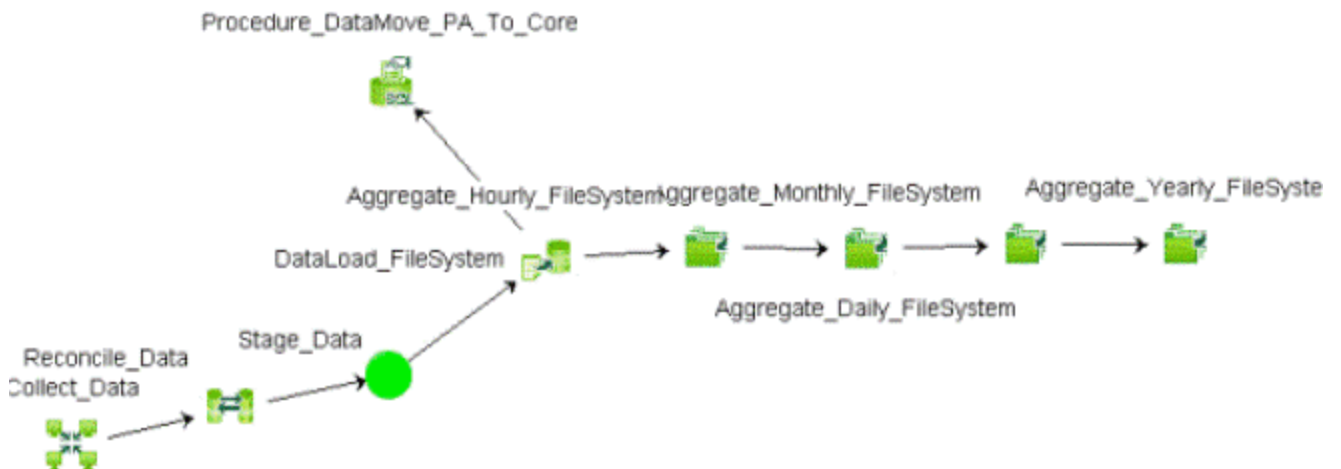
This job stream contains nine job steps. All of the job steps completed successfully, as indicated by the green color. In the **Step Status (Completed/Total)** column, the value for this stream will be 9/9 because there were nine steps and all the steps completed execution. The **Step Status** column displays the SUCCESS indicator because all the job steps completed successfully. Therefore, the job stream status is OK.

To know the state and status of the particular job step, such as DataLoad_FileSystem, you must click the job step icon. This opens a pop-up window, which displays the job step details including the state and status of the step. For the DataLoad_FileSystem job step, the state of the job step will be FINISHED, while the status will be SUCCESS. This job stream will no longer be active and gets moved to the Historical Stream section of the page. Now, let's look at another scenario.

Scenario 2

Consider the following sample job stream.
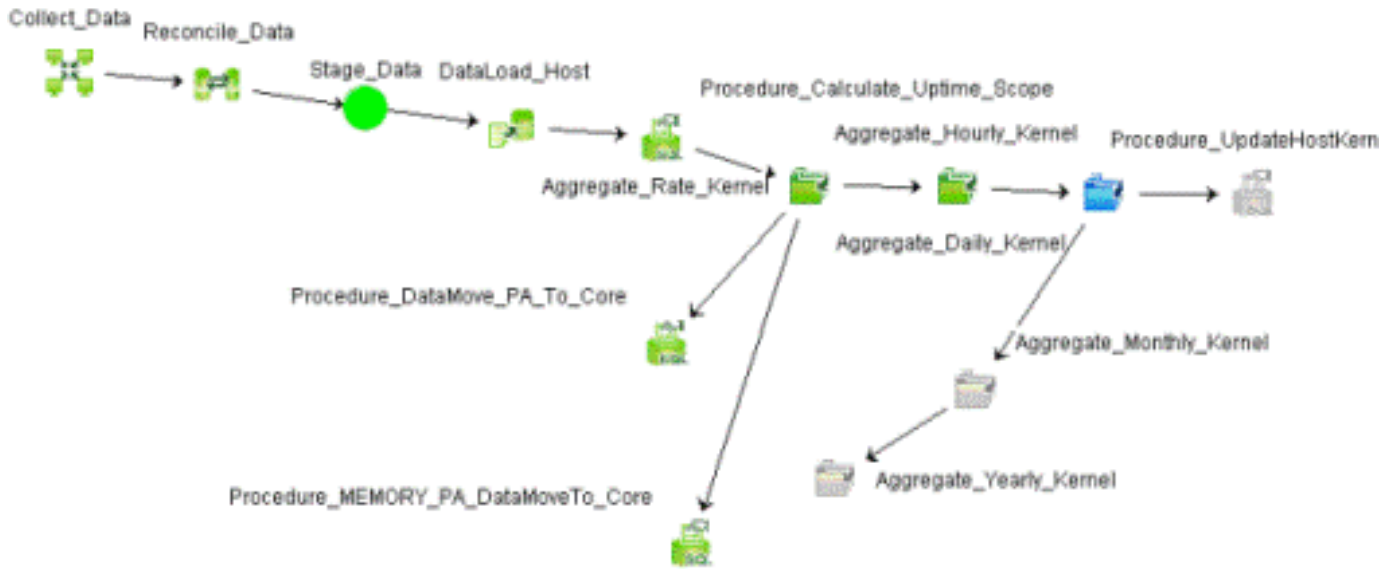
This job stream contains 13 job steps. In the **Step Status (Completed/Total)** column, the value for this stream will be 9/13 because only nine steps are complete. The tenth step, Aggregate_Daily_Kernel, is currently running, as indicated by the blue color. However, the **Step Status** column displays the

SUCCESS indicator. This is because all the job steps till the Aggregate_Daily_Kernel step completed successfully.

The job stream status is calculated based on the status of all job steps till the step that is currently running; in this case, the Aggregate_Daily_Kernel step. Therefore, the overall status of the job stream is OK because all job steps till Aggregate_Daily_Kernel completed successfully.

The state of the Aggregate_Daily_Kernel step will be RUNNING, while its status will be WAITING. The state and status of the remaining three job steps that are in gray color will be WAITING because these job steps will only start after Aggregate_Daily_Kernel completes.

Scenario 3

Consider the following sample job stream.
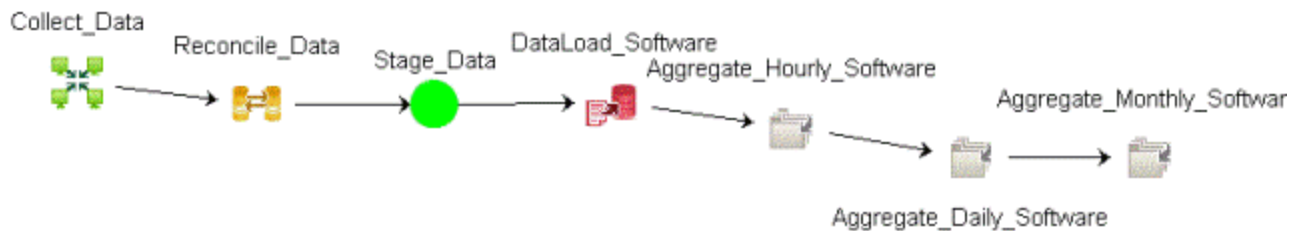
This job stream contains seven job steps. In the **Step Status (Completed/Total)** column, the value for this stream will be 4/7. However, the **Step Status** column displays the ERROR indicator because

the DataLoad_Software job step failed to complete. A failed job step continues to block the execution of the remaining steps until it is resolved. Therefore, only four job steps are complete in this stream.

The workflow framework will retry running the failed job step based on the number of retries defined for this job stream. Once all the retries are exhausted, the job stream will be blocked. The status of this job stream will be error. The state of the DataLoad_Software job step will be FINISHED, while the status will be ERROR or MAX_EXEC_TIME_EXCEEDED.

If you observe the Reconcile_Data icon, it has a yellow color. This indicates that Reconcile_Data job step completed but with warnings. However, this does not block the job stream and, as you can see, the Stage_Data job step completed successfully. The state of the Reconcile_Data job step will be FINISHED, while the status will be WARNING.
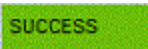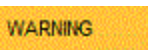
View the historical stream details

To view the number of historical job streams for a Content Pack component:

1. In the Administration Console, click **Internal Monitoring > Data Processing**.
   The Data Processing page opens.

2. Click **Historical Stream Overview**, select one of the following **Stream Details** options:

   - Last 1 day

   - Last 7 days

   Note: The workflow framework stores information about job steps in run-time tables for a maximum period of 7 days, after which the data is automatically purged by the PMDB_Platform_ IM_Service.

3. In the table, view:

Field	Description
Content Pack Component name	Name of the Content Pack component.
Number of Streams	Total number of job streams that ran during the specified period of time.

Field	Description
Stream Status Details	Status of the job stream which can be one among the following: ■ OK—The number of job streams that completed successfully. ■ Warning—The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream. ■ Error—The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved. ■ Total—The total number of streams that are running.

To view the details of the job stream:

1. Click a number in the **Number of Streams** column to open the Stream Detail for Content Pack table.

2. View:

Field	Description
Stream name	Name of the job stream.
Stream Status Details	Status of the job stream which can be one among the following: ■ OK—The number of job streams that completed successfully. ■ Warning—The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream. ■ Error—The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved. ■ Total—The total number of streams that are running.

View the historical trend of the streams

1. In the Administration Console, click **Internal Monitoring > Data Processing**.
   The Data Processing page opens.

2. On the **Historical Stream Details** tab, under **Select Filter**, select a Content Pack component in the **CP** list.

3. In the **Stream** list, select a stream.

4. In the **Severity** list, select the appropriate severity option that you want to generate the graph for. The option include:

   ■ WARNING—displays the number of warning states encountered by the job stream during its execution.

   ■ ERROR—displays the number of error states encountered by the job stream during its execution.

5. In the **State** list, select the required state of the job stream. The options include:

   ■ ALL—all states of the job stream.

   ■ FINISHED—state where the job stream completed successfully irrespective of the warning or error encountered during its execution.

   ■ ABORTED—state where the execution of the job stream was aborted by the user.

6. Click **Find**.

   The graph for the selected stream is displayed. This graph displays the number of times a job stream generated a warning or error over a specific period of time.

Alternatively, you can access the historical stream trends directly from the Historical Stream Overview tab. On the **Historical Stream Overview** tab, click the hyperlink or the 📊 icon in the **Content Pack Component name** column or the **Stream Name** column to view the historical trend for the job stream.

Back up and restore SHR PostgreSQL management database

The SHR PostgreSQL management database stores three types of information:

- Data processing stream information

- Internal tables that control the deletion of stage tables (stage_control)

- Collection audit information (Data Audit)

Backing up the database

You might want to back up the management database for data recovery purposes. To back up the database, follow these steps:

1. Stop the PMDB Platform Timer service.

2. Stop the PMDB Platform Collection service.

3. Wait for all the loaded data processing stream processes to stop running.

4. Check the status of the streams on the Data Processing page of the Administration Console. You can also check the status by typing the following command:
   `abcMonitor -stream ID=ALL, state=active`

5. Back up the database using a PostgreSQL database backup utility.

Restoring the database

You might want to restore the management database to get the historical step execution status details. To restore the database, follow these steps:

1. Stop the PMDB Platform Timer service.

2. Stop the PMDB Platform Collection service.

3. Wait for all the loaded data processing stream processes to stop running.

4. Check the status of the streams on the Data Processing page of the Administration Console. You can also check the status by typing the following command:
   `abcMonitor -stream ID=ALL, state=active`

5. Restore the Management database using a PostgreSQL restore utility.

6. Restart the PMDB Platform Collection Service and the PMDB Platform Timer service after the restore operation is complete.

After the services are started, the data processing framework automatically starts executing the restored steps from where it stopped, handling the Step status automatically. Restoration of the old database also results in old data for the stage_control and data audit tables. However, these tables are automatically updated by the framework within a couple of hours.

Monitoring the SHR database

SHR uses the Sybase IQ database for managing and storing the data that is collected from the various HP product center repositories. Workflow operations are performed on the collected data after which the data is stored in the data store for analysis purposes. Unlike traditional databases, which store data in rows, Sybase IQ stores data by columns, which can be stored separately and across multiple disks. This method of data storage ensures easier and faster data access, improved storage management, faster aggregations, and improved analytical performance.

In Sybase IQ, indexes have been redesigned to improve data retrieval performance. Traditionally, indexes are often used as a reference mechanism that pointed to the storage area that contained the

capability, which is used to manage large query loads on the database.

At an application level, Sybase IQ distributes data across multiple disks by representing each device as a dbspace. A dbspace can be an operating system file (dbfile) or a raw disk partition. Dbspaces can contain both user data and internal database structures used for startup, recovery, backup, and transaction management.

A database that you create using a Sybase IQ server is called an IQ database. Each IQ database that you create includes three stores:

- IQ main store—Contains the IQ_SYSTEM_MAIN dbspace and other user dbspaces, where persistent database structures, such as permanent data tables, backup metadata, and rollback data for committed transactions, are stored.

- IQ temporary store—Consists of a set of temporary tables. The database server uses them for sorting and other temporary processing purposes.

Note: The size of the total database space depends on the volume and retention policies you select while creating the schema.

Sybase IQ is the platform on which PMDB, the database repository for all SHR-related data, is created. The data is stored in the database in designated table, which are created when you create the database schema during the post-installation stage of SHR.

Monitoring the database health and availability

The Database Monitoring page of the Administration Console provides a detailed status of the health and availability of SHR database. Monitoring the database helps you to:

- Check the availability of database servers.

- Monitor the database size, buffer cache size, database connection time, and database polling time.

- Analyze the number of user connections to the databases at various time.

- Analyze usage trends.

- Identify potential database performance problems.

- Take actions proactively before critical incidents occur.

Using the Database Monitoring page, you can view the database details.

View the database details

To view the database information including the availability, CPU, and memory usage of the database:

[1]Multiplexing is a highly scalable shared disk grid technology where the database that is stored in a disk array is shared across multiple data sources. This technology provides application scalability through a clustered server configuration and can support tens of thousands of users with little or no data load or query performance degradation.

1. In the Administration Console, click **Internal Monitoring > Database Monitoring**.
   The Database Monitoring page opens.

2. Under **Database Information**, view:

Field	Description
Status	Connection status of the SHR database: ■ ⬆ indicates that the connection to the database has been successfully established. The database is up and running. ■ ⬇ indicates that there is no connection to the database. The database is down.
Host Name	Name or IP address of the SHR database server.
Port	Port number to query the database. The default port is 21424.
Version	Version number of the database.
Database type	Type of the SHR database.
Platform Detail	Operating system installed on the platform that is hosting the SHR database.
Multiplexed	Multiplexing capability of the database is enabled or not.
Database Size	Total size of the database main store in megabytes.
Page Size	Amount of memory allocated for storing database entries.
Last Backup Time	Time at which the database instance was last backed up.
Last Full Backup Time	Time when a full backup was performed on the database.
Last Started	Time at which the database service was last started.
Last DB Polled	Time at which the database was last polled.

3. Under **Database Availability**, view the availability of the database:

Field	Description
Database Availability	The amount of time the database was available in the: ■ Last 7 days ■ Last 1 day **Legend description**: ● indicates the amount of time, in hours, the database was available. ● indicates the time, in hours, the database was not available.

4. Under **DBSpace Usage**, view the dbspace usage information:

Field	Description
DBSpace Usage	Graphical representation of the database space, in megabytes: ■ **IQ_System_Main**: The IQ_System_Main dbspace is created at database creation. IQ_SYSTEM_MAIN is a special dbspace that contains structures necessary for the database to open such as the IQ checkpoint log, IQ rollforward/rollback data for each committed transaction and each active checkpointed transaction, the incremental backup metadata, and database space and identity metadata. IQ_SYSTEM_MAIN is always online when the database is open. ■ **IQ_System_Temp**: The IQ_System_Temp is a single dbspace for the IQ temporary store created when you create a database. It stores the temporary database files. ■ **PMDB_User_Main**: This is the user main dbspace that is used for storing user-defined tables, indexes, and table metadata that is specific to SHR data. **Legend description**: ■ indicates reserved space, which is used for storing certain small but critical data structures used during release savepoint, commit, and checkpoint operations. ■ indicates used space, which is used for storing the main user tables and indexes. ■ indicates free space, which is the space available for use.

5. Under **DBSpace Usage**, click a specific histogram, which represents the IQ System Main Store, IQ System Temp Store, and the main user database.
    The DBSpace Fill Details box opens.

6. Select **Last 1 Day** or **Last 7 Day** to view the graphical representation of the amount of database space, in megabytes, used by the selected store over a period of time.

7. Under **Current Activities**, view the current activities of the database:

Field	Description
Connection (Used/Max)	Number of active user connections to the database and the maximum number of connections the database can handle.
(%) CPU Utilization	Percentage of CPU time that is being used by all the activities in the database.
Open Transaction	Number of transactions that are currently running in the database.
Active Txn Versions	The number of active write transactions and the amount of data they created and destroyed.
Other Versions	Other database versions and the total space consumed.
Active Requests	Number of server threads currently handling a request.
IQ Threads (Used/Free)	Number of threads that are allocated to process queries and data loads and the number of threads that are not in use.

8. Click the following icons on the **Current Activities** header to start or stop the current activity polling of the database:
   - Click the icon to start current activity polling.

   - Click the icon to stop current activity polling.

9. Under **IQ Physical Memory Trend**, view the physical memory usage trend:

Field	Description
IQ Physical Memory Trend	Graphical representation of the physical memory usage of the Sybase IQ server, in megabytes, for the last one day. — indicates the current physical memory usage trend. — indicates the maximum physical memory usage trend.

Monitoring the application platform

The Platform page of the Administration Console enables you to monitor the Administration Console's application server. Monitoring the application server platform provides data to diagnose the cause of poor application performance.

Using the Platform page, you can view the application server details.

View the application server details

To view information about the application server, its availability, CPU, and memory usage:

1. In the Administration Console, click **Internal Monitoring > Platform**.
   The Platform page opens.

2. Under **Application Server Information**, view:

Field	Description
Host Name	Name of the Administration Console application server.
Port	Port number to query the Administration Console application server.
Host OS	Operating system installed on the application server.
Server Type	Type of application server.
Virtual Machine Name	Name of the application server host virtual machine.
Virtual Machine Version	Version number of the application server host virtual machine.
Virtual Machine Vendor	Provider of the host virtual machine.

3. Under **Application Server Availability**, view the availability of the application server:

Field	Description
Application Server Availability	Graphical representation of the time the application server was available in the: ■ Last 7 days ■ Last 1 day **Legend description**: ● indicates the time, in hours, the server was available. ● indicates the time, in hours, the server was not available.

4. Under **Memory Usage**, select **Heap Memory** in the **Memory Type** list to view the heap[1] memory usage.

5. Under **Latest (%) Heap Memory Usage**, view:

[1]Dynamic memory allocation or heap-based memory allocation is the allocation of memory storage for use in a computer program during the runtime of that program.

Field	Description
Latest (%) Heap Memory Usage	Graphical representation of the percentage of heap memory usage. **Legend description**: ⬤ indicates that the heap memory usage is within the critical limits. ⬤ indicates that the heap memory usage is outside the critical limits.

6. Under **Memory Usage**, select **Non-Heap Memory** in the **Memory Type** list to view the non-heap memory usage.

7. Under **Latest (%) NonHeap Memory Usage**, view:

Field	Description
Latest (%) NonHeap Memory Usage	Graphical representation of the percentage of non-heap memory usage. **Legend description**: ⬤ indicates that the non-heap memory usage is within the critical limits. ⬤ indicates that the non-heap memory usage is outside the critical limits.

8. Under **Memory Usage**, select the following options to view the historical memory usage of the application server:

Field	Description
Memory Type	Type of memory, heap or non-heap.
Memory Usage	Maximum available memory and a graphical representation of the amount of Heap and Non-Heap memory used, in megabytes, by the application server in the: ■ Last 7 Days ■ Last 1 Day

9. Under **Latest (%) CPU Utilization**, view the current CPU utilization of the application server:

Field	Description
Latest (%) CPU Utilization	Graphical representation of the percentage of CPU utilization. **Legend description**: indicates that the CPU utilization is within the critical limits. indicates that the CPU utilization usage is outside the critical limits.

10. Under **CPU Usage**, view the historical CPU utilization of the application server:

Field	Description
CPU Usage	Graphical representation of the percentage of CPU used by the application server in the: ■ Last 7 Days ■ Last 1 Day

Administering SHR

Using the Administration Console, you can perform additional administrative tasks that improve the accessibility, usability, and operability of SHR.

You can use the Administration Console to perform the following administrative tasks:

- View the database credentials.

- View the licensing details.

- Configure the security access for the database.

- Control the execution of the workflow job streams.

- Manage user accounts.

- Configure the data retention period.

- Manage the SHR services.

- Configure the time shifts.

Configuring SHR

System configuration involves managing the centralized SHR database. The SHR database stores fact and topology information collected from different data sources based on the policies that are

defined in the Content Packs. The database is configured when you perform the post-install configuration steps after installing the SHR application. The database size is allocated based on the volume and retention policies that you select during the post-installation stage.

Note: After you set the volume and retention policies and define the database size the first time, you cannot modify the database size through the Administration Console.

Managing the database

Using the System Configuration page, you can perform the following tasks:

- View database configuration details

- Change the SHR database password

- Change the SHR management database password

View database configuration details

1. In the Administration Console, click **Administration > System Configuration**.
    The System Configuration page opens.

2. Under **HP SHR Database Parameters**, view:

Field	Description
Database Type	Type of the database engine that is used for the SHR database. **Note**: SHR only supports Sybase IQ database.
Host name	Name or IP address of the host system on which the SHR database is running.
Server name	Name of the SHR database server.
Port	Port number to query the database. The default port is 21424.
User name	Name of the SHR database user account. This account is created during the post-installation stage.

3. On the **Management Database Configuration** tab, under **HP SHR Management Database Parameters**, view:

Field	Description
Database Type	Type of the database engine that is used for the SHR management database.

Field	Description
Host name	Name or IP address of the host system on which the SHR management database is running.
Database name	Name of the SHR management database instance.
Port	Port number to query the management database. The default port is 21425.
User name	Name of the SHR management database user account. This account is created during the post-installation stage.

Change the SHR database password

1. In the Administration Console, click **Administration > System Configuration**.
    The System Configuration page opens.

2. Click **Reset Password**.
    The Reset Password dialog box opens.

3. In the **Reset Password** dialog box, type the database password details:

Field	Description
Old Password	Enter the existing database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value and less than 25 characters in length.
Confirm New Password	Retype the new password for confirmation purposes.

4. Click **OK**.
    A `Password Successfully Changed` message appears in the Information message panel indicating that the password has been successfully changed.

Change the SHR management database password

1. In the Administration Console, click **Administration > System Configuration**.
    The System Configuration page opens.

2. On the **Management Database Configuration** tab, click **Reset Password**.
    The Reset Password dialog box opens.

3. In the **Reset Password** dialog box, type the database password details:

Field	Description
Old Password	Enter the existing management database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value and less than 25 characters in length.
Confirm New Password	Retype the new password for confirmation purposes.

4. Click **OK**.

   A `Password Successfully Changed` message appears in the Information message panel indicating that the password has been successfully changed.

Managing licenses

By default, SHR includes a temporary, instant-on license, which is valid for 60 days. To continue using SHR after 60 days, you must install a permanent license.

The SHR license includes:

- **HP Service Health Reporter Software**: This license includes the data collection framework, the SAP BusinessObjects Enterprise, a high-performance Performance Management Database for storing and processing the collected metrics, and the out-of-the-box Content Packs. Also included is an entitlement to collect and report on the metrics for up to 250 nodes.

- **Additional scalability packs of 50 nodes**: Additional data collection and reporting entitlements can be added to grow the solution to fit your environment.

SHR is integrated with the HP License Manager licensing package for its licensing needs. The HP License Manager provides the SHR license framework and the functionality of installing a temporary or permanent license.

Basic license information is displayed on the Licensing page of the Administration Console. To obtain a permanent license, you can either use the HP License Manager or directly retrieve the license from the HP Password Center by using the HP Webware web site.

Configuring license

Using the Licensing page, you can perform the following tasks:

- View license information

- Obtain a Permanent license key

- Install the Permanent license key

- SAP BOBJ license reactivation

View license information

1. In the Administration Console, click **Administration > Licensing**.
   The Licensing page opens.

2. Under **HP SHR License Details**, view:

Field	Description
Active License Type	Type of existing license; license types include: ■ Instant On (IO) ■ Permanent (PERM)
License Expiry Date	Date and time of expiry of the existing license in local time.
Days to License Expiry	Number of days remaining for the license to expire.
License Entitlement	The maximum number of nodes that are supported under the current license.
License Usage	The number of nodes being used under the current license.
Nodes Remaining\Nodes Exceeded	The remaining number of nodes that can be added under the current license or the number of nodes that exceed the current license usage.

Obtain a Permanent license key

1. From the Administration Console, select **Administration > Licensing**.
   The Licensing page opens.

2. Click **Launch HP Password Center**.
   The HP License Key Delivery Service page opens.

3. Click **Generate New licenses** under Welcome.

4. Log on to HP Passport with your user ID and password. If you do not have an account, you must create one before you can proceed. The Order number page opens.

5. Type the order number in the **Order number** field and click **Next**.
   The Product selection page opens.

6. Select **PERM** and click **Next**.
   The License redemption page opens.

7. Select **Find or create a license owner** and type your email address in the **License Owner e-mail address** field.

8. Type the IP address of the SHR host system and click **Next**.
   The Create license owner page opens.

9. Type the license owner information:

Field	Description
Create license owner (End-User) information	Name, phone number, and email address of the license owner.
Company e-mail domain	Domain name of the license owner's company.
Mailing address	Mailing address of the license owner.
License owner privacy policy (Optional)	Optional settings for License owner privacy policy.

10. Click **Next** to continue.
    The Transaction summary page opens.

11. Review the summary and click **Next** to continue.
    The License certificate page opens.

12. Review the license certificate information, save the license to your system, and then close the License certificate page.

Install the Permanent license key

You must install the permanent license key by using HP License Manager.

To install the license:

1. *On Windows.* Click **Start > Programs > HP Software > Service Health Reporter> License Manager**.

   On Linux. Run the command **$PMDB_HOME/bin/LicenseManager.sh**.

   The Retrieve/Install License Key window opens.

2. Click **Install/Restore License Key from file**.
   The Install/Restore License Key from file page opens.

3. Browse to the location of the saved license certificate, click **View file content**, select **PERM**, and then click **Install**.

Reactivate SAP BOBJ license and Re-enable the SAP BOBJ Servers

The SAP BOBJ license depends on the validity of the SHR license. If the SHR license expires, it deactivates the SAP BOBJ license key and disables all the SAP BOBJ servers.

To reactivate the SAP BOBJ license

1. Obtain a new SHRlicense key, see "Obtain a Permanent license key" on page 113

2. Install a new SHR license key, see "Install the Permanent license key" on the previous page

> **Note:** After you install the Permanent license key , wait for at least five minutes before accessing the Administration Console to reactivate the SAP BOBJ license.

3. Access the SHR Administration Console.

After you reactivate the SHR license and access the Administration Console, SHR automatically reactivates the SAP BOBJ license key. However, the SAP BOBJ servers remain in the disabled state. To ensure that SAP BOBJ works, you must manually enable the servers.

To enable the SAP BOBJ servers:

1. Log on to the Central Management Console by launching the following URL:

   http://I<SHR_System_FQDN>:8080/CmcApp

   In this instance, *<SHR_System_FQDN>* is the fully qualified domain name of the SHR system.

2. Log on as Administrator.

3. Click **Servers**.

4. Right-click each server, and then click **Enable Server**.

If Business Object services do not get activated even after installing new license, see Troubleshooting Business Object Services

Managing security

SHR provides seamless access to integrated HP and SAP BusinessObjects applications through Lightweight Single Sign-On (LW-SSO) and SAP BusinessObjects Trusted Authentication.

LW-SSO

Single Sign-On allows you to log on once to SHR and gain access to multiple integrated HP products or software systems without being prompted to log on again. The products within the configured group of products trust the authentication, and there is no need for further authentication when moving from one application to another. All requests to integrated applications are channeled through the LW-SSO authentication.

LW-SSO is embedded in SHR and does not require an external machine for authentication. You need only to specify the shared key (Init String[1]), which is used for encryption and decryption of the LW-SSO session token[2]. You must ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same Init String.

SHR supports LW-SSO authentication with the following HP products:

- HP Business Service Management

- HPOM

- HP OMi

Note: In SHR, all applications participating in an LW-SSO integration must use the same GMT time.

SAP BusinessObjects Trusted Authentication

SAP BusinessObjects Trusted Authentication facilitates single sign-on between SHR and SAP BusinessObjects applications. Applications that have established trust with the SAP BusinessObjects Central Management Server (CMS)[3] can use Trusted Authentication to allow users to log on without providing their passwords.

To use single sign-on, you must specify the SAP BusinessObjects shared key (Shared Secret), which is used for encryption and decryption of the Trusted Authentication session token. You must ensure that all the other applications in the Trusted Authentication environment have Trusted Authentication enabled and are working with the same shared key.

SHR supports Trusted Authentication with the following SAP BusinessObjects applications:

- SAP BusinessObjects Central Management Console (CMC)

- SAP BusinessObjects InfoView

For more information, see the *SAP BusinessObjects Enterprise Administrator's Guide*. For the latest documents, see http://help.sap.com/businessobject/product_guides/.

Configuring security

Using the Security page, you can perform the following tasks:

[1]Init String is a connection string that contains the initialization information. This information is passed as a parameter from the data provider to the data source while attempting to open a connection with the data source.
[2]A session token is a unique identifier—8-byte binary value—that is generated and sent from a server to a client to identify the connection between the server and the client.
[3]The CMS is a key component of the SAP BusinessObjects Enterprise XI that is bundled with SHR. It is responsible for handling security and managing services. The CMS maintains a database which contains information that helps you manage the SAP BusinessObjects Enterprise infrastructure.

- Configure LW-SSO authentication

- Configure SAP BusinessObjects Trusted Authentication

Configure LW-SSO authentication

1. In the Administration Console, click **Administration > Security**.
   The Security page opens.

2. Under **LW-SSO Configuration**, specify or type the authentication details:

Field	Description
Enabled	Enable or disable LW-SSO.
Domain	Domains for which LW-SSO is valid. By default, the SHR host system's domain is enabled.
Expiration Period (mins)	Period for which the LW-SSO session is valid. The default value is 60 minutes. **Note**: The LW-SSO expiration period should be at least the same value as that of the application session expiration value. The recommended value is 60 minutes. For applications that do not require high levels of security, you can configure higher values, such as 300 minutes. **Note**: All applications participating in an LW-SSO integration must use the same GMT time.
Init String	Shared key used for encryption and decryption of a LW-SSO session token. **Note**: For LW-SSO, ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same Init String.
Protected Domains	List of domains for which SSO is protected. By default, the SHR host system's domain is protected.

3. Click **Save**.
   The following message appears in the Information message panel: `LW-SSO Configuration saved successfully. Please restart the 'HP_PMDB_Platform_Administrator' service for these changes to take affect`. Restart the `HP_PMDB_Platform_Administrator` service for the LW-SSO Configuration changes to take effect.

Note: This page is only visible if SHR is installed on the system.

Configure SAP BusinessObjects Trusted Authentication

1. In the Administration Console, click **Administration > Security**.
   The Security page opens.

2. Click the **BO Trusted Authentication** tab.

3. Under **BO Trusted Authentication Configuration**, specify or type the authentication details:

Field	Description
Enabled	Enable or disable SAP BusinessObjects Trusted Authentication.
Shared Secret	Shared key used for encryption and decryption of a SAP BusinessObjects Trusted Authentication session token.

4. Click **Save**.
   A `Saved Successfully` message appears in the Information message panel. On successful save, the Shared key value gets automatically configured to CMC.

> **Note:** This page is only visible if SHR is installed on the system.

Managing data processes

Using the Data Processing page of the Administration Console, you can view the number and status of the job streams corresponding to each installed Content Pack. You can also configure the job streams and specify a maximum number of retries for the batches in the event of its failure during execution as well as a maximum execution time per step. When the number of retries for a job step exceeds the maximum number allowed, the workflow framework blocks the job stream and generates an error event.

The maximum execution time and maximum retries are two configuration parameters that directly impact the stream execution functionality. In the case of the maximum execution time, setting a very high value can result in delay in identifying hanged processes. Setting a low value can result in the step being marked as Error too often. In addition, the maximum retries option should be set to a positive value only if a retry could result in successful execution. This option is most commonly used to overcome resource unavailability issues.

However, the best way to arrive at the value for the configuration parameters is to understand the use case, test, and arrive at an optimum value.

The number of job steps that are run simultaneously in the workflow framework is proportional to the number of job streams under execution. However, if the number of streams deployed on a system is high, it can result in a very high load on the system, which can lead to system failure. In such a situation, the resource control feature of data processing helps mitigate problems caused by the high load by providing the ability to limit resource usage to configured limits.

By managing the job stream resources, you can:

- Provide exclusive access to resources and help resolve locking issues with critical resources. If the pool count is zero, then the access to the resource becomes exclusive.

- Control the number of processes that are launched. For example, if you set a pool count of "5" for a resource named "Summary" and attach the resource to all the data aggregation jobs, then only a maximum of five instances of five aggregations can run at any point of time. This way, you can control the number of processes that are running.

You can also specify the resource definition details and set limits for the number of streams that can access the resource types concurrently. By default, all resource types are configured with the unlimited count, which means that there is no control based on the resource type.

Using the Data Processing page, you can perform the following job stream administration tasks:

- Configure the maximum number of retries and the maximum execution time

- Configure the stream resource details

Configure a maximum number of retries and the maximum execution time

You can configure the maximum number of retries and the maximum execution time across all installed Content Packs, for a particular Content Pack, for a particular job stream in the Content Pack, or for a particular job step in the job stream. Perform the following steps:

1. In the Administration Console, click **Administration > Data Processing**.
   The Data Processing page opens.

2. On the **Active Stream Details** tab, in the **Select Filter** pane, perform any one of the following steps:
   - To configure the maximum number of retries and maximum execution time for all Content Packs, in the **Level** list, select **All content packs**.

   - To configure the maximum number of retries and maximum execution time for a particular Content Pack, in the **Level** list, select **Content pack**, and then in the **Content Pack component name** list, select the Content Pack component.

   - To configure the maximum number of retries and maximum execution time for a particular job stream, in the **Level** list, select **Stream**, in the **Content Pack Component name** list, select the Content Pack component, and then in the **Stream Name** list, select the job stream.

   - To configure the maximum number of retries and maximum execution time for a particular job step, in the **Level** list, select **Step**, in the **Content Pack Component name** list, select the Content Pack, and then in the **Stream Name** list, select the job stream.

3. Click **Enter maximum retries count** in the **Maximum Number of Retries** column, and type a value.
   Note: The maximum value that you can set for this field is 8640.

4. Click ✔ to accept the new value. If you want to change the value, click ✖, and then type a new value.

5. Click **Enter maximum execution time** in the **Maximum Execution Time (Mins)** column, and then type a value.
    Note: The maximum value that you can set for this field is 180 minutes.

6. Click ✔ to accept the new value. If you want to change the value, click ✖, and then type a new value.

7. Click **Save**.
    A `Saved Successfully` message appears in the Information message panel.

Configure the stream resource details

1. In the Administration Console, click **Administration > Data Processing**.
    The Data Processing page opens.

2. Click the **Stream Resource Control** tab to view the resource details.

3. For a specific resource type, if you want to provide the job streams with unlimited access resources, select the check box under the **Unlimited Resources** column.

4. To specify the number of streams that can access the resource type, under the **Resource Count** column, type a value in the box.
    Note: The maximum value that you can set for this field is 20,000.

5. Click **Save**.
    A `Saved Successfully` message appears in the Information message panel.

Managing user accounts

In SHR, user accounts are managed by using the SAP BusinessObjects Central Management Console (CMC). By default, SHR includes an Administrator account, which is created during the post-install configuration stage. The Administrator account is a privileged account for managing and configuring SHR. Only accounts with administrative privileges can log onto the Administration Console. You can create additional accounts with administrative privileges by using the SAP BusinessObjects CMC.

SAP BusinessObjects CMC

You create and manage user accounts by using the SAP BusinessObjects CMC, which is integrated with SHR. After you create user accounts and groups, you can specify access rights to them.

Using the SAP BusinessObjects CMC, you can perform the following user management tasks:

- Manage enterprise and general accounts

- Add users to groups

- Manage passwords

- Manage aliases

For more information, see the Central Configuration Manager documentation. This guide is located in the installation directory of SAP BOBJ at:

Windows: `<drive>:\Program Files (x86)\Business Objects\BusinessObjects Enterprise 12.0\Help\en`

Linux:
`/opt/HP/BSM/BO/bobje/enterprise120/warfiles/WebApps/CmcApp/help/en/administration`

For the latest help documents, see http://help.sap.com/businessobject/product_guides/.

SAP BusinessObjects InfoView

SAP BusinessObjects InfoView is the central web-based GUI in SHR that allows you to view and interface with reports and dashboards. You can use the integrated search facility or the folder navigation tree to locate specific reports. In addition, InfoView allows you to personalize your experience by customizing the Start page to display reports that you want to view when you log on, change your password, choose your preferred language, and the level of interaction for different information.

To know more about SAP BOBJ InfoView, see *Web Intelligence online guide*. This guide is located in the installation directory of SAP BusinessObjects at:

Windows: `C:\Program Files (x86)\Business Objects\BusinessObjects Enterprise 12.0\Web Content\Enterprise12\Help\en\webintelligence`

Linux: `/opt/HP/BSM/BO/bobje/enterprise120/warfiles/WebApps/CmcApp/help`

For additional information and the latest help documents, see http://help.sap.com/businessobject/product_guides/.

Managing accounts

Using the SAP BOBJ page, you can perform the following tasks:

- Access SAP BusinessObjects Central Management Console

- Access SAP BusinessObjects InfoView

- Create a password for the Administrator account

- Troubleshooting BusinessObjects Services

Access SAP BusinessObjects Central Management Console

1. In the Administration Console, click **Administration > SAP BOBJ**.
   The SAP BOBJ page opens.

2. Click **Launch CMC**.
   The SAP BusinessObjects CMC Login page opens.

Note: This page is only visible if SHR is installed on the system.

Access SAP BusinessObjects InfoView

1. In the Administration Console, click **Administration > SAP BOBJ**.
   The SAP BOBJ page opens.

2. Click **Launch InfoView**.
   The SAP BusinessObjects InfoView Login page opens.

3. Type

Field	Description
User Name	Name of the SAP BusinessObject InfoView user.
Password	Password of the SAP BusinessObject InfoView user.

4. Click **Log On**.
   The SAP BusinessObjects InfoView portal opens.

Note: This page is only visible if SHR is installed on the system.

Create a password for the Administrator account

If you want to create a password for the default Administrator user name, perform the following steps:

1. Access the SAP BOBJ CMC.

2. On the Central Management Console login screen, in the **User Name** field, type `Administrator`.

3. Click **Log On**. The CMC Home screen opens.

4. Click **Users and Groups**. The Users and Groups screen opens.

5. On the right pane, double-click **Administrators**.

6. Right-click **Administrator** and then click **Properties**. The Properties:Administrator dialog box opens.

7. Under **Enterprise Password Settings**, in the **Password** field, type a new password.

8. In the **Confirm** field, retype the password to confirm it. You can change the Administrator user name, if required, and specify other necessary details on this screen.

9. Click **Save & Close** to accept the changes.

10. Click **Log Out** to exit the Central Management Console.

Note: This task is valid only if SHR is installed on the system.

Troubleshooting BusinessObjects Services

1. Log in to **CMC** Application using http://<servername>:8080/CmcApp.

2. Click on **License Key** and verify if license exist. If no license exists then you have to obtain the license see SAP BOBJ License Reactivation

3. If license exist, click **Servers**, a page opens where you can check if the servers are enabled.

4. If not, select all servers and click on the **Enable** button to enable all the servers.

5. Go to the next page.

6. Enable the items in the **Server** section.

Managing data aging

SHR collects data from different data sources at periodic intervals based on the collection policies predefined in the Content Packs. The collected data is stored in the database in various types of fact tables. If the data is collected as polled events from the data source, it is called raw data and stored in "As-polled" tables. Data can also be collected as a 5-minute summarized data. This type of data is called rate data and stored in "5-minute" tables.

The SHR database performs aggregation routines on the raw or rate data through the workflow process. The aggregation routines convert the data into hourly and daily data. This data is then stored in the following physical data tables:

- Hourly—This table contains the raw or rate data that is aggregated at an hourly level.

- Daily—This table contains the hourly data that is aggregated at the daily level.

- Monthly—This table contains the daily data that is aggregated at the monthly level. (not available in OOTB content packs)

- Yearly—This table contains the monthly data that is aggregated at the yearly level. (not available in OOTB content packs)

When reports are generated for a month or year, the data from daily tables is aggregated online to display in the SHR reports. Monthly table and yearly table are not physical tables in the database for any out-of-the-box (OOTB) content packs.

The data tables vary based on the content pack. For a given content pack, the available data tables is based on the model defined for that content pack.

Active retention

To prevent the accumulation of excessive data in the tables, SHR ages the data. Aging involves the concept of retention time, which is the number of days the data is stored in the table. The aging process deletes the data when it has been in the table longer than the specified retention time for that table. Each table has a default retention time:

- As-polled table: 90 days

- 5-minute table: 90 days

- Hourly table: 365 days

- Daily table: 1825 days

- Monthly table: 1825 days (not available in OOTB content packs)

- Yearly table: 1825 days (not available in OOTB content packs)

Note: Dimension data such as CI types and nodes that is collected by SHR remains in the database tables. SHR does not delete this data.

Managing aging

Using the Aging page of the Administration Console, you can configure the active retention period.

Configure active retention period

1. In the Administration Console, click **Administration > Aging**
   The Aging page opens.

2. For a specific Content Pack component, click **Configure Retention**.
   The Content Pack retention configuration details appear.

3. Click **Edit**.

4. For a specific type of periodic data, type the number of days for which the data is to be retained.

5. Click **Save**.

A `Saved Successfully` message appears in the Information message panel.

Important Considerations:

- You cannot modify the active retention policies of the Core Content Pack components.

- You cannot modify the active retention policies of the ETL and App components for all content packs (modification is allowed only on the Domain component of all content packs).

Warning: For the Service Health and OMi Content Pack components, you should not change the retention period of the "As-polled" table. The data in this table is a snapshot data and the status might not change within a short period of time. However, you can change the retention periods of the hourly, daily, monthly, or yearly data.

Managing services

The SHR services are long-running executables that perform specific functions. These services are designed to automatically start when the application is launched or when the operating system is booted. If required, you can also start these services manually. You can use the Administration Console to monitor two sets of services—one for the SHR database and the other for SAP BOBJ Enterprise.

The SHR database services include:

- PMDB Platform Collection Service—This service handles the configuration of the data collection policies based on the rules defined in the Content Packs. Stopping this service halts all collection-related tasks.

- PMDB Platform DB Logger Service—This service handles all logging-related tasks and is responsible for capturing and logging serious and critical events. This service reads the events and displays the information to the end user through the Administration Console and log files. In addition, the PMDB Platform DB Logger service logs events in the BSMRApp.log file. If this service is stopped, SHR cannot update the log files or display any alerts or events.

- PMDB Platform Timer—This service manages the scheduling of the SHR database processes. If this service is stopped, all data processes become affected such as data summarization, aggregation, and storage. In addition, maintenance tasks no longer occur. In short, the SHR database stops to function.

- PMDB Platform IM Service—This service handles the internal monitoring-related tasks of the SHR system. It collects and displays information related to the health and performance of the system to the user through the Administration Console. Stopping this service prevents SHR from displaying monitoring-related information, such as the status of the fact tables, the data processes, and the performance and availability of the SHR database and the application server platform.

- SHR PostgreSQL service—This service manages the PostgreSQL management database processes. This database is used by SHR to store data processing information, internal tables that control the deletion of stage tables, and collection audit information.

The SAP BOBJ Enterprise services include:

- SAP BOBJ Apache Tomcat—This service handles the deployment of SAP BusinessObjects-related administrative web applications and servers. Stopping this service prevents the deployment of the web applications.

- SAP BOBJ CMS—This service collectively manages all the other SAP BusinessObjects services and applications. If this service is stopped, all SAP BusinessObjects-related services and applications cannot work.

Managing services

Using the Services page, you can perform the following tasks:

- View the status of an SHR service

- Start or stop an SHR service

- View the status of a SAP BOBJ Enterprise service

View the status of an SHR service

1. From the Administration Console, select **Administration > Services**.
   The Services page opens.

2. In the **Service** list, select **HP SHR Status**.

3. View:

Field	Description
Service Name	The name of the SHR service.
Description	A description of the service.

Field	Description
Status	The status of the service. **Legend description**: ⬤ indicates that the service is up and running. ⬤ indicates that the service is not running. ⚠ indicates a warning. ⬤ indicates that the status of the service is unknown.
Start/Stop	Option to start or stop the service.

4. For a detailed status of the service, click the hyperlink in the **Service Name** column.
   The Service Detail for table appears, which provides detailed status information such as status of the service, status of the Java Virtual Machine (JVM), and status of the disk space. This table organizes information into two tabs:
   - Service Message Detail—Displays details of the status message.

   - Service Dependency—Displays the services that have a dependency on the selected service.

5. On the **Service Message Detail** tab, view:

Field	Description
Severity	The severity of the message. **Legend description**: ⬤ indicates that the service is running. ⬤ indicates an error. ⚠ indicates a warning. ⬤ indicates that the status of the service is unknown.
Message	A detailed description of the status.

6. On the **Service Dependency** tab, view:

Field	Description
Name	The name of the SHR service that has a dependency on the selected service.

Field	Description
Service Name	The name of the service as displayed in the Services window.
Dependent	Indicates that the displayed service is depends on the selected service.
Depends On	Indicates that the selected service depends on the displayed service.

Start or stop a SHR service

1. From the Administration Console, select **Administration > Services**.
   The Services page opens.

2. In the **Service** list, select **HP SHR Status**.

3. In the table, perform any one of the following steps:
   - Click **Start** to start a service that is currently not running.

   - Click **Stop** to stop a service that is currently running.

Important: If you change the system date after installing SHR, make sure that you restart all the SHR services.

View the status of a SAP BOBJ Enterprise service

1. From the Administration Console, select **Administration > Services**.
   The Services page opens.

2. In the **Service** list, select **SAP BOBJ Enterprise status**.
   The list of services and their status is displayed.

Note: This page is only visible if SHR is installed on the system.

Managing time shifts

Using SHR, you can configure the shift timings and enable shift-based availability reporting for the monitored system resources in your environment. Out-of-the-box, SHR defines a default shift period, which ranges from 0 to 23 hours.

Using the Shift Management page of the Administration Console, you can define the shift timings. Once configured, the shifts are applied globally across all relevant reports.

When configuring the shifts, you must consider the following points:

- Shift-based data is available to a maximum of the initial history (by default, this is set to 15 days) prior to the current date when the shift is created.

- You can modify the start and end times of the shifts.

- A shift must have a time range defined.

- The value must be in the 24-hour format.

- You can define multiple shifts.

- A single shift can have multiple time ranges.

- Shifts can have overlapping time ranges.

- You can delete a time range from the shift.

- If you delete a shift, all the time ranges within that shift are also deleted.

- You cannot create a shift that has the same name of an existing shift.

- Time ranges that do not correspond to any shift is referred to as off-shift.

- Node or group-level shift configuration is not supported.

Using the Shift Management page, you can:

- View time shifts

- Create a new time shift

- Modify the time shift

- Expire the time shift

View shift information

1. In the Administration Console, click **Administration > Shift Management**.
   The Shift Management page opens.

2. View:

Field	Description
Shift Name	Name of the shift.
Status	The current status of the shift. It can be either ACTIVE or INACTIVE.
Effective From	The date from which shift-based data is collected by SHR.

Field	Description
Expires On	The date when the shift will expire. If a shift is configured to not expire, "Do Not Expire" is displayed.

Create a new time shift

1. In the Administration Console, click **Administration > Shift Management**.
   The Shift Management page opens.

2. To create a new shift, click **Create New Shift**.
   The Create New Shift box opens.

3. Type:

Field	Description
Shift Name	Name of the shift that you want to create such as prime, swing, or graveyard.
Effective From	Select the date from when you want the shift to be implemented.
Expires On	Select the date when the shift should expire.
Do Not Expire	Select this check box if you do not want the shift to expire. If you select this option, the shift will remain active until you manually expire it.
Shift Day	Select the day that you want to include in your shift period.
Start Time	The starting time of the shift. The value must in 24-hour format. The range of the start time is 0 to 23 hours.
End Time	The ending time of the shift. The value must in 24-hour format. The range of the end time is 1 to 24 hours.

4. To add additional days to the shift, click **Add New Row**.

5. Click **Save**.
   The newly create shift appears in the Shift Management table.

Modify the time shift

A shift includes all the time ranges that you defined for that shift. To modify the shift, you need to modify the time ranges in that shift or you can add new time ranges to that shift.

To modify the shift:

1. In the Administration Console, click **Administration > Shift Management**.
   The Shift Management page opens.

2. In the **Shift Name** column, click the shift that you want to modify.
   The Edit Shift box opens.

3. To edit a shift, you can:
   - Change the day in the Shift Day column.

   - Change the start and end times of the shift.

   - Click **Add New Row** to add a new shift day.

   - Click the 🗑 icon to remove a shift day.

   > **Note:** You cannot change the shift name or the Effective from date. These field are disabled by default. If the shift is modified, data that is already collected by SHR will not be reprocessed.

4. Click **Save** to save the changes.

Expire a time shift

Once a time shift is created, SHR does not allow you to delete it. This is because the data collected and aggregated based on that shift period can be used for data analysis purposes. This data remains in the SHR database. However, if you no longer require the time shift, you can disable it by expiring it. Once expired, SHR does not collect any data for that shift period.

To expire a shift:

1. In the Administration Console, click **Administration > Shift Management**.
   The Shift Management page opens.

2. In the **Shift Name** column, click the shift that you want to expire.
   The Edit Shift box opens.

3. Click **Expire Shift** to expire the shift.

4. In the confirmation message box, click **Yes**.

   > **Note:** If the shift is modified, data that is already collected by SHR will not be reprocessed.

Configuring custom groups

Custom groups in SHR help to retrieve information pertaining to the set of nodes that comprise a specific dimension. Custom groups in SHR can be created for conformed dimensions only. For instance, if you wish to view the nodes that are linked to a specific network, you can create a custom group that displays information pertaining only to the nodes that are a part of the specific network. Custom groups are created as an XML and imported to SHR through the platform stream.

To create a Custom Group:

1. Create an XML for the Custom Group. For syntax on creating the Custom Group XML, see Creating Custom Groups.

2. After creating the XML, save it in the **%PMDB_HOME%/config** folder.

After you create the Custom Group:

- The Custom Group is processed by the PMDB Platform stream **PMDB_ Platform@CustomGroup**.

- To confirm whether the Custom Group is imported to SHR, check whether the PMDB_ Platform@CustomGroup stream is loaded successfully.

- You must wait for the SHR dimension stream to populate the SHR data tables with the Custom Group information.

SHR enables you to:

- Create multiple custom groups for an operating system in a single XML file, by changing the values of the syntax.

- Select the desired custom group from the **Prompts** section of the reports.

Creating custom group

To create a Custom Group, copy the following syntax in an XML file:

> **Note:** You can enter a file name of your choice for the XML file, but follow the **<name>customgroup.xml** restriction; where, *<name>* is any file string supported by the operating system.
>
> For example, shr_customgroup.xml or SHR9XXcustomgroup.xml and so on.

```
<groups>

<group name=" " type=" ">

<instances type=" ">

<instance>

<attribute name=" " value=" " operator=" " relation=" " />

</instance>

</instances>

</group>

</groups>
```

> **Note:** Copy the attribute tag for each entity type that you want to define for the Custom Group.

The following table provides a description of the tags used in the above example.

Field	Description
group name	New Custom Group name.
type	The Group type.
instances type	Dimension table conformed to the K_CI table. The dimensions are extracted from this table.
attribute name	Name of the string column (not numeric column) in the dimension table defined in the *<instance type>* tag.
value	The column value in the dimension table must match this value.
operator	Operator for searching the node name value.
	To perform an exact match of values, use the EQUALS operator. For example, `"abcvalue1"`
	To perform a pattern based match of values, use the LIKE operator. You can specify the value as `"abcvalue1%"` or `"%abcvalue1%"` and so on.
	For other operators such as IN, NOT IN, NOT LIKE, EXISTS, "=", or "!=", you must specify the values enclosed within double quotes. For example, the IN operator must have the values as `"'abcvalue1','abcvalue2','abcvalue3'"`.
	Note: All the value comparisons in the XML against the SHR database is case insensitive.
relation	Determines the relation between the attribute name and value. The relation value can either be AND or OR.
	Note: If you do not define a relation value, SHR considers the default value as AND.

For examples of Custom Group syntax, see:

Custom Groups in Windows ® and Linux operating systems

```
<groups>

<group name="Windows" type="CUSTOMGROUP">

<instances type="K_CI_System">

<instance>

<attribute name="OS" value="NT" operator="LIKE" relation="OR" />
```

```
<attribute name="OS" value="Windows" operator="LIKE" relation="OR" />

<attribute name="OS" value="windows" operator="LIKE" relation="OR" />

<attribute name="OS" value="Win" operator="LIKE" relation="OR" />

<attribute name="OS" value="win" />

</instance>

</instances>

</group>

</groups>
```

Custom Groups in UNIX Operating System

```
<groups>

<group name="Unix" type="CUSTOMGROUP">

<instances type="K_CI_System">

<instance>

<attribute name="OS" value="%ux%" operator="LIKE" relation="OR" />

<attribute name="OS" value="%UX%" operator="LIKE" relation="OR" />

<attribute name="OS" value="AIX" operator="LIKE" relation="OR" />

<attribute name="OS" value="Sun%" operator="LIKE" />

</instance>

</instances>

</group>

</groups>
```

Managing dimensions

When a data source is configured in SHR, it collects dimension and fact data from the nodes (host, network device, application, and so on) for generating reports. Dimension data is collected from the topology source. But, when you remove a node or CI from your environment, it is not removed from the SHR database. This is meant to enable you to generate historical reports on deleted dimensions.

Inactive dimension: When a node is deleted from your environment and you continue to have an inactive dimension in the SHR database.

Duplicate dimension: When a new node is added to the environment with the name of an older node, you have a duplicate dimension in the SHR database.

When you have retired nodes or CIs permanently from your environment and no longer generate reports on them, you can delete the inactive dimensions. You can do it for both local and conformed dimensions from the SHR system using the Command Line Interface (CLI).

If you have added new nodes and they have taken up the names of older nodes, you can rename the duplicate dimensions. You can do it for only conformed dimensions from the SHR system using the Command Line Interface (CLI).

> **Note:** When you delete a dimension, the dimension and its fact data is deleted permanently. Take a backup of the SHR database before you perform this operation. For more information on database back up, refer *Database backup and Recovery* chapter in the *HP Service Health Reporter Configuration Guide*.

For more information on fact, dimension, and types of dimensions, see the section, "*Architecture*" in the *HP Service Health Reporter Concepts Guide*.

To view the CLI Help that lists the commands you can use, run the following command:

`dimensionManager -help`

Before running the commands in this section, stop the *HP_PMDB _Platform_Timer* service (Windows) or the *TrendTimer* service (Linux).

Managing inactive dimensions

You can identify the dimensions that have remained inactive for a certain period in the SHR database and delete them.

List inactive dimensions

To generate a list of inactive dimensions, run the following command:

`dimensionManager –inactive_dim_list -caption <caption name> -inactive <number of days inactive> -output_dir <directory location>`

For details on the command parameters, see "Inactive Dimension Parameters" on the next page

Delete inactive dimensions

To delete inactive dimensions, run the following command:

`dimensionManager -inactive_dim_delete -caption <caption name> -file <input file> -mode <test/commit>`

For details on the command parameters, see "Inactive Dimension Parameters" on the next page

> **Caution:** When you execute this command in the commit mode, the dimension and its fact data will be deleted permanently. Take a backup of the SHR database before you perform this operation. For more information on database back up, refer *Database backup and Recovery*

chapter in the *HP Service Health Reporter Configuration Guide*

The following table provides a description of the parameters used in the preceding commands:

Inactive Dimension Parameters

Parameter	Description
inactive_dim_list	Operation for listing the inactive dimensions.
inactive_dim_delete	Operation for deleting inactive dimensions.
caption	Caption name or table name for a dimension. Obtain it from the model interface document available with each content pack in their respective */doc* folder. **Example**: "K_CI_System" or "System".
file	Absolute path of the input CSV file that lists the inactive dimensions to be deleted.
inactive	Number of days for which data does not exist for the dimension. **Example**: 180
output_dir	Directory location of the output CSV file that lists inactive dimensions. **Example**: Directory location:*{PMDB_HOME}\DLC* CSV file: `<dimension_table_name>_0_*.csv`
mode	Mode of the operation [test/commit]. Use the test (default) mode to review the data that will be modified or deleted. Execute the commit mode to permanently apply the changes to the SHR database. You should use the test mode and review the affected files before you perform the commit operation.

Managing duplicate dimensions

When a new node is added to the environment with the name of an older node, you have a duplicate dimension in the SHR database. You can list out duplicate entries and delete them or rename them. The Configuration Item (CI) with the latest time-stamp is considered the original dimension and the earlier entries are considered duplicate dimensions. This feature is supported only on conformed dimensions.

List duplicate dimensions

To generate a list of duplicate dimensions, run the following command:

```
dimensionManager –duplicate_dim_list -caption <caption name> -file <input file>
```

For details on the command parameters, see "Duplicate Dimension Parameters" below.

Delete duplicate dimensions

To delete duplicate dimensions, run the following command:

```
dimensionManager -duplicate_dim_delete -caption <caption name> -file <input file> -
mode <test/commit>
```

For details on the command parameters, see "Duplicate Dimension Parameters" below.

> **Caution:** When you execute this command in the commit mode, the dimension and its fact data
> will be deleted permanently. Take a backup of the SHR database before you perform this
> operation. For more information on database back up, refer *Database backup and Recovery*
> chapter in the *HP Service Health Reporter Configuration Guide*

The following table provides a description of the parameters used in the preceding commands:

Duplicate Dimension Parameters

Parameter	Description
duplicate_dim_list	Operation for listing duplicate dimensions.
duplicate_dim_delete	Operation for deleting duplicate dimensions.
caption	Caption name or table name for a dimension. Obtain it from the model interface document available with each content pack. **Example**: "K_CI_System" or "System".
file	Delete or remove duplicate dimension: Absolute path of the input CSV file that lists the duplicate dimensions to be deleted or renamed.
mode	Mode of the operation [test/commit]. Use the test (default) mode to review changes to your reports. Execute the commit mode to permanently apply the changes to the SHR database. You should use the test mode and review the affected files before you perform the commit operation.

Managing dimensions using business key

To list the business keys (CI_UID) of a conformed dimension, run the following command:

```
dimensionManager -dim_list -business_keys all -caption <caption name> -output_dir
<directory location>
```

To delete business keys (CI_UID) based on your requirement, run the following command:

```
dimensionManager -dim_delete -caption <caption name> -file <input file> -mode
<test/commit>
```

To modify the business key (CI_UID) of the duplicate or older dimensions, run the following command:

```
dimensionManager -rename_key -caption <caption name> -file <input file>
```

The format of the `input file` for rename option is `caption name_0_timestamp.csv`.

Dimension Parameters

Parameter	Description
dim_list	Operation for listing dimensions.
dim_delete	Operation for deleting dimensions.
business_keys	Comma separated values/patterns (only '*' wildcard is supported) for listing business keys. Use '-business_keys all' to list all the business keys (CI_UID).
rename_key	Operation for renaming the old value of business key (CI_UID) with new value.
caption	Caption name or table name for a dimension. Obtain it from the model interface document available with each content pack. **Example**: "K_CI_System" or "System".
file	Absolute path of the input CSV file that lists the business keys to be deleted or renamed.
output_dir	Directory location of the output CSV file. **Example**: *C:\DLC*
mode	Mode of the operation [test/commit]. Use the test (default) mode to review changes to your reports. Execute the commit mode to permanently apply the changes to the SHR database.

Managing dimensions using natural key

To list the natural keys of a conformed dimension, run the following command:

```
dimensionManager -dim_list -natural_keys all -caption <caption name> -output_dir
<directory location>
```

To delete natural keys based on your requirement, run the following command:

```
dimensionManager -dim_delete -caption <caption name> -file <input file> -mode
<test/commit>
```

To modify the natural key of the duplicate or older dimensions, run the following command:

```
dimensionManager -rename -caption <caption name> -file <input file>
```

The format of the `input file` for rename option is `caption name_0_timestamp.csv`.

The following table provides a description of the parameters used in the preceding commands:

Dimension Parameters

Parameter	Description
dim_list	Operation for listing dimensions.
dim_delete	Operation for deleting dimensions.
natural_keys	Comma separated values/patterns (only '*' wildcard is supported) for listing natural keys. Use '-natural_keys all' to list all the natural keys.
rename	Operation for renaming the old value of natural key with new value.
caption	Caption name or table name for a dimension. Obtain it from the model interface document available with each content pack. **Example**: "K_CI_System" or "System".
file	Absolute path of the input CSV file that lists the natural keys to be deleted or renamed.
output_dir	Directory location of the output CSV file. **Example**: *C:\DLC*
mode	Mode of the operation [test/commit]. Use the test (default) mode to review changes to your reports. Execute the commit mode to permanently apply the changes to the SHR database.

Managing inactive or duplicate dimensions in data source

You can list and delete the dimensions that have remained inactive for a certain period in the Run-time Service Model (RTSM) data source from which SHR gathers data.

List inactive dimensions in data source

To generate a list of inactive dimensions in the RTSM data source, run the following command:

```
dimensionManager –check_datasource -list_inactive -output_dir <directory location>
```

For details on the command parameters, see "Check data source dimension parameters" on the next page

List duplicate dimensions in data source

To generate a list of duplicate dimensions in the RTSM data source, run the following command:

```
dimensionManager –check_datasource -list_duplicate -output_dir <directory location>
```

For details on the command parameters, see "Check data source dimension parameters" below

The following table provides a description of the parameters used in the preceding commands:

Check data source dimension parameters

Parameter	Description
list_inactive	Operation for listing the inactive dimensions in data source.
list_duplicate	Operation for listing duplicate dimensions in data source.
check_datasource	Operation for verifying dimensions in the RTSM data source.
output_dir	Directory location of the output CSV file that lists inactive dimensions. **Example**: Directory location:*{PMDB_HOME}\DLC* CSV file: `<dimension_table_name>_0_*.csv`

Configuring downtime in reports

Downtime refers to periods when a system, network, or application is not available to the user because of known or unknown reasons. Downtime is important for calculating the availability of a system, application, or network, which is typically expressed as the percentage of uptime in a given period. When using SHR to generate service-level agreement (SLA)-based reports, there is a need to exclude the predefined downtime to provide accurate availability information. This is because downtime can skew the CI data in the reports.

In SHR, there are two types of downtime:

- **Planned downtime**: This refers to the scheduled periods of time where the system or network is brought down to run maintenance job such as running a backup, or patching software, or performing a system reboot. Planned downtime is a result of logical, management-initiated event.

- **Excused downtime**: This refers to the unscheduled periods of time when the system is not available because of some physical event, such as hardware or software failure or a power outage.

Downtimes are configured based on associated CIs. For example, you might want to exclude a recurring maintenance event or a holiday for a specific host CI whose physical host you know will be down for that period of time.

SHR enables you to:

- Configure the downtime to occur once or to recur weekly or monthly.

- Select multiple CIs to be affected by the downtime.

The downtime information is defined for each CI in an XML file, where you must manually specify the downtime period, the duration, and the specific instances of the CIs. SHR uses this XML file to update the collected fact data with the downtime information before loading the data into the database.

The downtime period is marked on the "As-polled" data or "5-minute" data only. When this data is summarized for the hourly table and upwards, the downtime period is excluded from it. SHR OOTB Availability reports display the overall uptime and downtime of the node in your environment over a period of time.

The following table tells you what content packs downtime applies to:

Content Pack	Yes/No
Real User Monitor	No (SHR obtains downtime data from the data source; provision downtime at the source)
Business Process Monitor	No (SHR obtains downtime data from the data source; provision downtime at the source)
Service Health	No (SHR obtains downtime data from the data source; provision downtime at the source)
IBM WebSphere Application Server	Yes
Microsoft Active Directory	No (SHR obtains downtime data from the data source; provision downtime at the source)
Microsoft Exchange	Yes
Microsoft SQL Server	Yes
Oracle	Yes
Oracle WebLogic Server	Yes
Network	No (SHR obtains downtime data from the data source; provision downtime at the source)
HP Operations Manager	No (SHR obtains downtime data from the data source; provision downtime at the source)
OMi	No (SHR obtains downtime data from the data source; provision downtime at the source)
System Management	Yes
Virtualization	Yes

Create the downtime XML file

You can provide the downtime information at any time after installing the Content Packs. To provide downtime information to SHR, following these steps:

1. Depending on the deployment scenario, identify the CIs or managed nodes that are going to be affected by downtime.

2. Get the CI details from the Model Automation XSD file. For more information, see the *SHR Content Development Guide*.

3. Decide whether the downtime will occur once or recur at a weekly or monthly basis.

4. Based on the recurrence, create a downtime schedule XML file using any one of the following examples:

   ■ Downtime schedule with one occurrence

   ■ Weekly downtime schedule

   ■ Monthly downtime schedule

5. After creating the XML file, place the file in the C:\HP-SHR\PMDB\data\downtime folder.

After the files are placed in the downtime folder, the data processing in SHR handles the downtime enrichment on the collected data. The enriched data is aggregated and stored in the database for reporting purposes. You can monitor the downtime enrichment on the Internal Monitoring > Data Processing page, which displays the downtime stream details for a particular Content Pack.

Syntax for downtime schedule with one occurrence

To create a downtime schedule that occurs only once, you can use one of the following XML syntax:

Syntax 1

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<downtime>

    <name>Sample1</name>

    <category>Other</category>

    <schedule >

      <type>ONCE</type>

      <startDate>2012-02-07 10:00:00</startDate>

      <endDate>2012-02-07 22:00:00</endDate>

    </schedule>

    <instances type="system">

      <instance>

            <attribute name="CI_UID"
            value="c2fa6553dd16af591b128e19feec3d49"/>

      </instance>
```

```
        </instances>

    </downtime>
```

Syntax 2

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<downtime>

    <name>Sample1</name>

    <category>Application maintenance</category>

    <schedule >

      <type>ONCE</type>

      <startDate>2012-02-07 10:00:00</startDate>

      <endDate>2012-02-07 22:00:00</endDate>

    </schedule>

    <selectedCIs>

      <ci>

            <id>ciid_bizsvc1</id>

      </ci>

      <ci>

            <id>ciid_bizsvc2</id>

      </ci>

    </selectedCIs>

    </downtime>
```

The following table provides a description of the tags used in the above sample.

Tag	Description
<name>	Provide a name for the downtime in the tag.

Tag	Description
`<category>`	The category assigned to the downtime. Options include: • Application installation • Application maintenance • Hardware installation • Hardware maintenance • Network maintenance • Operating system reconfiguration • Other • Security issue
`<schedule>`	Define the downtime schedule in this section of the XML.
`<type>`	Define the type of downtime schedule that you want to create. The values can be ONCE, WEEKLY, or MONTHLY.
`<startDate>`	Specify the starting date and time of the scheduled downtime for the monitored component or CI. The date format is yyyy-mm-dd hh:mm:sis. You can change this value at any time. However, data that is enriched with downtime information will not be reprocessed.
`<endDate>`	Specify the ending date and time of the scheduled downtime for the CI. The date format is yyyy-mm-dd hh:mm:ss. You can change this value at any time. However, data that is enriched with downtime information will not be reprocessed.
`<instances type>`	In this section, you define the CI type that will be affected by downtime such as node, CPU, Disk, Web server, application, event, and so on. The downtime XML that you create is applicable for one CI type only. For additional CIs, you must create additional XML files.
`<instance>`	Each instance of the CI type must be defined in a separate <instance> tag. The attribute name refers to the instance metric and the value refers to the value of that metric. If a particular CI instance is defined by more than one metric, additional instances must also be defined by the same number and type of metrics. For the CI parameters, see the Model Automation XSD.

Tag	Description
`<selectedCIs>`	In this section, you can directly define multiple CIs that will be affected by downtime. You can refer to these CIs by using their unique IDs. This section is applicable if SHR is deployed in the SaOB and APM deployment scenarios where RTSM is the topology source.

Syntax for weekly downtime schedule

To create a downtime schedule that occurs on a weekly basis, you can use one of the following XML syntax:

Syntax 1

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<downtime>

    <name>Sample2</name>

    <category>Other</category>

    <schedule >

      <type>WEEKLY</type>

      <days>

            <selectedDays>SUNDAY</selectedDays>

            <selectedDays>MONDAY</selectedDays>

            <selectedDays>TUESDAY</selectedDays>

            <selectedDays>WEDNESDAY</selectedDays>

      </days>

      <startTimeInSecs> 57600</startTimeInSecs>

      <durationInSecs> 10800</durationInSecs>

      <validFrom>2012-02-02 12:00:00</validFrom>

      <validTo>2012-03-10 12:00:00</validTo>

    </schedule>

    <instances type="CPU">

      <instance>
```

```
                <attribute name="CI_UID"
                value="c2fa6553dd16af591b128e19feec3d49"/>

        </instance>

        <instance>

                <attribute name="CI_UID"
                value="b1ta83456aa13rf352h908e19teec3d49"/>

        </instance>

    </instances>

</downtime>
```

Syntax 2

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<downtime>

    <name>Sample2</name>

    <category>Other</category>

    <schedule >

      <type>WEEKLY</type>

      <days>

            <selectedDays>SUNDAY</selectedDays>

      </days>

      <startTimeInSecs> 57600</startTimeInSecs>

      <durationInSecs> 10800</durationInSecs>

      <validFrom>2012-02-02 12:00:00</validFrom>

      <validTo>2012-03-10 12:00:00</validTo>

    </schedule>

    <selectedCIs>

      <ci>

            <id>ciid_bizsvc1</id>

      </ci>

      <ci>
```

```
            <id>ciid_bizsvc2</id>

       </ci>

</selectedCIs>

</downtime>
```

The following table provides a description of the tags used in the above sample.

Tag	Description
`<name>`	Provide a name for the downtime in the tag.
`<category>`	The category assigned to the downtime. Options include: • Application installation • Application maintenance • Hardware installation • Hardware maintenance • Network maintenance • Operating system reconfiguration • Other • Security issue
`<schedule>`	Define the downtime schedule in this section of the XML.
`<type>`	Define the type of downtime schedule that you want to create. The values can be ONCE, WEEKLY, or MONTHLY.
`<days>`	Specify the days of the week when downtime for the CI type is planned for in this section.
`<startTimeInSecs>`	Specify the starting time of the scheduled downtime in seconds. For example, 57600 seconds equals to 16:00, which means that the downtime is scheduled to start at 4 P.M. on each day that is defined in the `<days>` tag.
`<durationInSecs>`	Specify the duration of the downtime in seconds. For example, 10800 seconds equals to 3 hours, which means that the downtime period lasts for 3 hours from 4 P.M. to 7 P.M.

Tag	Description
`<validFrom>`	Specify the starting date and time when SHR must start collecting the downtime information for data enrichment. The date format is yyyy-mm-dd hh:mm:ss.
`<validTo>`	Specify the ending date and time when SHR must stop collecting the downtime information for data enrichment. The date format is yyyy-mm-dd hh:mm:ss.
`<instances type>`	In this section, you define the CI type that will be affected by downtime such as node, CPU, Disk, Web server, application, event, and so on. The downtime XML that you create is applicable for one CI type only. For additional CIs, you must create additional XML files.
`<instance>`	Each instance of the CI type must be defined in a separate <instance> tag. The attribute name refers to the instance metric and the value refers to the value of that metric. If a particular CI instance is defined by more than one metric, additional instances must also be defined by the same number and type of metrics. For the CI parameters, see the Model Automation XSD.
`<selectedCIs>`	In this section, you can directly define multiple CIs that will be affected by downtime. You can refer to these CIs by using their unique IDs. This section is applicable if SHR is deployed in the SaOB and APM deployment scenarios where RTSM is the topology source.

Syntax for monthly downtime schedule

To create a downtime schedule that occurs on a monthly basis, you can use one of the following XML syntax:

Syntax 1

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<downtime>

    <name>Sample3</name>

    <category>Other</category>

    <schedule >

      <type>MONTHLY</type>

      <days>

            <selectedDays>4</selectedDays>
```

```
            <selectedDays>8</selectedDays>

      </days>

      <startTimeInSecs>57600</startTimeInSecs>

      <durationInSecs>10800</durationInSecs>

      <validFrom>2012-02-02 12:00:00</validFrom>

      <validTo>2012-03-10 12:00:00</validTo>

   </schedule>

   <instances type="CPU">

      <instance>

            <attribute name="CI_UID"
            value="c2fa6553dd16af591b128e19feec3d49"/>

      </instance>

   </instances>

</downtime>
```

Syntax 2

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<downtime>

   <name>Sample3</name>

   <category>Other</category>

   <schedule >

      <type>MONTHLY</type>

      <days>

            <selectedDays>4</selectedDays>

            <selectedDays>8</selectedDays>

      </days>

      <startTimeInSecs>57600</startTimeInSecs>

      <durationInSecs>10800</durationInSecs>

      <validFrom>2012-02-02 12:00:00</validFrom>

      <validTo>2012-03-10 12:00:00</validTo>
```

```
    </schedule>

    <selectedCIs>

      <ci>

          <id>ciid_bizsvc1</id>

      </ci>

      <ci>

          <id>ciid_bizsvc2</id>

      </ci>

    </selectedCIs>

</downtime>
```

The following table provides a description of the tags used in the above sample.

Tag	Description
`<name>`	Provide a name for the downtime in the tag.
`<category>`	The category assigned to the downtime. Options include: • Application installation • Application maintenance • Hardware installation • Hardware maintenance • Network maintenance • Operating system reconfiguration • Other • Security issue
`<schedule>`	Define the downtime schedule in this section of the XML.
`<type>`	Define the type of downtime schedule that you want to create. The values can be ONCE, WEEKLY, or MONTHLY.

Tag	Description
`<days>`	Specify the days of the month when downtime for the CI type is planned for in this section. For example, 4 and 8 refers to the 4th and 8th day of the month when the downtime for the particular CI is planned.
`<startTimeInSecs>`	Specify the starting of the scheduled downtime in seconds. For example, 57600 seconds equals to 16:00, which means that the downtime is scheduled to start at 4 P.M. each day that is defined in the <days> tag.
`<durationInSecs>`	Specify the duration of the downtime in seconds. For example, 10800 seconds equals to 3 hours, which means that the downtime period lasts for 3 hours from 4 P.M. to 7 P.M.
`<validFrom>`	Specify the starting date and time when SHR must start collecting the downtime information for data enrichment. The date format is yyyy-mm-dd hh:mm:ss.
`<validTo>`	Specify the ending date and time when SHR must stop collecting the downtime information for data enrichment. The date format is yyyy-mm-dd hh:mm:ss.
`<instances type>`	In this section, you define the CI type that will be affected by downtime such as node, CPU, Disk, Web server, application, event, and so on. The downtime XML that you create is applicable for one CI type only. For additional CIs, you must create additional XML files.
`<instance>`	Each instance of the CI type must be defined in a separate <instance> tag. The attribute name refers to the instance metric and the value refers to the value of that metric. If a particular CI instance is defined by more than one metric, additional instances must also be defined by the same number and type of metrics. For the CI parameters, see the Model Automation XSD.
`<selectedCIs>`	In this section, you can directly define multiple CIs that will be affected by downtime. You can refer to these CIs by using their unique IDs. This section is applicable if SHR is deployed in the SaOB and APM deployment scenarios where RTSM is the topology source.

Configuring downtime in the past

Past downtime in SHR can be configured by performing the following steps:

1. Log on to the system as an administrator.

2. Configure downtime under the **%pmdb_home%/data/downtime** folder. To configure the downtime, see "Configuring downtime in reports" on page 140

3. Click **Start** > **Run** > type **cmd**. The command prompt window opens.

4. Type downtime to populate the CIs that are associated with the downtime streams.

Past downtime for all the streams in SHR can be processed as follows:

1. Click **Start** > **Run** > type **cmd**. The command prompt window opens.

2. Type downtimeutility to process all the downtime streams as shown below.

```
C:\Users\Administrator>downtimeutility
PID:28108
Started processing all the streams...
Processing downtime streams, please wait for some time...
in executer
Waiting for all running streams to complete there job
Aborting all ABC streams...
Aborted all ABC streams...
Running ABCBatch load (loading all streams)..
Finished loading streams..
Running streams..
Starting Timer service..
in executer
Successfully processed all the streams...
```

Processing past downtime for all the streams is time consuming. If you wish to process past downtime for a single stream perform the following steps:

1. Log on to the Administration Console.

2. Go to **Home Page**, click **PMDB Platform** under the **Content Pack Component Name** for the list of streams that are configured in SHR.

3. Select the Stream ID of the specific stream for which you wish to process past downtime.

4. Click **Start** > **Run** > type **cmd**. The command prompt window opens.

5. Type downtimeutility -streamid *<stream ID>*

6. This processes the past downtime only for the specific stream and the associated CI.

Note: Processing past downtime stops the **HP_PMDB_Platform_Timer** service. Reprocessing of the streams is started after processing the streams that are currently running. The **HP_PMDB_Platform_ Timer** service is automatically restarted after reprocessing the streams.

Past Downtime is automatically configured for a period of 7 days. To change this value, perform the following steps:

1. Open the file **config.prp** present in the **%pmdb_home%/data folder**.

2. Change the value assigned to the field **downtimedays**. The default number of days is 7.

Configuring customer in reports

If you are a Managed Service Provider (MSP) using SHR, you can generate reports per customer or aggregate data per customer by:

1. Provisioning customers and customer-dimension associations in an XML file.

2. Creating custom reports using the Customer Name object in the SAP BusinessObjects Universe.

You can associate only conformed dimensions [Configuration Items (CIs)] to customers. You can configure multiple customers in a single XML file which is processed periodically. Newer dimensions that meet the conditions defined in the XML file are automatically associated to the customer.

To provision customers and associate them with dimensions in SHR:

1. Create an XML file with the name of the customer and associate it with the appropriate dimensions. For the syntax of this XML file, see Creating customer XML.

2. Save the XML file in the **PMDB_HOME/config** folder.

3. Wait for a few minutes and verify if the **PMDB_Platform@CustomerEnrichment** stream has run successfully. This stream processes the XML and creates CSV files that SHR consumes for generating reports.

To generate reports grouped by customers you configured,use the Customer Name object from the SAP BusinessObjects Universe. You can enhance out-of-the-box (OOTB) reports or create new reports.

> **Note:** You must make a copy of the OOTB reports when you modify them.

Creating Customer XML

To provision customers, copy the following syntax in an XML file:

> **Note:** You can enter a file name of your choice for the XML file, but follow the *<name>***customerenrich.xml** restriction; where, *<name>* is any file string supported by the operating system.
>
> For example, shr_customerenrich.xml or SHR9XXcustomerenrich.xml and so on.

```
<customers>
```

```
<customer name="">

<Address1></Address1>

<Address2></Address2>

<City></City>

<State></State>

<Zipcode></Zipcode>

<Phonenumber></Phonenumber>

<Description></Description>

<instances type="">

<instance>

<attribute name="" value="" operator="" relation=""/>

<attribute name="" value="" operator=""/>

</instance>

</instances>

</customer>

</customers>
```

The following table provides a description of the attribute tags used in the above syntax.

Field	Description
<customer name>	Enter name of a customer. Entering a value in this field is mandatory.
<address1>	Enter address here. (Optional)
<address2>	Enter address here. (Optional)
<city>	Enter the name of a city here. (Optional)
<state>	Enter the name of a state here. (Optional)
<zipcode>	Enter the zipcode here; only numbers are allowed. (Optional)
<phonenumber>	Enter the phone number here; only numbers are allowed. (Optional)
<description>	Enter a description of your choice. (Optional)
<instances type>	Dimension table name conformed to the K_CI table. See the model interface document available with each content pack in their respective /doc folder to fetch the list of dimensions. The dimensions are extracted from this table.
<attribute name>	Name of the string column (not numeric column) in the dimension table defined in the <instance type> tag.

Field	Description
<value>	The column value in the dimension table must match this value.
<operator>	Operator for searching the node name value. To perform an exact match of values, use the EQUALS operator. For example, `"abcvalue1"` To perform a pattern based match of values, use the LIKE operator. You can specify the value as `"abcvalue1%"` or `"%abcvalue1%"` and so on. For other operators such as IN, NOT IN, NOT LIKE, EXISTS, "=", or "!=", you must specify the values enclosed within double quotes. For example, the IN operator must have the values as `"'abcvalue1','abcvalue2','abcvalue3'"`. **Note:** All the value comparisons in the XML against the SHR database is case insensitive.
<relation>	Determines if the AND or OR operation must be performed when multiple attribute-value pairs are specified. If you do not define a relation value, SHR considers the default value as AND.

Applicable Content Packs

You can associate customers to conformed dimensions in the following content packs:

- Cross-Domain Operations Events

- IBM WebSphere Application Server

- Microsoft Active Directory

- Microsoft Exchange Server

- Microsoft SQL Server

- Network Performance

- Oracle

- Oracle WebLogic Server

- System Performance

- Virtualization Infrastructure Management

The customer information is available from the data source for the following content packs:

- Real User Transaction Monitoring

- Health and Key Performance Indicators

- Synthetic Transaction Monitoring

The customer information is not available in the Operations Events content pack.

Customer XML Example

```
<customers>

<customer name="Hewlett-Packard Company">

<Address1>3000 Hanover Street</Address1>

<Address2></Address2>

<City>Palo Alto</City>

<State>California</State>

<ZipCode>94304</ZipCode>

<PhoneNumber>16508571501</PhoneNumber>

<Description></Description>

<instances type="K_CI_Oracle">

<instance>

<attribute name="CI_UID" value="8c5e2d0fd63a0b0bd66d6e" operator="EQUALS"
relation="OR" />

<attribute name="CI_UID" value="3f5a2d0fd64a0b0wg66d6e" operator="EQUALS"
relation="OR" />

<attribute name="CI_UID" value="98cd49a3e850a455788286" operator="EQUALS" />

</instance>

</instances>

</customer>

</customers>
```

Configuring location in reports

You can use SHR to generate reports on infrastructure and applications based on their geographical location.

To generate reports grouped by location, you must associate dimensions with location information as follows:

1. Create an XML file, enter location details, and associate dimensions to the location. For the syntax of this XML file, see Creating location XML.

2. Save the XML file in the **PMDB_HOME/config** folder.

3. Wait for a few minutes and verify if the **PMDB_Platform@platform_poller_registry_build** stream has run successfully. This stream processes the XML and creates CSV files that SHR consumes for generating reports.

You can associate only conformed dimensions [Configuration Items (CIs)] to locations. Newer dimensions that meet the conditions defined in the XML file are automatically associated to the location.

Creating Location XML

To create a location record, copy the following syntax in an XML file:

Note: You can enter a file name of your choice for the XML file, but follow the **<name>locationenrich.xml** restriction; where, *<name>* is any file string supported by the operating system.

For example, shr_locationenrich.xml or SHR9XXlocationenrich.xml and so on.

```
<locations>

<location name="">

<country></country>

<state ></state>

<city></city>

<region></region>

<address></address>

<building></building>

<floor></floor>

<instances type=" ">

<instance>

<attribute name="" value="" operator="" relation=""/>

<attribute name="" value="" operator="" />

</instance>

</instances>

</location>

</locations>
```

The following table provides a description of the tags used in the above example:

Field	Description
<location name>	Enter name of the location. Entering a value in this field is mandatory.
<country>	Enter the name of a country here. (Optional)
<state>	Enter the name of a state here. (Optional)
<city>	Enter the name of a city here. (Optional)
<region>	Enter the name of a region here. Entering a value in this field is mandatory.
<address>	Enter address here. (Optional)
<building>	Enter the name of a building here. (Optional)
<floor>	Enter the floor here. (Optional)
<instances type>	Dimension table name conformed to the K_CI table. See the model interface document available with each content pack in their respective */doc* folder to fetch the list of dimensions. The dimensions are extracted from this table.
<attribute name>	Name of the string column (not numeric column) in the dimension table defined in the *<instance type>* tag.
<value>	Value of the column in the dimension table for which you create the location, such as values in the column "node_name"of the "K_CI_Oracle" dimension table. Or, values in the column "dns_name" of the "K_CI_System" dimension table, and so on.
< operator>	Operator for searching the node name value. To perform an exact match of values, use the EQUALS operator. For example, `"abcvalue1"` To perform a pattern based match of values, use the LIKE operator. You can specify the value as `"abcvalue1%"` or `"%abcvalue1%"` and so on. For other operators such as IN, NOT IN, NOT LIKE, EXISTS, "=", or "!=", you must specify the values enclosed within double quotes. For example, the IN operator must have the values as `"'abcvalue1','abcvalue2','abcvalue3'"`. **Note:** All the value comparisons in the XML against the SHR database is case insensitive.
<relation>	Determines if the AND or OR operation must be performed when multiple attribute-value pairs are specified. If you do not define a relation value, SHR considers the default value as AND.

Applicable Content Packs

You can associate location to conformed dimensions in the following content packs:

- IBM WebSphere Application Server

- Microsoft Active Directory

- Microsoft Exchange Server

- Microsoft SQL Server

- Oracle

- Oracle WebLogic Server

- System Performance

- Virtualization Infrastructure Management

The location information is available from the data source in the following content packs:

- Network Performance

- Real User Transaction Monitoring

- Synthetic Transaction Monitoring

The location information is not available in the following content packs:

- Operations Events

- Cross-Domain Operations Events

- Health and Key Performance Indicators

Location XML Example

```
<locations>
<location name="Santa Clara County">
<Country>USA</Country>
<State>California</State>
<City>Palo Alto</City>
<Region>San Francisco Bay Area</Region>
<3000 Hanover Street/>
<Building />
```

```
<Floor />

<instances type="K_CI_System">

<instance>

<attribute name="dns_name" value="abc%" operator="LIKE" relation="OR" />

<attribute name="dns_name" value="abc1" operator="EQUALS" relation="OR" />

<attribute name="dns_name" value="abc2%" operator="LIKE" />

</instance>

</instances>

<instances type="K_CI_SQLServer">

<instance>

<attribute name="database_dbsid" value="abc123" operator="EQUALS" />

</instance>

</instances>

</location>

</locations>
```

Managing Content Packs

SHR enables you to install and manage Content Packs with the help of the Deployment Manager utility, a web-based interface that is a part of the Administration Console.

The Deployment Manager simplifies the selection of the Content Packs by filtering them based on the topology source that you defined in the post-install configuration phase. From the filtered list, you can then select the Content Packs or specific Content Pack components that you want to install.

The Deployment Manager provides the following benefits:

- Gives you more control over how you want to install a Content Pack; whether it is the entire Content Pack or individual components.

- Displays the data source dependencies for each Content Pack

- Supports the installation of custom Content Pack and custom Content Pack components

- Provides a single, easy-to-use interface for installing and uninstalling Content Packs.

Using the Deployment Manager page, you can:

- Install a Content Pack

- Remove an Installed Content Pack

Install a Content Pack

1. In the Administration Console, click **Administration > Deployment Manager**.
   The Deployment Manager page opens. By default, all the Content Pack components that have not been installed are selected for installation.

2. To modify the selection of the Content Pack components, perform any one of the followings steps:
   - In the **Content** column, clear the Content for which you do not want to collect data.

   - In the **Data Source Application** column, clear the data sources from which you do not want SHR to collect data for the selected Content Pack. The corresponding Content Pack components will not be selected for installation.

   - In the **Content Pack Component Name** column, clear the components of the selected Content Pack that you do not want to install.

   - Click **Restore Default** if you want to go back to the default selection.

3. Click **Deploy** to install the Content Packs.
   An `Installation Started` status appears in the **Status** column for each Content Pack. The Deployment Manager page automatically refreshes itself to display the updated status. Once the installation completes, an `Installation Successful` status appears. If the installation fails, an `Installation Failed` status appears.

4. Click the link in the **Status** column for more information about the installation process.
   The Content Pack Component Status History window opens. It displays the details of the current and historical status of that Content Pack component's installation.

> **Note:** During the installation process, you cannot remove a Content Pack component that is already installed. Instead, you must wait till installation of the all the Content Pack components is complete before you can perform any other operations on the Deployment Manager page.

Remove an Installed Content Pack

1. In the Administration Console, click **Administration > Deployment Manager**.
   The Deployment Manager page opens.

2. In the **Remove** column for each Content Pack component, click the 🗑 icon to uninstall the component.
   The Content Pack Components Removal Summary dialog box opens. This dialog box lists the selected component and all the dependent components that will be uninstalled.

3. Click **OK** to confirm the removal of the selected Content Pack component.
   An `Uninstallation Started` status appears in the **Status** column for each Content Pack. The Deployment Manager page automatically refreshes itself to display the updated status

of the uninstallation. Once the uninstallation completes, an `Uninstallation Successful` or an `Uninstallation Successful with Warnings` status appears in the **Status** column. If the uninstallation fails, an `Uninstallation Failed` status appears.

4. Click the link in the **Status** column for more information about the uninstallation process. The Content Pack Component Status History window opens. It displays the details of the current and historical status of that Content Pack component's uninstallation.

Note: If the Status column displays either the `Uninstallation Successful with Warnings` or `Uninstallation Failed` status, you must uninstall the Content Pack component again for it to succeed.

Configuring a Collector Installed on a Remote System

To configure a collector that is installed on a remote system (and not on the SHR system), do the following:

1. In the Administration Console, click **Administration >Configure Collectors**

2. Click **Create New**, **Configuration Parameters** section opens

3. In the **Name** field write the display name of the collector

4. In the **Host name** field write the host name of the collector.

5. Click **Ok** and Click **Save** to complete the configuration.

.

Disabling a Collector Installed on a Remote System

To disable a collector that is installed on a remote system (and not on the SHR system), do the following:

1. .Uncheck the **Enable** field in the Collector Configuration

2. Click **Save** in the Collector Summary section.

Note : If a source is assigned to the collector, you will not be able to uncheck the **Enable** field ; it is required to ensure that no data source is assigned to the collector.

Administration Console Screens

This section lists the context-sensitive Help pages for the different Administration Console screens. These Help pages provide an overview of the screens that are present in the Administration Console.

You can directly launch these Help pages for a particular screen by clicking the 🔵 icon on the top-right corner of the screen.

The Administration Console screens include:

- Home

- Service Definition

- HP Operations agent

- Operations Manager

- Generic Database

- VMware vCenter Data Source

- SiteScope

- BSM/OMi

- System Configuration

- Licensing

- Security

- Data Processing

- SAP BOBJ

- Aging

- Services

- Shift Management

- Deployment Manager

- Collector Configuration

- Content

- Data Processing

- Database Monitoring

- Platform

- About

Home

The Home page is the main page of the Administration Console. This page gives you an overall view of the status of SHR, its associated services, the database, and the host platform. You can also view the status of the data collection, check the performance of the Content Packs, and view a list of ABC and database alerts generated by SHR.

The Home page includes:

Group	Field	Description
Status Summary	Services Status	This table displays the status of the SHR database and SAP BOBJ Enterprise services. Status of the service: • ⬆ indicates that all the services are running successfully. • ⬇ indicates that one or all of the services are not running. The data displayed in this table is refreshed periodically. Click ↻ to update the table with the latest data.
	Connectivity Status	The table displays the status of SHR's connectivity to the following components: • Tomcat service (SAP BOBJ Tomcat Service) • SAP BusinessObjects Central Management Service (SAP BOBJ CMS) • SHR database (HP PMDB Platform Sybase)
	SHR Server System	This panel displays the host name, disk space, memory utilization (graph), and CPU utilization (graph) of the SHR system.
	IQ Server System	This panel displays the host name, disk space, memory utilization (graph), and CPU utilization (graph) of the SHR database system. If Sybase IQ is installed on a remote system and HP Operations agent is not installed on the same remote system, this panel displays "NA" to indicate that no data is available.
	BO Server System	This panel displays the host name, disk space, memory utilization (graph), and CPU utilization (graph) of the SAP BusinessObjects system of the SHR installation. If SAP BusinessObjects is installed on a remote system and HP Operations agent is not installed on the same remote system, this panel displays "NA" to indicate that no data is available.

Group	Field	Description
	Runtime File Distribution	Displays the data distribution of the SHR file system according to the size of the files in the following folders: • archive • collect • extract • stage • failed_to_* Before the data collected from the data sources are loaded into the appropriate Sybase IQ database tables, it is held in the SHR system for processing. Also, the data that failed to pass the data processing streams (\stage\failed_to_* folder). are also stored on the SHR file system. Runtime file distribution shows the disk space used by these files.
	Content Health Summary	Displays the status of the data health in SHR fact tables for each installed content pack represented as follows: • **Success**: When data in SHR fact tables has been resolved. • **Failed**: When data in SHR fact tables could not be resolved and require attention. If a fact table encounters any of the following conditions, its health is marked 'Failed': • Data is not available for >10% of the dimensions. • Data is not available in hourly tables for the last 6 hours. • Data is not available in daily table for the last 1 day. • The table holds data for more than the configured period.

Group	Field	Description
ETL Status Summary	Content Pack Component Name	This table displays details of the Content Pack streams such as the total number of streams and the number of streams with errors. The total number of streams value indicates the number of streams that are currently running, or the number of streams that are loaded for execution, or the number of streams that completed in the last run. For additional information, you can drill down to the Data Processing page by clicking either the Content Pack component name or the stream number hyperlinks.
	Collection Status	Displays the number of data sources that are configured for each data collector. The status is represented in the following ways: • **Success**: When data collection from the data sources occurs without issues. • **Failed**: When data collection from the data sources has failed. • **Never Started**: When data collection from the data source has never occurred. The data displayed in this table is refreshed periodically. Click ⬚ to retrieve the data from the memory to the database. Click ⟳ to update the table with the latest data.
Alerts	ABC Alerts	This table list of all data processing job streams that have failed to complete along with their stream names, steps where the error occurred, messages, and dates. For more information, see View details of the ABC alerts.
	Health Alerts	This table displays the severity, message, and date of the all error, warning, and information alerts generated by SHR. The following icons are used to identify the types of alerts: • ⓘ indicates an information alert. No action is required for this type of alert. • ⚠ indicates a warning alert. You might need to resolve these types of alerts to ensure SHR functions properly. However, immediate action might not be required. • ✖ indicates an error alert. These are critical alerts and immediate action is required to resolve these issues.

Use the Home page to:

- View the SHR status

- View details of the ABC alerts

Service Definition

You can use the Service Definition page to create and configure RTSM and HPOM data source connections to provide topology-related data of your enterprise. On this page, you can schedule SHR to collect data from the data repositories at specific intervals. In addition, you can view the status of the connection and data collection.

The Service Definition page includes:

Service Definition Source

Field	Description
RTSM	Option to select RTSM as the source of the service definition data.
HP OM	Option to select HPOM database as the source of the service definition data.
VMware vCenter	Option to select VMware vCenter as the source of service definition data.
Host name	IP address or fully-qualified name (FQDN) of the service definition host system.
Enable Collection	Enable or disable the service definition data collection.
Schedule Frequency	Time (in hours) to synchronize the SHR database with the RTSM database.
Schedule HP OM Synchronization	Time (in hours) to synchronize the SHR database with the HPOM database.
Status	Status of the service definition source connection and data collection.
• Connection	Status of the service definition source connection. • Indicates that the SHR host system is connected to the data source. • Indicates that the SHR host system is not connected to the data source.

Field	Description
• Collection	Status of the collection showing the date and time of the latest collection attempt and the current status: • ⬆ indicates that the data collection is in progress. • ✓ indicates that the data collection completed successfully in the previous attempt. • ✖ indicates that the data collection failed in the previous attempt. • ⏸ indicates that the data collection was never started.
Configuration	Modify an existing service definition source connection.
Test Connection	Test a service definition source connection.
Create New	Create a new service definition source connection.
Save	Save a specific service definition source configuration attribute.

Connection Parameters: RTSM

Field	Description
Host name	IP address or FQDN of the Business Service Management server. If your HP Business Service Management deployment is distributed, type the name of the gateway server in this field.
Port	Port number to query the RTSM web service. The default port is 80.
User name	Name of the RTSM web service user. The default user name is admin.
Password	Password of the RTSM web service user. The default password is admin.

Connection Parameters: HP OM

Field	Description
Datasource Type	Select the type of HPOM that is configured in your environment. The options include: • HPOM for Windows • HPOM for Unix • HPOM for Linux • HPOM for Solaris
OM on Oracle RAC	Option to enable HPOM database on Oracle RAC. This option is not displayed when HPOM for Windows is selected.
Service Name	Specify the name by which SHR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.
File Name	The *.ora configuration file that defines database addresses for establising connections. Manually copy this file from the data source system to the SHR system. This option appears only if OM on Oracle RAC is selected.
Database Type	Depending on the data source type that you select, the database type is automatically selected for you. For the HPOM for Windows data source type, the database type is MSSQL. For the HPOM for Unix, HPOM for Linux, or HPOM for Solaris, the database type is Oracle.
Host name	IP address or fully-qualified domain name (FQDN) of the HPOM database server. This field is not displayed when OM on Oracle RAC is selected.
Database instance	System identifier (SID) of the database instance. The default database instance is OVOPS. This field is not displayed when OM on Oracle RAC is selected.
Database name	Name of the HPOM database. This field only appears if HPOM for Windows is selected as the data source type. The name of the database is openview.
Port	Port number to query the HPOM database server. For more information, see *HP Service Health Reporter Configuration Guide*.

Field	Description
Windows Authentication	Option to enable Windows authentication for accessing the HPOM database. The user can use the same credentials to access HPOM as that of the Windows system hosting the database. **Note**: If you are using the database method of authentication to connect to the HPOM database server, you must provide the user details that have the select and connect permissions for the "openview" database here. This option only appears if HPOM for Windows is selected as the data source type.
User name	Name of the HPOM database user. **Note**: For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.
Password	Password of the HPOM database user. **Note**: For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled.

Connection Parameters: VMware vCenter

Field	Description
Host name	IP address or FQDN of the VMware vCenter server.
User name	Name of the VMware vCenter user.
Password	Password of the VMware vCenter user.

Use the Service Definition page to:

- Select a service definition source

- Create a service definition source connection

- Modify a service definition source connection

- Enable or disable a service definition data collection

- Schedule a service definition synchronization

- Test the service definition source connection

- View a service definition source connection status

- View a service definition data collection status

HP Operations Agent

You can use the HP Operations agent page to manage the HP Operations agent data collection. You do not need to create new HP Operations agent data source connections because, by default, all the nodes on which the HP Operations agent is installed are automatically discovered when the topology data is collected. These data sources or nodes are listed on the HP Operations agent page. Using this page, you can schedule the HP Operations agent data collection, enable or disable the data collection, and delete HP Operations agent connections.

The HP Operations agent Data Source page includes:

View tab: HP Operations Agent Data Source Summary

Field	Description
Domain name (Content Pack Component Name)	A list of topology views for the installed Content Packs. These topology views contain the specific CI attributes that the HP Operations agent collector uses to collect the relevant data. *All* indicates all the views. *Unassigned* indicates the HP Operations agent data sources that do not have any topology views assigned to it.
Hosts	The number of HP Operations agent data sources for that particular view.
Collection: Passed	The number of distinct HP Operations agent data sources from where the raw data was successfully collected.
Collection: Failed	The number of distinct HP Operations agent data sources from where data collection failed.
Collection: Never Collected	The number of distinct HP Operations agent data sources from where data was never collected.
Enabled/Disabled	The number of distinct HP Operations agent data sources that are enabled or disabled for data collection.

View tab: HP Operations Agent Data Source Application Details

SHR shows all the managed nodes discovered from the HPOM topology where the HP Operations agent is installed. In an HPOM for Windows environment, the table lists the message allowed nodes too. However, the message allowed nodes do not contribute to the licensing computation.

Field	Description
Search: Host name	Search option that support pattern matching search. You can use this feature to search for a particular HP Operations agent data source node or filter this displayed list of nodes.

Field	Description
Host name	Name of the HP Operations agent data source.
Enable Collection	Enable or disable data collection from the HP Operations agent data source. **Note**: Use the enable or disable option in the header to enable or disable data collection from all the HP Operations agent Data Sources in the list.
Schedule Polling Frequency	Time (in hours) to synchronize the SHR database with the HP Operations agent data source.
Remote Collector	List of remote collectors enabled for data collection configured in SHR.
Rule Type	List of rules you can apply on the remote collector. User: Select it when you want to overwrite any pre-assigned rule or when you want to manually assign a remote collector to a host. System: If the remote collector assignment is based on the rules mentioned by the user from the Assignment tab. Unassigned: Indicates that no rules are defined for the host. You must manually assign a remote collector to the host using the rule type "User" or add/modify the rule from the Assignment tab to assign a remote collector to the host.
Connection Status	Status of the HP Operations agent data source connection. • ⊘ indicates that the host system is connected to the data source. • ⊗ indicates that the host system is not connected to the data source.
Collection Status	Status of the data collection showing the date and local time of the latest collection attempt and the current status. • ⊘ indicates that the data collection completed successfully. • ⊗ indicates that the data collection failed. • ⏸ indicates that the data collection was never started.
Test Connection	Test an HP Operations agent data source connection.
Save	Save the changes made to an HP Operations agent data source connection.
Update All	Opens the Apply schedule to group section where you can apply the collection schedule for all the listed hosts. This option does not appear for the **All** or **Unassigned** options in the View name column.

Assignment tab: Summary

Field	Description
Collector	Hostname of the remote collector.
Rules Assigned	Shows the rules or node/view groups assigned to the collector.

Assignment tab: Node Assignment

Field	Description
Collection Station	List of remote collectors configured in the SHR system.
Rule Type: Pattern Based	Select it for writing a regular expression to assign a remote collector to HP Operations agents.
Rule Type: View/Node Group Based	Select it to assign a remote collector to a view or node group of the installed content packs.
Rule	If the Rule Type is "Pattern Based", it lists rules defined by the user.
	If the Rule Type is "View/Node Group Based", it lists view or node groups of the installed content packs.

Use the HP Operations agent page to:

- View the HP Operations agent data source details

- Enable an HP Operations agent data source data collection

- Schedule an HP Operations agent data source synchronization

- Test the HP Operations agent data source connection

- Assign View/Node Group based Rules for Data Collection

- Assign Pattern based Rules for Data Collection

HP Operations Manager

You can use the HP Operations Manager (HPOM) page to view a list of HPOM data sources, which collect performance and event-related data of business-critical enterprise systems, applications, and services. Using this page, you can schedule the data collection frequency, enable, or disable data collection, and also add or delete data collection connections based on your requirements.

The Operations Manager page includes:

Field	Description
Host name	IP address or FQDN of the HPOM database server.

Field	Description
Enable Collection	Enable or disable a HPOM data collection.
Schedule Frequency	Time (in hours) to synchronize the SHR database with the HPOM data source.
Status	Status of an HPOM connection and data collection.
Connection	Status of the HPOM connection. • ✅ Indicates that the SHR host system is connected to the data source. • ❌ Indicates that the SHR host system is not connected to the data source.
Collection	Status of the collection showing the date and time of the latest collection attempt and the current status: • ⬆ indicates that the data collection is in progress. • ✅ indicates that the data collection completed successfully in the previous attempt. • ❌ indicates that the data collection failed in the previous attempt. • ⏸ indicates that the data collection was never started.
Configuration	Modify an existing HPOM data source connection.
Test Connection	Test an HPOM data source connection.
Delete	Delete an HPOM data source connection.
Create New	Create a new HPOM data source connection.
Save	Save a specific HPOM configuration attributes.

Connection Parameters

Field	Description
OM on Oracle RAC	Option to enable HPOM database on Oracle RAC.
Service Name	Specify the name by which SHR connects to the Oracle instance. This option appears only if OM on Oracle RAC is selected.

Field	Description
File Name	The *.ora configuration file that defines database addresses for establishing connections. Manually copy this file from the data source system to the SHR system. This option appears only if OM on Oracle RAC is selected.
Host name	IP address or FQDN of the HPOM database server. If the HPOM database is configured on a remote system, the machine name of the remote system must be typed here.
Port	Port number to query the HPOM database server. The default port is 1433 if SQL Server is the database type and 1521 if Oracle is the database type.
Database Instance	System Identifier (SID) of the database instance. The default database instance is OVOPS. **Note**: For information about the database host name, port number, and SID, contact your HPOM database administrator.
Database type	The type of database engine that is used to create the HPOM database. It can either be Oracle or MSSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database. **Note**: If you are using the database method of authentication to connect to the HPOM database server, you must provide the user details that have the select and connect permissions for the "openview" database here.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type. The name is openview.
User name	Name of the HPOM database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the HPOM database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

Use the HPOM page to:

- Create an HPOM data source connection

- Modify an HPOM data source connection

- Enable an HPOM data collection

- Schedule an HPOM data collection

- Test the HPOM data source connection

- View the HPOM data source connection status

- View the HPOM data collection status

- Delete an HPOM data source connection

Generic Database

You can use the Generic Database page to configure generic databases from where you want to collect any type of data. This page is typically used to configure the Network Performance Server (NPS) to collect performance date from Network Node Manager i (NNMi). Using this page, you can schedule the data collection frequency, enable, or disable data collection, and also add or delete data collection connections based on your requirements.

Out-of-the-box, SHR supports configuration to generic data sources that use Oracle, Sybase, or Microsoft SQL Server database types. However, using this page, you can also configure SHR to connect to and collect data from other generic database types as well, such as MySQL, PostgreSQL, and so on. For a particular database type, you can specify the domain for which you want SHR to collect data such as system data, network data, and so on. For more information on how to configure such data sources, contact HP Support.

The Generic Database page includes:

Field	Description
Host name	IP address or FQDN of the generic database server.
Enable Collection	Enable or disable data collection from a generic database.
Schedule Frequency	Time (in hours) to synchronize the SHR database with the generic database.
Status	Status of a generic database connection and data collection.

Field	Description
Connection	Status of the generic database connection. • ✅ Indicates that the SHR host system is connected to the data source. • ❌ Indicates that the SHR host system is not connected to the data source.
Collection	Status of the collection showing the date and time of the latest collection attempt and the current status: • ⬆ indicates that the data collection is in progress. • ✅ indicates that the data collection completed successfully in the previous attempt. • ❌ indicates that the data collection failed in the previous attempt. • ⏸ indicates that the data collection was never started.
Configuration	Modify an existing generic database connection.
Test Connection	Test a generic database connection.
Delete	Delete a generic database connection.
Create New	Create a new generic database connection.
Save	Save specific generic database attributes.

Connection Parameters

Field	Description
Host name	IP address or FQDN of the generic database server.
Port	Port number to query the database server.
Time zone	The time zone in which the database instance is configured. **Note:** You must select the same time zone for the database as the time zone of the data collected from data sources. They cannot be in different time zones.
Database type	The type of database engine that is used to create the database. It can be Sybase IQ, Sybase ASE, Oracle, or MSSQL.

Field	Description
Domain	Select the domain (s) for which you want SHR to collect data from the selected database type.
URL	The URL of the database instance. The syntax for the URL for each of the database types is: **Oracle**: `jdbc:bto:oracle://<server>:<port>;SID=<sid>` In an Oracle Real Application Cluster (RAC), copy the TNS ORA file to the SHR system and provide the absolute path in the following URL syntax: `jdbc:bto:oracle:TNSNamesFile=<absolute path of TNS ORA file>;TNSServerName=<Service name>` **MSSQL**: `jdbc:jtds:sqlserver://<server><port>/<database>;instance=<dbInstance>` **Sybase IQ**: `jdbc:sybase:Tds:<server>:<port>/<database>` **Sybase ASE**: `jdbc:sybase:Tds:<server>:<port>?ServiceName=<dbInstance>` **PostgreSQL**: `jdbc:postgresql://<server>:<port>/<database>` where <*server*>, <*port*>, <*sid*>, <*database*>, and <*dbInstance*> are replaceable variables that you must enter.
User name	Name of the generic database user.
Password	Password of the generic database user.
Collection Station	This option is used for a collector installed on a remote system.

Use the Operations Manager page to:

- Create a generic database connection

- Modify a generic database connection

- Enable or disable a generic database data collection

- Schedule a generic database data collection

- Test the generic database connection

- View the generic database connection status

- View the generic database collection status

- Delete a generic database connection

VMware vCenter

You can use the VMware vCenter Data Source page to view a list of VMware vCenter data sources, which collect performance and event-related data of business-critical VMware installed in your environment. Using this page, you can schedule the data collection frequency, enable, or disable data collection, and also add or delete data collection connections based on your requirements.

The VMware vCenter Data Source page includes:

Field	Description
Host name	IP address or FQDN of the VMware vCenter database server.
Enable Collection	Enable or disable a VMware vCenter data source data collection.
Schedule Frequency	Time (in minutes) to synchronize the SHR database with the VMware vCenter data source.
Connection	Status of the VMware vCenter connection. • Indicates that the SHR host system is connected to the data source. • Indicates that the SHR host system is not connected to the data source.
Configuration	Modify an existing VMware vCenter data source connection.
Test Connection	Test a VMware vCenter data source connection.
Delete	Delete a VMware vCenter data source connection.
Create New	Create a new VMware vCenter data source connection.
Save	Save a specific VMware vCenter configuration attributes.

Connection Parameters

Field	Description
Host name	IP address or FQDN of the VMware vCenter database server. If the VMware vCenter database is configured on a remote system, the machine name of the remote system must be typed here.

Field	Description
User name	Name of the VMware vCenter database user.
Password	Password of the VMware vCenter database user.
Collection Station	This option is used for a collector installed on a remote system.

Note: If you have configured VMware vCenter as the topology source, data collection parameters are automatically configured.

Use the VMware vCenter page to:

- "Create VMware vCenter data source connection" on page 78

- "Modify a VMware vCenter data source connection" on page 78

- "Enable or disable a VMware vCenter data collection" on page 79

- "Schedule a VMware vCenter data collection" on page 79

- "Test the VMware vCenter data source connection" on page 79

- "View the VMware vCenter data source connection status" on page 80

SiteScope

You can use the SiteScope page to configure a SiteScope data source, which collects data from several SiteScope monitors in your environment. Using this page, you can enable or disable data collection and add or delete the data collection connection according to your requirements.

The SiteScope page includes:

Field	Description
Host name	IP address or FQDN of the SiteScope server.
Enable Collection	Enable or disable data collection.
Status	Status of SiteScope connection and data collection.
Connection	Status of SiteScope connection.
	 • ⊘ indicates that the host system is connected to the data source. • ⊗ indicates that the host system is not connected to the data source.

Field	Description
Collection	Status of the collection showing the date and time of the latest collection attempt and the current status: • ⬆ indicates that the data collection is in progress. • ✔ indicates that the data collection completed successfully in the previous attempt. • ✖ indicates that the data collection failed in the previous attempt. • ⏸ indicates that the data collection was never started.
Configuration	Modify an existing SiteScope data source connection.
Test Connection	Test a SiteScope data source connection.
Discover Data Source	If you have configured the RTSM topology source, this button discovers all the associated SiteScope servers. Also, you must have deployed the SiS_Profile view.
Delete	Delete a SiteScope data source connection.
Create New	Create a new SiteScope data source connection. **Note**: The Create New option is disabled after you create a new connection or if an SiteScope connection already exists.
Save	Save the changes made on this page.

Connection Parameters

You must fill out the following fields to create a new SiteScope data source.

Field	Description
Connection Settings	
Host name	IP address or FQDN of the SiteScope server.
Port	Port number to query the SiteScope server.
Communication Mode	Select whether you want an HTTP or HTTPS connection to the SiteScope server.
User name	Name of the SiteScope user.
Password	Password of the SiteScope user.
Init String	Shared key used to establish a connection to SiteScope server.

Field	Description
Collection Station	This option is used for a collector installed on a remote system.
General Data Integration Settings: These settings create a generic data integration between the SiteScope server and the SHR server. After the connection is successful, SiteScope servers push data to the SHR server. Also, you must create a tag in SHR that you must manually apply to the SiteScope monitors that you want to report on. For more information on applying the tag, see documentation for SiteScope.	
Integration name	Enter the name of the integration. **Note**: You cannot change it later.
Encoding	The encoding type for communication between SHR and SiteScope.
Use SSL	Optional; if selected, you must enable the SiteScope server too to support communication over Secure Sockets Layer (SSL).
Reporting interval (seconds)	User configurable; frequency at which SiteScope pushes data to SHR.
Request timeout (seconds)	User configurable; the time to wait before the connection times out. Value of zero (0) gives you infinite timeout period.
Connection timeout (seconds)	User configurable; timeout until connection is reestablished. Value of zero (0) means timeout is not used.
Number of retries	Number of retries that SiteScope server attempts during connection error with SHR.
Authentication when requested	Optional; if selected, authentication is performed using the Web server user name and password.
Authentication user name	If SHR is configured to use basic authentication, specify the user name to access the server.
Authentication password	If SHR is configured to use basic authentication, specify the password to access the server.
Proxy address	If proxy is enabled on SiteScope, enter the proxy address.
Proxy user name	Enter user name of the proxy server.
Proxy password	Enter password of the proxy server.
Create tag	Select it to create a tag for the SiteScope monitors that you must manually apply from the SiteScope server.
Tag name	User defined name of the tag.

Use the SiteScope page to:

- Create a SiteScope data source connection

- Modify a SiteScope data source connection

- Enable or disable SiteScope data collection

- Test the SiteScope data source connection

- View the SiteScope data source connection status

- View the SiteScope data collection status

- Delete a SiteScope data source connection

BSM/OMi

You can use the BSM/OMi page to create and configure the Management Database, Profile Database, and OMi as a data source.

Management Database and Profile Database connections collect performance-related data of your enterprise for various HP BSM applications such as Business Process Monitor (BPM), Real User Monitor (RUM), and so on. You can schedule SHR to collect data from the data repositories at specific intervals. In addition, you can view the status of the connection and data collection.

You can use the OMi page to view an HP OMi data source, which collect events and health indicators from managed entities in your environment. Using this page, you can schedule the HP OMi data collection times, enable or disable data collection, and delete the data collection connection according to your requirements.

Before you create a new HP OMi data source connection, make sure that a data source connection for the HP BSM Management Database exists. This data connection is a prerequisite for the HP OMi connection because SHR collects the KPI metadata for HP OMi from the Management Database.

If you have one or more OMi setups in your environment, you must configure the OMi data source belonging to the HP BSM RTSM that was configured as the topology source.

The BSM/OMi page includes three tabs (Management Database, Profile Database, and OMi) that have the following options:

Management Database

Field	Description
Host name	IP address or FQDN of the Management Database host system.
Data source	Name of the data source configured for the Management Database.
Status	Status of the Management Database connection and data collection.

Field	Description
Connection	Status of the Management Database connection. • ✅ Indicates that the SHR host system is connected to the data source. • ❌ Indicates that the SHR host system is not connected to the data source.
Collection	Status of the collection showing the date and time of the latest collection attempt and the current status: • 🔼 indicates that the data collection is in progress. • ✅ indicates that the data collection completed successfully in the previous attempt. • ❌ indicates that the data collection failed in the previous attempt. • ⏸ indicates that the data collection was never started.
Configuration	Modify the existing Management Database connection.
Test Connection	Test the Management Database connection.
Discover Database	Discovers the Profile Database if it exists in the same Management Database host system.
Delete	Delete the Management Database connection.
Create New	Create a new Management Database connection.
Save	Save the changes made to the Management database connection parameters.

Management Database: Create New: Connection Parameters

Field	Description
Data source	Select your data source: BSM or OMi.
Host name	IP address or FQDN of the Management Database server. Not displayed when **Database in Oracle RAC** is selected.
Port	Port number to query the Management Database server. Not displayed when **Database in Oracle RAC** is selected.

Field	Description
Database type	The type of database engine that is used to create the Management Database. It can either be Oracle, MSSQL, or PostgreSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when **Database in Oracle RAC** is selected. **Note**: For information about the database host name, port number, and SID, contact your *HP Business Service Management* administrator.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
Database in Oracle RAC	This option appears only if you have selected Oracle as the database type.
Service name	Name of the service. This option appears only if **Database in Oracle RAC** is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if **Database in Oracle RAC** is selected.
User name	Name of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the Management Database user, which was specified in the BSM Configuration Wizard when setting up the Management Database. **Note**: If the Windows Authentication option is selected, this field is disabled.

Profile Database

Field	Description
Host name	IP address or FQDN of the Profile Database host system.
Enable Collection	Option to enable or disable data collection.

Field	Description
Frequency	Time (in hours) to synchronize the SHR database with the Profile Database.
Status	Status of the Profile Database connection and data collection.
Connection	Status of the Profile Database connection. • ⊘ Indicates that the SHR host system is connected to the data source. • ⊗ Indicates that the SHR host system is not connected to the data source.
Collection	Status of the collection showing the date and time of the latest collection attempt and the current status: • ⬆ indicates that the data collection is in progress. • ⊘ indicates that the data collection completed successfully in the previous attempt. • ⊗ indicates that the data collection failed in the previous attempt. • ⏸ indicates that the data collection was never started.
Configuration	Modify the existing Profile Database connection.
Test Connection	Test the Profile Database source connection.
Delete	Delete the Profile Database connection.
Create New	Create a new Profile Database connection.
Save	Save the changes made to the Profile Database connection parameters.

Profile Database: Create New: Connection Parameters

Field	Description
Host name	IP address or FQDN of the Profile Database server. Not displayed when **Database in Oracle RAC** is selected.
Port	Port number to query the Profile Database server. Not displayed when **Database in Oracle RAC** is selected.

Field	Description
Database type	The type of database engine that is used to create the Profile Database. It can either be Oracle, MSSQL, or PostgreSQL.
Management Database	Links Profile Database to the Management Database. If you collect data from only SiteScope, no Management Database needs to be selected.
Domains	Select the domains for which you want to enable data collection. **Note:** You must select the domains from which you want to enable data collection. If you have skipped topology configuration during post-install configuration and installed the content packs, you must return here to select from among the following domains to enable data collection. • HP Operations Manager • OMi • RUM • BPM • Service Health
Database instance	System Identifier (SID) of the Profile Database instance. Not displayed when **Database in Oracle RAC** is selected. **Note**: For information about the database host name, port number, and SID, contact your *HP Business Service Management* administrator.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
Database in Oracle RAC	This option appears only if you have selected Oracle as the database type.
Service name	Name of the service. This option appears only if **Database in Oracle RAC** is selected.
ORA file name	The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if **Database in Oracle RAC** is selected.

Field	Description
User name	Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

OMi

Field	Description
Host name	IP address or FQDN of the HP OMi database server.
Enable Collection	Option to enable or disable data collection.
Frequency	Time (in hours) to synchronize the SHR database with the HP OMi database.
Data source	Name of the data source configured for the HP OMi database.
Status	Status of HP OMi database connection and data collection.
Connection	Status of HP OMi connection. • ⊘ indicates that the host system is connected to the data source. • ⊗ indicates that the host system is not connected to the data source.
Collection	Status of the collection showing the date and time of the latest collection attempt and the current status: • ⬆ indicates that the data collection is in progress. • ⊘ indicates that the data collection completed successfully in the previous attempt. • ⊗ indicates that the data collection failed in the previous attempt. • ⏸ indicates that the data collection was never started.
Configuration	Modify an existing HP OMi database connection.

Field	Description
Test Connection	Test an HP OMi database connection.
Delete	Delete an HP OMi database connection.
Create New	Create a new HP OMi database connection. **Note**: The Create New option is disabled after you create a new connection or if an HP OMi connection already exists.
Save	Save the changes made on this page.

OMi: Create New: Connection Parameters

Field	Description
Host name	IP address or FQDN of the HP OMi database server.
Port	Port number to query the HP OMi database server.
Database Instance	System Identifier (SID) of the HP OMi database instance. **Note**: For information about the database hostname, port number, and SID, contact your HP OMi database administrator.
Database type	The type of database engine that is used to create the HP OMi database. It can either be Oracle, MSSQL, or PostgreSQL.
Windows Authentication	If you have selected MSSQL as the database type, you have the option to enable Windows authentication for MSSQL, that is, the user can use the same credentials to access SQL Server as that of the Windows system hosting the database.
Database name	Name of the database. This field appears only if MSSQL is selected as the database type.
User name	Name of the HP OMi database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Password	Password of the HP OMi database user. **Note**: If the Windows Authentication option is selected, this field is disabled.
Collection Station	This option is used for a collector installed on a remote system.

System Configuration

You can use the System Configuration page to manage the centralized SHR database and the SHR management database. You can view the details of the SHR database and change the database administrator password on this page.

The System Configuration page includes:

HP SHR Database Parameters

Field	Description
Database Type	Type of the database engine that is used for the SHR database.
Host name	FQDN or IP address of the host system on which the SHR database is running.
Server name	Name of the SHR database server.
Port	Port number to query the database. The default port is 21424.
User name	Name of the SHR database user account. This account is created during the post-installation stage.
Reset Password	Change the database password. Opens the Reset Password dialog box.

HP SHR Management Database Parameters

Field	Description
Database Type	Type of the database engine that is used for the SHR management database.
Host name	Name or IP address of the host system on which the SHR management database is running.
Database name	Name of the SHR management database instance.
Port	Port number to query the management database. The default port is 21425.
User name	Name of the SHR management database user account. This account is created during the post-installation stage.
Reset Password	Change the database password. Opens the Reset Password dialog box.

Reset Password

Field	Description
Old Password	Enter the existing database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value and less than 25 characters in length.
Confirm New Password	Retype the new password for confirmation purposes.

Use the System Configuration page to:

- View database configuration details

- Change the SHR database password

- Change the SHR management database password

Licensing

The Licensing page displays the SHR license details. You can change the license type by accessing the HP Password Center through the hyperlink provided on the page.

The Licensing page includes:

Filed	Description
Active License Type	Type of existing license; license types include: - Instant On (IO): 60-day evaluation license (default) - Permanent (PERM): Permanent license
License Expiry Date	Date and time of expiry of the existing license in local time.
Days to License Expiry	Number of days remaining for the license to expire.
License Entitlement	The maximum number of nodes that are supported under the current license.
License Usage	The number of nodes being used under the current license.
Nodes Remaining\Nodes Exceeded	The remaining number of nodes that can be added under the current license or the number of nodes that exceed the current license usage.
Launch HP Password Center	Link to access the HP Password Center web site to obtain a permanent license key.

Use the Licensing page to:

- View license information

- Obtain a Permanent license key

Security

You can use the Security page to configure the security authentication protocols that are used by SHR—Lightweight Single Sign-On (LW-SSO) and SAP BusinessObjects Trusted Authentication.

The Security page includes:

LW-SSO tab

Field	Description
Enabled	Enable or disable LW-SSO.
Domain	Domain for which LW-SSO is valid; by default, the SHR host system's domain is enabled
Expiration Period	Period for which the LW-SSO session is valid; The default value is 60 minutes **Note**: The LW-SSO expiration period should be at least the same value as that of the application session expiration value. The recommended value is 60 minutes. For applications that do not require high levels of security, you can configure higher values, such as 300 minutes. **Note**: All applications participating in an LW-SSO integration must use the same GMT time.
Init String	Shared key used for encryption and decryption of a LW-SSO session token **Note**: For LW-SSO, ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same Init String.
Protected Domains	Domains for which LW-SSO is protected; by default, the SHR host system's domain is protected

BO Trusted Authentication tab

Field	Description
Enabled	Enable or disable SAP BusinessObjects Trusted Authentication
Shared Secret	Shared key used for encryption and decryption of a Trusted Authentication session token

Use the Security page to:

- Configure LW-SSO authentication

- Configure SAP BusinessObjects Trusted Authentication

Note: This page is only visible if SHR is installed on the system.

Data Processing

The Data Processing page enables you to control the workflow job stream. Information on this page is divided between the following two tabs:

Active Stream Details tab

This tab allows you to configure the job streams and specify a maximum number of retries for the streams as well as a maximum execution time per step. You can specify the number of retries and the execution time across all Content Packs, for a particular Content Pack component, for a job stream, or for a particular job step in a stream.

The Active Stream Details tab includes:

Field	Description
Level	Select the level at which you want to configure the maximum number of retries and the maximum execution time. The options include: - All content packs - Content pack - Stream - Step
Content Pack name	Name of the Content Pack. This drop-down list appears only when you select **Content pack**, **Stream**, or **Step** in the **Level** list.
Stream Name	Name of the job stream present in the selected Content Pack. This drop-down list appears only when you select **Stream** or **Step** in the **Level** list.
Step ID	Unique identifier for the job step. This column appears only when you select **Step** in the **Level** list.
Business Name	An alias name for the stream. This column appears only when you select **Step** in the **Level** list.
Maximum Number of Retries	Maximum number of retries for the job step in the event of its failure. The maximum value that you can set for this field is 8640.

Field	Description
Maximum Execution Time (Mins)	Maximum amount of time, in minutes, for a job step to complete running. The maximum value that you can set for this field is 180 minutes.
Save	Save the changes made.

Stream Resource Control tab

This tab displays the job stream resource details and helps you to manage the resources attached to a particular step in a job stream and set limits for the number of jobs that can access the resource types.

The Stream Resource Control tab includes:

Field	Description
Resource Type	Type of resource that is used for data processes.
Unlimited Resources	Option to provide access to unlimited resources. Selecting this option disables the Resource Count field.
Resource Count	Maximum number of streams that can access the resource concurrently. The maximum value that you can set for this field is 20,000.
Save	Save the changes made.

Use the Data Processing page to:

- Configure the maximum number of retries and the maximum execution time

- Configure the stream resource details

SAP BOBJ

You can use the SAP BOBJ page to create and manage user accounts by using the SAP BusinessObjects CMC, which is integrated with SHR. SAP BusinessObjects InfoView allows you to personalize user experience when viewing the SHR reports by providing interactivity and customization options.

The SAP BOBJ page includes:

Field	Description
Launch CMC	Launch the SAP BusinessObjects CMC.
Launch InfoView	Launch the SAP BusinessObjects InfoView.

Use the SAP BOBJ page to:

- Access SAP BusinessObjects Central Management Console

- Access SAP BusinessObjects InfoView

- Create a password for the Administrator account

- Troubleshooting BusinessObjects Services

Note: This page is only visible if SHR is installed on the system.

Aging

You can use the Aging page to manage the retention time of the data stored in the SHR database tables. You can specify the period for which SHR retains the data in the tables, after which it is purged.

The Aging page includes:

Aging

Field	Description
Content Pack Component Name	Name of the Content Pack component for which to view aging and archiving details.
Installed Date	Date and time of the Content Pack component installation.
Version	Version number of the Content Pack component.
Status	Status of the Content Pack component installation; the status include: • Installed—Indicates that the Content Pack component is installed. • Install failed—Indicated that the Content Pack component installation attempt failed.
Configure Retention	Options to configure retention policies.

Configure Retention

Field	Description
Time Type	The type of data table used for storing the collected or summarized data. The types are: • As-polled—This table contains the as polled or raw data. • 5-minute—This table contains the summary data collected every five minutes. • Hourly—This table contains the raw or rate data that is aggregated at an hourly level. • Daily—This table contains the hourly data that is aggregated at the daily level. • Monthly—This table contains the daily data that is aggregated at the monthly level. • Yearly—This table contains the monthly data that is aggregated at the yearly level. **Note:** Monthly table and yearly table are not physical tables in the database for any out-of-the-box (OOTB) content packs.
Active Retention	Period for which SHR retains data. The default values are: • Raw or as polled data: 90 days. • Rate or 5-minute data: 90 days • Hourly data: 365 days • Daily data: 1825 days • Monthly data: 1825 days • Yearly data: 1825 days

Use the Aging page to configure active retention period.

Services

The Services page displays a list of SHR database and SAP BOBJ Enterprise services.

The Services page includes:

Field	Description
Service	Types of services that are included with SHR; the options include: • SHR Status • SAP BOBJ Enterprise status
Service Name	Name of the service.
Description	Description of the service. For a detailed description, see Managing services.
Status	Status of the service. **Legend description**: ✅ indicates that the service is up and running. ❌ indicates that the service is not running. ⚠️ indicates a warning. ❓ indicates that the status of the service is unknown.
Start/Stop	Option to start a service that is not running or stop a service that is running. This option is not available for the SAP BOBJ Enterprise services.

Service Detail for:

Service Message Detail tab:

Field	Description
Severity	The severity of the message. **Legend description**: ✅ indicates that the service is running. ❌ indicates an error. ⚠️ indicates a warning. ❓ indicates that the status of the service is unknown.
Message	A detailed description of the status.

Service Dependency

Field	Description
Name	The name of the SHR service that has a dependency on the selected service.
Service Name	The name of the service as displayed in the Services window.
Dependent	Indicates that the displayed service is depends on the selected service.
Depends On	Indicates that the selected service depends on the displayed service.

Use the Services page to:

- View the status of an SHR service

- Start or stop an SHR service

- View the status of a SAP BOBJ Enterprise service

Shift Management

You can use the Shift Management page to create new time shifts, modify the shift, and expire shifts that are no longer required.

The Shift Management page includes:

Shift Management

Field	Description
Shift Name	Name of the shift.
Status	The current status of the shift. It can be either ACTIVE or INACTIVE.
Effective From	The date from which shift-based data is collected by SHR.
Expires On	The date when the shift will expire. If a shift is configured to not expire, "Do Not Expire" is displayed.

Create New Shift

Field	Description
Shift Name	Name of the shift that you want to create such as prime, swing, or graveyard.

Field	Description
Effective From	The date from when you want the shift to be implemented.
Expires On	The date when the shift should expire.
Do Not Expire	Select this check box if you do not want the shift to expire. If you select this option, the shift will remain active until you manually expire it.
Shift Day	The day that you want to include in your shift period.
Start Time	The starting time of the shift. The value must in 24-hour format. The range of the start time is 0 to 23 hours.
End Time	The ending time of the shift. The value must in 24-hour format. The range of the end time is 1 to 24 hours.
Delete	Delete a row.
Add New Row	Add multiple days to the shift period.
Cancel	Cancel the changes.
Save	Save the changes.
Expire Shift	Expire the shift if it no longer required.

Edit Shift

Field	Description
Shift Name	Name of the shift. This field is disabled by default.
Effective From	The date from when you want the shift to be implemented. This field is disabled by default.
Expires On	The date when the shift should expire. This field is disabled if the Do Not Expire check box is selected.
Do Not Expire	Select this check box if you do not want the shift to expire. If you select this option, the shift will remain active until you manually expire it.
Shift Day	The day that you want to include in your shift period.
Start Time	The starting time of the shift. The value must in 24-hour format. The range of the start time is 0 to 23 hours.
End Time	The ending time of the shift. The value must in 24-hour format. The range of the end time is 1 to 24 hours.

Field	Description
Delete	Delete a row.
Add New Row	Add multiple days to the shift period.
Cancel	Cancel the changes.
Save	Save the changes.
Expire Shift	Expire the shift if it no longer required.

Use the Shift Management page to:

- View time shifts

- Create a new time shift

- Modify the time shift

- Expire the time shift

Deployment Manager

You can use the Deployment Manager page to install and remove Content Pack components. In SHR, the Content Packs are structured into the following layers or components:

Domain Content Pack component

The Domain or Core Domain component defines the data model for a particular Content Pack. It contains the rules for generating the relational schema. It also contains the data processing rules, including a set of standard pre-aggregation rules, for processing data into the database. The Domain component can include the commonly-used dimensions and cubes, which can be leveraged by one or more Report Content Pack components. The Domain Content Pack component does not depend on the configured topology source or the data source from where you want to collect data.

ETL Content Pack component

The ETL Content Pack component defines the collection policies and the transformation, reconciliation, and staging rules. It also provides the data processing rules that define the order of execution of the data processing steps. The ETL Content Pack component is data source dependent. Therefore, for a particular domain, each data source application has a separate ETL Content Pack component. For example, if you want to collect system performance data from the HP Performance Agent and HP SiteScope data source applications, you must install the **SysPerf_ETL_ PerformanceAgent** and **ETL_SystemManagement_SiS** ETL components respectively. A single data source application can have multiple ETL components. For example, you can have one ETL component for each virtualization technology supported in Operations agent such as Oracle Solaris Zones, VMware, IBM LPAR, and Microsoft HyperV. The ETL component can be dependent on one or more Domain components. In addition, you can have multiple ETL components feeding data into the same Domain component.

Report Content Pack component

The Application Content Pack component defines the application-specific aggregation rules, business views, SAP BOBJ universes, and the reports for a particular domain. Application components can be dependent on one or more Domain components. It also provides the flexibility to extend the data model that is defined in one or more Domain components.

The Deployment Manager simplifies the selection of the Content Pack components by filtering them based on the topology source that you defined in the post-install configuration phase. From the filtered list, you can then select the Content or specific Content Pack components that you want to install. The Deployment Manager performs a silent installation or uninstallation of the Content Pack components while displaying the updated status on the page.

The Deployment Manager page includes:

Deployment Manager

Field	Description
Content	The type of content or domain for which data is collected by SHR. The list of Content displayed is filtered based on the topology source that is defined, that is, RTSM or HPOM.
Data Source Application	The data sources from where SHR will collect data for the Content.
Content Pack Component Name	Name of the Content Pack component. A Content Pack is typically comprised of three components—domain, ETL, and report. For more information about these Content Pack types, see the *HP Service Health Reporter Concepts Guide*. The name of the Content Pack component is based on the following syntax: **AcronymofContentPack_Component_** ***<Technology>_<DatasourceVersion>*** For example, SysPerf_Domain, VirtualEnvPerf_ETL_ HyperV_PerformanceAgent, RealUsrTrans_Reports The technology, data source, and version of the data source are optional. The data source and its version will be appended only in the case of the ETL component where the component is data-source dependent.
Version	Version of the Content Pack component.

Field	Description
Status	Displays the status of the installation or uninstallation process. During the installation or uninstallation process, the Deployment Manager page automatically refreshes and displays the updated status of the process.
Remove	Removes an installed Content Pack component.
Deploy	Installs the selected Content Pack components.
Restore Default	Resets the page to the default Content selection. Use this button if you modified the list of Content to be installed or uninstalled and want to go back to the default selection.

Content Pack Component Status History

Field	Description
Content Pack Component Name	Name of the Content Pack component.
Status	Displays the status of the installation or uninstallation process. During the installation or uninstallation process, the Deployment Manager page automatically refreshes and displays the updated status of the process.
Install Date	The data and time when the selected Content Pack component was installed or uninstalled.
Version	Version of the Content Pack component.
Message	Description of the installation or uninstallation status.

The list of all ready-to-use Content Packs available on the Deployment Manager page:

Core Content Pack

You must install this content pack before or while installing any other content pack. Following are the components:

- Core_Domain

- Core_Domain_AppServer

- Core_Domain_EUM

Cross-Domain Operations Events

HP OMi: If you are installing this content pack to generate reports on data from OMi 10, select the following and click Install/Upgrade:

- HP Operations Manager i

  - CrossOprEvent_ETL_OMi10

  - CrossOprEvent_ETL_OMi (if topology is RTSM)

  - CrossOprEvent_Domain_Reports

OMi Extended: The OMi Extended content pack includes an extended set of attributes from OMi as follows:

- Event Annotations

- Event Property Changes

- Event Forwarding Details

- Custom Message Attributes (CMAs)

If you are installing the OMi Extended content pack to generate reports on data from OMi, select the following and click Install/Upgrade:

- HP Operations Manager i

  - CrossOprEvent_ETL_OMi10_Extended

  - CrossOprEvent_ETL_OMi_Extended (if topology is RTSM)

  - CrossOprEvent_Domain_Reports_Extended

> **Tip:** Install the following dependent content packs (and their components) along with this content pack for it to function:
>
> - Core
>
>   - Core_Domain

Health and Key Performance Indicators (Service Health)

BSM: If you are installing this content pack to generate reports on data from BSM, select the following and click Install/Upgrade:

- HP BSM Service Health

  - HIKPI_ETL_ServiceHealth

  - HIKPI_Domain

  - HIKPI_Reports_ServiceHealth

HP OMi: If you are installing this content pack to generate reports on data from OMi 10, select the following and click Install/Upgrade:

- HP BSM Service Health

  - HIKPI_ETL_ServiceHealth_OMi10

  - HIKPI_Domain

  - HIKPI_Reports_ServiceHealth

> **Tip:** Install the following dependent content packs (and their components) along with this content pack for it to function:
>
> - Core
>
>   - Core_Domain

IBM WebSphere Application Server

HPOM: If you are installing this content pack to generate reports on data from HPOM, select the following and click Install/Upgrade:

- HP Operations Smart Plug-in for WebSphere Application Server

  - IBMWebSphere_ETL_WebSphereSPI

  - IBMWebSphere_Domain

  - IBMWebSphere_Reports

Also, review the Prerequisite Policies for IBM WebSphere Reports (SPI).

BSM/OMi: If you are installing this content pack to generate reports on data from BSM/OMi, select the following and click Install/Upgrade:

- OMi Management Pack for IBM WebSphere Application Server

  - IBMWebSphere_ETL_WebSphereMP

  - IBMWebSphere_Domain

  - IBMWebSphere_Reports

Also, review the Prerequisite Policies for IBM WebSphere Reports (SPI). If you have an underlying HPOM environment that collects data through SPIs and feeds it to OMi, review these Prerequisite Policies for IBM WebSphere Reports (MP).

> **Tip:** Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core

  - Core_Domain

  - Core_Domain_AppServer

- Operations Manager

  - OprEvent_Domain_Reports

- System Performance

  - SysPerf_Domain

Microsoft Active Directory

HPOM and BSM/OMi: If you are installing this content pack to generate reports on data from HPOM, BSM, or OMi, select the following and click Install/Upgrade:

- HP Operations Smart Plug-in for Microsoft Active Directory, OMi Management Pack for Microsoft Active Directory

  - MicrosoftActiveDirectory_ETL_ADSPI

  - MicrosoftActiveDirectory_Domain

  - MicrosoftActiveDirectory_Reports

Also, review the Prerequisite Policies for Microsoft Active Directory Reports (SPI) and Prerequisite Policies for Microsoft Active Directory Reports (MP).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core

  - Core_Domain

  - MSAppCore

Microsoft Exchange Server

HPOM and BSM/OMi: If you are installing this content pack to generate reports on data from HPOM, BSM, or OMi, select the following and click Install/Upgrade:

For Microsoft Exchange 2007

- HP Operations Smart Plug-in for Microsoft Exchange 2007

  - MicrosoftExchange_ETL_ExchangeSPI2007

  - MicrosoftExchange_Domain

  - MicrosoftExchange_Reports

For Microsoft Exchange 2010

- HP Operations Smart Plug-in for Microsoft Exchange 2010, OMi Management Pack for Microsoft Exchange Server

  - MicrosoftExchange_ETL_ExchangeSPI2010

  - MicrosoftExchange_Domain

  - MicrosoftExchange_Reports

For Microsoft Exchange 2013

- HP Operations Smart Plug-in for Microsoft Exchange 2013, OMi Management Pack for Microsoft Exchange Server

  - MicrosoftExchange_ETL_ExchangeSPI2013

  - MicrosoftExchange_Domain

  - MicrosoftExchange_Reports

Also, review the Prerequisite Policies for Microsoft Exchange Server Reports (SPI).

> **Tip:** Install the following dependent content packs (and their components) along with this content pack for it to function:
>
> - Core
>
>   - Core_Domain
>
>   - MSAppCore
>
> - System Performance
>
>   - SysPerf_Domain
>
>   - SysPerf_Reports

Microsoft SQL Server

HPOM and BSM/OMi: If you are installing this content pack to generate reports on data from HPOM, BSM, or OMi, select the following and click Install/Upgrade:

- HP Operations Smart Plug-in for Microsoft SQL Server, OMi Management Pack for Microsoft SQL Server

  - MicrosoftSQLServer_ETL_DBSPI

  - MicrosoftSQLServer_Domain

  - MicrosoftSQLServer_Reports

Also, review the Prerequisite Policies for Microsoft SQL Server Reports (SPI) and Prerequisite Policies for Microsoft SQL Server Reports (MP).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core

  - Core_Domain

- System Performance

  - SysPerf_Domain

Network Performance

RTSM: If you are installing this content pack to generate reports on network data where Network Mode Manager i (NNMi) is integrated with BSM, select the following and click Install/Upgrade:

- NNM iSPI for Performance

  - NetworkPerf_ETL_PerfiSPI_RTSM

  - NetworkPerf_Domain

  - NetworkPerf_Reports

Non-RTSM: If you are installing this content pack to generate reports on network data where Network Mode Manager i (NNMi) is not integrated with BSM, select the following and click Install/Upgrade:

- NNM iSPI for Performance

  - NetworkPerf_ETL_PerfiSPI_NonRTSM

  - NetworkPerf_Domain

  - NetworkPerf_Reports

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core

    - Core_Domain

- System Performance

    - SysPerf_Reports

Operations Events

HPOM: If you are installing this content pack to generate reports on events logged into HPOM, select the following and click Install/Upgrade:

- HP Operations Manager

    - OprEvent_ETL_HPOM

    - OprEvent_Domain_Reports

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core

    - Core_Domain

Oracle

HPOM and BSM/OMi: If you are installing this content pack to generate reports on data from HPOM, BSM, or OMi, select the following and click Install/Upgrade:

- HP Operations Smart Plug-in for Oracle, OMi Management Pack for Oracle

    - Oracle_ETL_DBSPI

    - Oracle_Domain

    - Oracle_Reports

Also, review the Prerequisite Policies for Oracle Database Reports (SPI) and Prerequisite Policies for Oracle Database Reports (MP).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core

    - Core_Domain

- Operations Manager

  - OprEvent_Domain_Reports

- System Performance

  - SysPerf_Domain

Oracle WebLogic Server

HPOM: If you are installing this content pack to generate reports on data from HPOM, select the following and click Install/Upgrade:

- HP Operations Smart Plug-in for Oracle WebLogic Server

  - OracleWebLogic_ETL_WebLogicSPI

  - OracleWebLogic_Domain

  - OracleWebLogic_Reports

Also, review the Prerequisite Policies for Oracle WebLogic Reports (SPI).

BSM/OMi: If you are installing this content pack to generate reports on data from BSM/OMi, select the following and click Install/Upgrade:

- OMi Management Pack for Oracle WebLogic Server

  - OracleWebLogic_ETL_WebLogicMP

  - OracleWebLogic_Domain

  - OracleWebLogic_Reports

Also, review the Prerequisite Policies for Oracle WebLogic Reports (MP). If you have an underlying HPOM environment that collects data through SPIs and feeds it to OMi, review these Prerequisite Policies for Oracle WebLogic Reports (SPI).

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core

  - Core_Domain

  - Core_Domain_AppServer

- Operations Manager

- OprEvent_Domain_Reports
- System Performance
  - SysPerf_Domain

Real User Transaction Monitoring (RUM)

HPOM: If you are installing this content pack to generate reports on data from HPOM, select the following and click Install/Upgrade:

- HP Real User Monitor
  - RealUsrTrans_ETL_RUM
  - RealUsrTrans_Domain_Reports

BSM/OMi: If you are installing this content pack to generate reports on data from BSM/OMi, select the following and click Install/Upgrade:

- HP Real User Monitor
  - RealUsrTrans_ETL_RUM_OMi
  - RealUsrTrans_Domain_Reports

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core
  - Core_Domain
  - Core_Domain_EUM
- Operations Manager
  - OprEvent_Domain_Reports
- System Performance
  - SysPerf_Domain
  - SysPerf_Reports
- Virtualization Performance
  - VirtualEnvPerf_Domain

- Operation Events (Operations Manager)

  - ServiceHealth

Synthetic Transaction Monitoring (BPM)

HPOM: If you are installing this content pack to generate reports on data from HPOM, select the following and click Install/Upgrade:

- HP Business Process Monitor

  - SynTrans_ETL_BPM

  - SynTrans_Domain_Reports

BSM/OMi: If you are installing this content pack to generate reports on data from BSM/OMi, select the following and click Install/Upgrade:

- HP Business Process Monitor

  - SynTrans_ETL_BPM_OMi

  - SynTrans_Domain_Reports

Tip: Install the following dependent content packs (and their components) along with this content pack for it to function:

- Core

  - Core_Domain

  - Core_Domain_EUM

System Performance

HP Operations Agent: If you are installing this content pack to generate reports on data from HP Operations Agent, select the following and click Install/Upgrade:

- HP Performance Agent, HP Operations agent

  - SysPerf_ETL_PerformanceAgent

  - SysPerf_Domain

    SysPerf_Reports

HP SiteScope: If you are installing this content pack to generate reports on data from HP SiteScope, select the following and click Install/Upgrade:

- HP SiteScope

  - SysPerf_ETL_SiS_API or SysPerf_ETL_SiS_DB (SysPerf_ETL_SiS is deprecated)

  - SysPerf_Domain

  - SysPerf_Reports

The `SysPerf_SiS_ETL` Content Pack component is deprecated. Instead of `SysPerf_SiS_ETL`, use `SysPerf_SiS_DB` or `SysPerf_SiS_API`.

If you have upgraded from an older version of SHR, follow these steps to move from `SysPerf_SiS_ETL` to `SysPerf_SiS_DB` or `SysPerf_SiS_API`:

1. Log on to the SHR Administration Console.

2. Go to the Administration tab.

3. Click **Data Source Selection**.

4. Make appropriate data source selection, and then, under every SiteScope check box, select **Direct API** or **ProfileDB**.

   > **Note:** These options appear only after you select the SiteScope check box.

5. Click **Save**.

6. Click **Deployment Manager**.

7. Select `SysPerf_SiS_API` if you select Direct API or `SysPerf_SiS_DB` if you selected ProfileDB, and then click **Install/Upgrade**.

> **Tip:** Install the following dependent content packs (and their components) along with this content pack for it to function:
>
> - Core
>
>   - Core_Domain

Virtual Environment Performance

HP Operations Agent: If you are installing this content pack to generate reports on data from HP Operations Agent, select the following and click Install/Upgrade:

- HP Performance Agent

  - VirtualEnvPerf_ETL_HyperV_PerformanceAgent

  - VirtualEnvPerf_ETL_IBMLPAR_PerformanceAgent

- VirtualEnvPerf_ETL_SolarisZones_PerformanceAgent

- VirtualEnvPerf_ETL_VMWare_PerformanceAgent

- VirtualEnvPerf_Domain

- VirtualEnvPerf_Reports

HP SiteScope: If you are installing this content pack to generate reports on data from HP SiteScope, select the following and click Install/Upgrade:

- HP SiteScope

  - VirtualEnvPerf_ETL_VMware_SiS_API

  - VirtualEnvPerf_ETL_VMware_SiteScope

  - VirtualEnvPerf_Domain_VMWare

    VirtualEnvPerf_Reports_VMWare

VMware vCenter: If you are installing this content pack to generate reports on data from VMware vCenter, select the following and click Install/Upgrade:

- VMware vCenter

  - VirtualEnvPerf_ETL_VMWare_vCenter

  - VirtualEnvPerf_Domain_VMWare

  - VirtualEnvPerf_Reports_VMWare

> **Tip:** Install the following dependent content packs (and their components) along with this content pack for it to function:
>
> - Core
>
>   - Core_Domain
>
> - System Performance
>
>   - SysPerf_Domain

Use the Deployment Manager page to:

- Install a Content Pack

- Remove an Installed Content Pack

Collector Configuration

You can use the Collection Configuration page to create and configure a collector that is installed on a remote system (and not on the SHR system).

Collection Summary

Field	Description
Name	Display name of the user (Note, it cannot be changed once configured)
Enable	To enable or disable the collector that is installed on the remote system. If a data source has already been assigned to any the collector for data collection, then the application will not allow you to disable the collector.
Connection	To test the connection between SHRsystem and the remote system where the collector is installed.
Install	It indicates whether the collector is installed.
Configuration: Policy	It indicates whether all necessary collection policies are installed on the collector system. If necessary policies are not present, click the Refresh ( ) icon.
Configuration: Data Source	It indicates whether any data sources are configured with the collector.

Configuration Parameters

Field	Description
Name	Display name of the user (Note, it cannot be changed once configured)
Host Name	To enable or disable the remote collector.If any data source has already been assigned to any remote collector for data collection, then the application will not allow you to disable the remote collector.

Use the Collection Configuration Page to perform the following tasks:

- Configuring a Collector Installed on a Remote System

- Disabling a Collector Installed on a Remote System

Content

The Content page allows you to monitor the status of the data in SHR fact tables for each installed content pack. You can verify the health of data flow from data source into the fact tables associated with the dimensions of each content pack.

When a caution status (⚠) is indicated in the row labeled "Health", you can drill down to the reports, fact tables, and dimensions or CIs that are impacted by gaps in data.

If the CIs have not logged data, verify if they have been decommissioned. If yes, you can delete those dimensions and their fact tables from SHR. For more information, see *HP Service Health Reporter Administration Guide*.

The Content page includes:

Field	Description
Content Pack Component Name	Name of the content pack.

Field	Description
Health	Indicates the health of data for the content pack based on the fact tables in the Sybase IQ database. **Legend description**: ⊘ indicates that the data tables have no issues. ⚠ indicates that the data tables need attention. If a fact table encounters any of the following conditions, its health is marked ⚠: • Data is not available for >10% of the dimensions. • Data is not available in hourly tables for the last 6 hours. • Data is not available in daily table for the last 1 day. • The table holds data for more than the configured period. You can configure these threshold values from *{PMDB_HOME} /adminServer/webapps/BSMRApp/threshold.prp* file. To exclude tables due to non-availability of data at the source, modify the *{PMDB_HOME}/adminServer/webapps/BSMRApp /tableExclusion.prp* file.
Reports Impacted	Indicates the number of reports impacted by data gaps in the corresponding content pack. You can click to view the names of the reports impacted and launch them.
Facts Affected	Indicates the number of fact tables impacted by data gaps in the corresponding content pack. You can click and launch a new pane to drill down for details.

Content Pack Component Name: Fact Details

Field	Description
Fact	Shows a list of affected hourly and daily fact tables.
Row Count	Total number of rows currently in the fact table.

Field	Description
Last Updated	The time stamp when data was last loaded to the fact table.
	By default, the caution status (⚠) is indicated if:
	• Hourly tables have not been updated for 6 hours.
	• Daily tables have not been updated for 24 hours.
	You can configure the default period by changing the values in the `latency.prp` file located at *{PMDB_HOME}\adminServer\BSMRApp*.
Fact/Dimension	Ratio of the number of dimensions that have fact data against the total number of dimensions in tables.
	You can click and launch a new pane to view the dimensions or CIs that have not logged data.
	This ratio is assigned a default threshold value of 90%. So, when more than 10% dimensions do not have fact data, the caution status (⚠) is displayed. You can configure the threshold values in the `threshold.prp` file located at *{PMDB_HOME}\adminServer\BSMRApp*.
Primary Dimension	The primary dimension associated with the fact table.
Reports Impacted	Indicates the number of reports impacted by data gaps in the corresponding content pack.
	You can click to view the names of the reports impacted and launch them.

For more information on troubleshooting data gaps in SHR reports, see section, "*Troubleshooting Reporting Issues*" in the *HP Service Health Reporter Troubleshooting Guide*.

Data Processing

You can use the Data Processing page to monitor the workflow processes that move data to the data store. You can monitor the status of the job streams of each installed Content Pack component. You can also use this page to view historical execution trends and variations of workload or focus on operational data about the job streams.
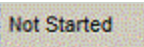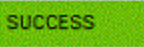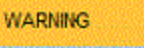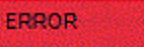
The Data Processing page includes:

Stream Details tab

The Stream Details tab includes:

Field	Description
Content Pack Component name	Name of the Content Pack component.
Number of Streams	Total number of job streams. This value indicates the number of streams that are currently running, or the number of streams that are loaded for execution, or the number of streams that completed in the last run.
Stream Status Details	Status of the job stream which can be one among the following: • OK—The number of job streams that completed successfully. • Warning—The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream. • Error—The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved. • Total—The total number of streams that are running.

Stream Detail for Content Pack

Field	Description
Stream Name	Name of the job stream.
Step Status (Completed/Total)	Status of the job stem in the stream. Completed indicates the number of steps in the job stream that have completed irrespective of whether it was successful or generated a warning or error. Total indicates the total number of job steps in the stream.
Step Status	Status of the job step execution: **Not Started** indicates that the job stream has not started running but has been loaded for execution. **SUCCESS** indicates that all job steps in the stream completed successfully. **WARNING** indicates that some job steps completed with warnings. **ERROR** indicates that a job step in the stream failed to complete and generated an error.
Start Time	Local time when the execution of the job step started.

To view a diagrammatic representation of the job stream, in the **Start Time** column, click a specific Start Time hyperlink.The **Stream Details** diagram opens which displays the execution flow and status of the job steps. Click a job step icon in the diagram to open a detailed message box about that job step.

Step Detail for Job Step

Field	Description
Step name	The name of the job step.
Process Id	The unique identifier for the job step.
State	The state of the job step. The options include: • FINISHED—indicates that the job step finished running. • WAITING—indicates that the job step is waiting to be run. • RUNNING—indicates that the job step is currently running.
Status	Status of the job step. The options are: • SUCCESS—indicates that the job step execution was successful. • WARNING—indicates that the job step completed but generated a warning. • ERROR—indicates that the job step failed to complete and generated an error. • MAX_EXEC_TIME_EXCEEDED—indicates that the job step failed to complete within the defined execution timeframe. • WAITING—indicates that the job step in currently in the waiting state because the preceding job step is yet to complete.
Detail Message	Displays the execution log of the job step with detailed information on how the warning or error was generated during the execution of the job step. An experienced user can also obtain all the necessary details related to the stream execution status by looking at the relevant dictionary and run-time tables.
Log File	The name of the log file where information about the job step process is logged.
Command	The command that was used to run the job step.
Max Retries	Maximum number of retries for the job step. This field only appears for job steps with error or warning states.

Field	Description
Remaining Retries	The number of remaining retries. This field only appears for job steps with error or warning states.
Max Execution Time (Mins)	Maximum execution time, in minutes, for the job step. This field only appears for job steps with error or warning states.
Start Time	Time when the execution of the job step started.
End Time	Time when the execution of the job step ended.
Audit Details	A summarized view of the data audit information for the job step. The information can include the number of files or rows that were processed, passed, and failed and the time taken for the audit step.

Historical Stream Overview tab

The Historical Stream Overview tab includes:

Field	Description
Stream Detail	Option to display the list of job stream that ran during a specified period. The options include: • Last 1 day • Last 7 days **Note**: The workflow framework stores information about the job steps in run-time tables for a maximum period of 7 days, after which the data is automatically purged by the PMDB Platform IM Service.
Content Pack Component name	Name of the Content Pack component.
Number of Streams	Total number of job streams that ran during the specified period of time.

Field	Description
Stream Status Details	Status of the job stream which can be one among the following: • OK—The number of job streams that completed successfully. • Warning—The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream. • Error—The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved. • Total—The total number of streams that are running.

Stream Detail for Content Pack Component

Field	Description
Stream name	Name of the job stream.
Stream Status Details	Status of the job stream which can be one among the following: • OK—The number of job streams that completed successfully. • Warning—The number of job streams that completed with warnings. These warnings do not hinder the execution of the remaining job steps in the stream. • Error—The number of job streams that failed to complete. This stops the entire job stream from running until the error is resolved. • Total—The total number of streams that are running.

Historical Stream Details tab

Field	Description
CP	Name of the Content Pack component the stream belongs to.
Stream	Name of the job stream.

Field	Description
Severity	The severity option to generate the graph for. The options include: • WARNING—displays the number of warning states encountered by the job stream during its execution. • ERROR—displays the number of error states encountered by the job stream during its execution.
State	Execution state of the job stream. The options include: • ALL—all states of the job stream. • FINISHED—state where the job stream completed successfully irrespective of the warning or error encountered during its execution. • ABORTED—state where the execution of the job stream was aborted by the user because of a job step error.
Graph	A graphical representation of the number of errors or warnings encountered by a job stream over a period of time.

Use the Data Processing page to:

- View the number of active data streams

- View the historical stream details

- View the historical trend of the streams

Database Monitoring

You can use the Database Monitoring page to view a detailed status of the health and availability of SHR database. This page displays details about the availability of the database for the past one day and for the past seven days. You can also view information about the database, the database space usage, current activities performed by the database, and the physical memory usage trends. Monitoring the SHR host database helps you to identify potential database performance problems and resolve those problems quickly and efficiently.

The Database Monitoring page includes:

Database Information

Field	Description
Status	Connection status of the SHR database:
	• ⬆ indicates that the connection to the database has been successfully established.
	• ⬇ indicates that there is no connection to the database.
Host Name	Name or IP address of the database server.
Port	Port number to query the database.
Version	Version number of the database.
Database type	Type of the SHR database.
Platform Detail	Operating system installed on the platform that is hosting the SHR database.
Multiplexed	Multiplexing capability of the database is enabled or not.
Database Size	Size of the database main store in megabytes.
PageSize	Amount of memory allocated for storing database entries.
Last Backup Time	Time at which the database instance was last backed up.
Last Full Backup Time	Time when a full backup was performed on the database.
Last Started	Time at which the database service was last started.
Last DB Polled	Time at which the database was last polled.

Database Availability

Field	Description
Database Availability	Percentage of time the database was available in the:
	• Last 7 days
	• Last 1 day
	Legend description:
	● indicates the amount of time, in hours, the database was available.
	● indicates the time, in hours, the database was not available.

DBSpace Usage

Field	Description
DBSpace Usage	Graphical representation of the database space, in megabytes, divided between the following dbspaces: • IQ_System_Main: The IQ_System_Main dbspace is created at database creation. IQ_SYSTEM_MAIN is a special dbspace that contains structures necessary for the database to open such as the IQ checkpoint log, IQ rollforward/rollback data for each committed transaction and each active checkpointed transaction, the incremental backup metadata, and database space and identity metadata. IQ_SYSTEM_MAIN is always online when the database is open. • IQ_System_Temp: The IQ_System_Temp is a single dbspace for the IQ temporary store created when you create a database. It stores the temporary database files. • PMDB_User_Main: This is the user main dbspace that is used for storing user-defined tables, indexes, and table metadata that is specific to SHR data. **Legend description**: ■ indicates reserved space, which is used for storing certain small but critical data structures used during release savepoint, commit, and checkpoint operations. ■ indicates used space, which is used for storing the main user tables and indexes. ■ indicates free space, which is the space available for use.

DBSpace Fill Details

Field	Description
DBSpace Usage	Graphical representation of the database space, in megabytes, used by the selected store over a period of time; the time period includes: • Last 7 days • Last 1 day

Current Activities

Field	Description
Connection (Used/Max)	Number of active user connections to the database and the maximum number of connections the database can handle.
(%) CPU Utilization	Percentage of CPU time that is being used by all the activities in the database.
Open Transaction	Number of transactions that are currently running in the database.
Active Txn Versions	The number of active write transactions and the amount of data they created and destroyed.
Other Versions	Other database versions and the total space consumed.
Active Requests	Number of server threads currently handling a request.
IQ Threads (Used/Free)	Number of threads that are allocated to process queries and data loads and the number of threads that are not in use.
Polling	Click the ▶ icon to start current activity polling. Click the ⏹ icon to stop current activity polling.

IQ Physical Memory Trend

Field	Description
IQ Physical Memory Trend	Graphical representation of the physical memory usage of the Sybase IQ server, in megabytes, for the last one day. **Legend description**: — indicates the current physical memory usage trend. — indicates the maximum physical memory usage trend.

Use the Database Monitoring page to view the database details.

Platform

The Platform page provides a detailed status of the health and availability of the Administration Console's application server.

The Platform page includes:

Application Server Information

Field	Description
Host Name	Name of the Administration Console application server.
Port	Port number to query the Administration Console application server.
Host OS	Operating system installed on the application server.
Server Type	Type of application server.
Virtual Machine Name	Name of the application server host virtual machine.
Virtual Machine Version	Version number of the application server host virtual machine.
Virtual Machine Vendor	Provider of the host virtual machine.

Application Server Availability

Field	Description
Application Server Availability	Graphical representation of the time the application server was available in the: • Last 7 days • Last 1 day **Legend description**: ● indicates the time, in hours, the server was available. ● indicates the time, in hours, the server was not available.

Latest (%) Heap Memory Usage

Field	Description
Latest (%) Heap Memory Usage	Graphical representation of the percentage of heap memory usage. **Legend description**: ● indicates that the heap memory usage is within the critical limits. ● indicates that the heap memory usage is outside the critical limits.

Latest (%) NonHeap Memory Usage

Field	Description
Latest (%) NonHeap Memory Usage	Graphical representation of the percentage of non-heap memory usage. **Legend description**: 🔵 indicates that the non-heap memory usage is within the critical limits. 🟠 indicates that the non-heap memory usage is outside the critical limits.

Memory Usage

Field	Description
Memory Type	Type of memory used, heap or non-heap.
Memory Usage	Maximum available memory and a graphical representation of the amount of Heap and Non-Heap memory used, in megabytes, by the application server in the: • Last 7 Days • Last 1 Day

Latest (%) CPU Utilization

Field	Description
Latest (%) CPU Utilization	Graphical representation of the percentage of CPU utilization. **Legend description**: 🔵 indicates that the CPU utilization is within the critical limits. 🟠 indicates that the CPU utilization usage is outside the critical limits.

CPU Usage

Field	Description
CPU Usage	Graphical representation of the percentage of CPU used by the application server in the: • Last 7 Days • Last 1 Day

Use the Platform page to view the application server details.

About SHR

This page displays the details about the PMDB Platform.

The About page includes:

Field	Description
Version	The version number of the product.
Build Number	The build number of the product.

Reference Information

This section provides reference information of key command line utilities provided by SHR.

abcImportDef

This module is responsible for importing/updating/deleting the stream definition of streams as designed by the Content Pack developer into management database for execution. Importing of stream definitions takes place during the Content Pack installation.

Log File	{PMDB_HOME}/log/dw_abclauncher.log
Usage	abcimportdef [-help] [-verbose] [-xmlfile <xmlfile>] [-xmlfile <xmlfile> -delete]
Options	• delete - delete stream • help - print this help message • verbose - verbose output • xmlfile - load the XML file into the metadata repository • returns - 0 for success 1 for success with warning(s) >1 for error(s)

abcLoadNRun

This module is responsible for loading and executing the streams that are already imported in the management database. This module is invoked through the *SHR Timer Server* and scheduling information can be found in {PMDB_HOME}/lib/trendtimer.sched.

The stream has to be loaded before it is subjected for execution. The streams are loaded in every 12 minutes. Execution of steps within the stream takes place once in every 3 minutes.

Stream with 4 steps, once loaded, are not guaranteed to complete in 12 minutes Following are the defaults for each type of step.

COLLECT_PROC	10
TRANSFORM_PROC	10

RECONCILE_PROC	10
STAGE_PROC	10
LOAD_PROC	15
AGGREGATE_PROC	10
EXEC_PROC_PROC	10

This indicates that, by default, only 15 LOADER steps can run in parallel. If there are more than 15 LOADERs that are eligible to run at a given point, the rest of the loaders are skipped in the current cycle.

Usage	
For loading the streams for execution	• abcloadNrun -loadBatch -streamId <streamId> • abcloadNrun -loadBatch -streamId <streamId> -forceLoad • abcloadNrun -loadBatch -allStreams • abcloadNrun -loadBatch -allStreams –forceLoad
For executing the loaded stream	• abcloadNrun -runSteps • abcloadNrun -runStream -streamId <streamId> • abcloadNrun -runStream -streamId <streamId> -stepId <stepId>
streamId	The business name for the stream
stepId	The business name for the step with the stream

collect

This module is responsible for moving data from `{PMDB_HOME}/collect` directory to `{PMDB_HOME}/stage` directory. This does merging of files with same type and category into a single file of configurable size (Default 25MB), unless there are left over files from the previous cycle. This identifies the batch of data, which the streams picks up for processing.

Source Directory	{PMDB_HOME}/collect
Destination Directory	{PMDB_HOME}/stage
Failure Directory	None, files are left in the {PMDB_HOME}/collect folder
Log File	{PMDB_HOME}/log/collectStep.log

Usage	collect [-category *<category>*] [-type *<type>*]
	• category - Specify the category of the collected data
	• type -Specify the type of the collected data
	• help - Provides Help message

Collection_Config

This module is responsible for importing/updating/deleting the ETL artifacts. ETL artifacts that are imported by collection_config are:

• Collection policies [PA, CMDB, SN, DB]

• Transformation Rules

• Reconciliation Rules

The imported rules are stored in the PostGreSQL management database. A cached copy of these policies is stored in the `{PMDB_HOME}/etl_rules` folder. All SHR ETL modules use rules from this cached folder instead of connecting to PostGreSQL.

Every time the collection_config module is executed, the cached copy is refreshed.

Usage
• collection_config -collect <Full path to collection policy xml file name> -cp <contentpack name>
• collection_config -transform <Full path to transformation policy xml file name> -cp <contentpack name>
• collection_config -reconcile <Full path to reconciliation policy xml file name> -cp <contentpack name>
• collection_config -delete -cp <contentpackName>
• collection_config -refreshCache -transformRules
• collection_config -refreshCache –reconcileRules

Mapper

This module is responsible for transforming the data and preparing it for loading to staging area. This module supports different types of transformation functions like, string functions, arithmetic functions, duplicate removal functions, pivot transfer functions and so on. These transformation function on the input data is defined by the content pack developer and imported during content pack installation.

Source Directory	{PMDB_HOME}/stage
Destination Directory	{PMDB_HOME}/stage
Failure Directory	{PMDB_HOME}/failed_to_transform
Log File	{PMDB_HOME}/log/mapperStep.log
Usage	mapper [-category <category>] [-type <type>] [stepid <id>] • category - Specify the category of the collected data • type -Specify the type of the collected data • stepId <step ID> - Specify the step id. Uses this argument to build the output file name • help - Provides Help message

Stage

This module is responsible for loading the collected, transformed and reconciled data to staging tables. The stage module is driven by stage rules that specifies how to move data from source CSV to stage tables. All the *Rate* and *dimension* in SHR has corresponding stage table. No summarization tables will have an associated stage table. Stage table name will generally be rate/dimension table name followed by an _. If the DWH table name is *SR_SM_NODE_RES*, then the stage table name for this DWH table will be *SR_SM_NODE_RES_*.

Staging involves following two modes of execution,

1. Compiling the stage rules

   In this mode, Stage module compiles and generates the compiled stage based on input stage rules designed by the content pack developer. The stage rule compilation occurs as part of content pack installation.

   Compiled stage rules are stored in {PMDB_HOME}/stagerules folder and the XML equivalent to this compiled stage rules is stored in {PMDB_HOME}/stagerules_source folder.

2. Executing the data load from CSV to stage table.

   In this mode, Stage modules takes the input as compiled stage rule and moves the data from the CSV file to stage table. The information on the CSV file patterns to be picked and the stage table to load the data, is mentioned in the compiled stage rule.

   There is some amount of processing that happens in the staging area. Important one is to perform column merge across different fact CSV's and move the resultant data to stage table.

Source Directory	{PMDB_HOME}/stage
Destination Directory	{PMDB_HOME}/stage/archive
Failure Directory	{PMDB_HOME}/failed_to_stage
Log File	{PMDB_HOME}/log/stage.log
Usage	
To Compile Stage Rule	- compile=true [To invoke compilation mode. Default is false.] - stagerule=<Stage Rule> [Full path to the file that has stage definitions] - interface=<Interface XML> [Full path to the stage interface XML] - outputLocation=<Output Directory> [Directory where the compiled stage rule is stored]
To Execute Stage table loading	- config=<Compiled Stage Rule> [Path to the compiled stage rule] - printSourceFile=true [Generated XML version of compiled stage rule. Provides mapping between CSV columns and stage table columns. Default value is false] - debugOutputLoc= <Folderpath> [Location where the XML equivalent of compiled stage rule is placed]

Reconcile

Reconciliation is a two-step process for checking the performance metrics and their dimensions discovered from topology sources. This involves:

1. Building Registry

   This process involves building a registry for reconciliation. This registry has a key and a value for each dimension discovered from a topology source. The key is the concatenated business key and value is the global unique identifier. The rule specifies the column to be used for building the keys from the dimension CSVs.

2. Reconciliation of the performance metrics

   This process is responsible for associating the global unique identifier with a dimension. This is governed by the reconciliation rules, which define the reconciliation registry to be used for the type

and category of data. This also defines the CSV columns from the collected data that can be used to build a key, to look into the reconciliation registry of the identified type, and get its matching global unique identifier.

Source Directory	{PMDB_HOME}/stage
Destination Directory	{PMDB_HOME}/stage
Failure Directory	{PMDB_HOME}/failed_to_reconcile
Log File	{PMDB_HOME}/log/reconcileStep.log
Usage	reconcile buildRegistry [-category <category] [-type <type>] [-stepid <step ID>] • buildRegistry - Build the registry • category -Specify the category of the collected data • type - Specify the type of the collected data • stepId <step ID> - Specify the step id. Uses this argument to build the output file name • help - Provides Help message

datapipe_manager

This module is responsible for creating/dropping the data warehouse tables in Sybase IQ. Along with creating or dropping table, the utility registers or deregisters the tables in the metadata maintained by SHR.

This module will be generally invoked for creating/dropping tables for Content Pack installation and uninstallation activities.

> **Note:** Stage tables are not part of data warehouse tables, and therefore, are not created or dropped by the Content Pack installation/uninstallation process.

Log File	• {PMDB_HOME}/log/trend.log
Usage1:To Create a table	• datapipe_manager -p create -a <path_to_ schema_definition_file> -d <debug_level>
Usage2:To Drop a table	• datapipe_manager -p delete -t <table> -d <debug_level>

p [create|delete]	*create* for creating table and *delete* for deleting a table
a	Full path to schema definition file. This file has a property format called as TEEL and is created by CDE by reading the model XML,
d	Level of debugging information to be generated. The data is logged to trend.log. Supported debug logging levels are 1, 2, 3.
t	The name of the table to be dropped.

Appendix

Parameters in the Config.prp file

The following table lists the `config.prp` parameters.

Parameters	Business Objects CMS Server Details
#Fully qualified hostname of the system that is running the SAP BO component for SHR	bo.cms = bohost
#Port number where the SAP BO is listening for connections	bo.cms.port = 6400
#Port number where the SAP BO InfoViewApp web application is running	bo.infoview.port = 8080
#Authentication type for logging in to BO and subsequently SHR Admin console as well **Note:** Supported options – Enterprise and Group based	bo.authType = secEnterprise
#Parameters that enable trusted authentication in SAP BO **Note:** These get updated when setting up CAC	bo.trusted.auth.enable = false bo.trusted.auth.shared.secret =
#SAP BO install location	bo.install.path=C:/Program Files (x86)/Business Objects/
#Parameters for logging errors from SHR logs to Sybase DB **Note:** Not enabled by default	dblogger.backupthreadruntime=60000 dblogger.buffersize=5
#Host and port details where Java messaging service is to be run **Note:** Deprecated in SHR 9.40	jms.host=localhost jms.port=21401

Parameters	Business Objects CMS Server Details
#Port where JMX beans from SHR are accessible via HTTP	jmx.port=21422
# Abc_ DataServicesWSMaxTimeToLaunch=60	BSMR_ABC_Version=0.16.5
#Port details where Tomcat Mbeans are exposed	tomcat.jmx.port=21416
#Default logger class for SHR modules	logger.classname=com.hp.bto.bsmr.util.logger.BsmrLoggerFactory
#default Image source for SHR admin console	DefaultImageSource=svcgen.32.gif
#Image size	GeneratedImageWidth=1035 GeneratedImageHeight=400
#Is BSM installed - Deprecated	bsm.install=false
# Indicate SHR installation. Value=Enterprise – SHR installation ,Value=headless SHR installation	SHR.install=Enterprise
#OS architecture for SHR	pmdb.os.platform=64
#Sybase IQ dbisql and bin (executable) path	sybase.dbisql.path=IQ-15_4 sybase.bin.path=IQ-15_4
#Name of DWH DB JDBC driver	database.driver.name=SQL Anywhere 12
#connection details for ABC - deprecated	abc.db.host=localhost abc.db.instance=dwabc abc.db.port=3699 abc.db.type=sybaseiq abc.db.pmdb.user=dwabc abc.db.pmdb.user.pwd=dwabc

Parameters	Business Objects CMS Server Details
#DWH DB connection details (Sybase IQ)	database.type=sybase database.port=21424 database.sybase.engine=databaseEngine database.host=databaseHost database.dsn=BSMR
#start/stop script by bsm, relative to PMDB home	bsm.start.script=bin/hp_bsm_pmdb_start bsm.stop.script=bin/hp_bsm_pmdb_stop
#Management DB connection details (PostgreSQL)	management.db.type=postgres management.db.driver=org.postgresql.Driver management.db.hostname = localhost management.db.port=21425 management.db.dialect=org.hibernate.dialect.PostgreSQLDialect
#property to specify distributed collection – deprecated	collection.distributed.mode = false
#Log level for loader.log	loader.debug.level=INFO
#Log level for aggregate.log	aggregate.debug.level=INFO aggregate.daily.interval=6
#Log level for runProc command	runProc.debug.level=INFO
#Name of the 64 bit DSN created to connect to Sybase IQ database from SHR	database.dsn64=SHRDB
# ADDED FOR SIS GROUP NAME	SISGroupName=SIS
# ADDED FOR COLLECTION MAX HISTORY AND INITIAL HISTORY SUPPORT	collector.maxHistory=360 collector.initHistory=360
# ADDED FOR DBCOLLECTOR MAX HISTORY AND INITIAL HISTORY SUPPORT	dbcollector.maxHistory=360 dbcollector.initHistory=360
#Host and port details where Collection MBeans are enabled	collection.host = localhost collection.jmx.port = 21409

Parameters	Business Objects CMS Server Details
#default frequency in minutes with which a newly discovered HP Operations agent source will be configured for collection	pa.frequency=60
#Number of hours of data a file is kept since its arrival in `{PMDB.HOME}` `/stage/archive` folder **Note:** Any file older than this period will be deleted	stage.archive.retention.period=48
#character encoding system for SHR	characterset=UTF8
#IM Threshold for Diskspace **Note:** Deprecated for SHR 9.40	im.disk.space.errorLimit=5 im.disk.space.warnLimit=15
#view name that is used for querying during test connection to RTSM configured	default.cmdb.view = Oracle
#ADDED FOR DEFAULT AGGREATE.BATCHSIZE	aggregate.batchsize=20000000
#default stage batch size	stage.batchsize=10000000
#default loader batch size	loader.batchsize=10000000
# min and max value used by Internal monitoring to generate database alert.	dbspace.min.percentage=70 dbspace.max.percentage=85 stage.backup.failedRows=false
#Added for enabling SSL	bo.protocol=http bo.ssl.enabled.port=8443 shr.admin.ui.port=21412
#Added for downtimeutility	downtimedays=7
#Added for chain of authentication, you have to update this property by appending comma separated value	shr.auth.classes=com.hp.bto.bsmr.security.auth.BOAuthenticator

Parameters	Business Objects CMS Server Details
#property to indicate whether any remote collectors are configured or not **Note:** Will change to true automatically on configuring the first remote collector	remote.poller.is.enabled=false
#Added for CAC authentication, needs to have a value certbased for CAC authentication and default otherwise	shr.loginMethod=default
#URL for the web service that is to be queried in case of RTSM collection	ucmdbservice.url=/axis2/services/UcmdbService
#Maximum number of retries attempted to acquire a connection to SHR management DB (PostgreSQL) before exiting with error	management.db.connection.retry=3
#Number of milliseconds to check that connection to SHR management DB held in the pool is not stale and in case it is, refresh the same	management.db.connection.check.interval=30000
#User group on BO used SHR authentication	shr.user.groups=administrators
#Minimum CPU and Memory requirements for various deployment configurations (low, medium and high)	low_volume_cpu_number=4 low_volume_ram_size=8 medium_volume_cpu_number=8 medium_volume_ram_size=16 high_volume_cpu_number=32 high_volume_ram_size=64
#Parameter to indicate whether this is a remote BO setup or not **Note:** Updated by SHR installer based on the features selected for installation on the system	isRemoteBO=false

Changing Default Passwords

This section guides you to change the default passwords for the following:

Administration Console log on password

Sybase IQ database password

Management database password

SAP BusinessObjects database password

Administration Console Log on Password

If you want to change the password for the default Administrator user name, perform the following steps:

1. Access the SAP BusinessObjects Central Management Console (CMC).

2. On the Central Management Console log on screen, in the **User Name** field, type `Administrator`.

3. Click **Log On**. The CMC Home screen opens.

4. Click **Users and Groups**. The Users and Groups screen opens.

5. On the right pane, double-click **Administrators**.

6. Right-click **Administrator** and then click **Properties**. The Properties:Administrator dialog box opens.

7. Under **Enterprise Password Settings**, in the **Password** field, type a new password.

8. In the **Confirm** field, retype the password to confirm it. You can change the Administrator user name, if required, and specify other necessary details on this screen.

9. Click **Save & Close** to accept the changes.

10. Click **Log Out** to exit the Central Management Console.

Note: This task is valid only if SHR is installed on the system.

Sybase IQ Database Password

If you want to change the password for the default Sybase IQ database administrator user through Administration Console, perform the following steps:

1. In the Administration Console, click **Administration > System Configuration**.
   The System Configuration page opens.

2. Click **Reset Password**.
   The Reset Password dialog box opens.

3. In the **Reset Password** dialog box, type the database password details:

Field	Description
Old Password	Enter the existing database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value and less than 25 characters in length.
Confirm New Password	Retype the new password for confirmation purposes.

4. Click **OK**.
   A `Password Successfully Changed` message appears in the Information message panel indicating that the password has been successfully changed.

Change Password for SybaseIQ Database User (dba)

Sybase IQ includes a database called the utility database (utility_db). The utility_db has no physical representation. There is no database file or any data contained in this database. The utility database runs on any Sybase IQ server.

To change the default password of the "dba" user in the "utility_db" database, follow these steps:

1. Take a backup of `util_db.ini` in the following location:

   Windows: %PMDB_HOME%\..\Sybase\IQ-15_4\Bin64

   Linux: $PMDB_HOME/../Sybase/IQ-15_4/bin64

2. Create a file `new.ini` in the same directory.

3. Add the following lines in the `new.ini` file:

   [UTILITY_DB]

   PWD=test

   where, `test` is the new password for the "dba" user.

4. Save and close the file in above format.

5. Run the following command to encrypt the password:

   Windows: %PMDB_HOME%\..\Sybase\IQ-15_4\Bin64\dbfhide new.ini util_db.ini

   Linux: $PMDB_HOME/../Sybase/IQ-15_4/bin64/dbfhide new.ini util_db.ini

The `util_db.ini` will have the encrypted password.

6. Run the following command to verify the new password by connecting to the utility_db:

   `dbisql -nogui -c "uid=dba;pwd=test;dbn=utility_db;eng=<short_hostname>"`

   where, `<short_hostname>` is the short hostname of the database server.

   You can delete the `new.ini` file.

> **Note:** You may need to use the "utility_db" database if Sybase datafiles of PMDB database in SHR needs to be migrated to another location/server and hence it is advised to note or remember the exact changed password safely.

Management Database Password

To change default password for PostgreSQL database administrator - *postgres* user:

Perform the following steps to change the password for the default PostgreSQL database administrator user:

Windows:

1. Go to

   Windows 2008: Start > All Programs > Administrative Tools > Computer Management.

   Windows 2012: Start > Administrative Tools > Computer Management.

   The Computer Management page appears.

2. Go to **System tools > Local Users and Groups > Users**.

3. Right-click **postgres** and click **Set Password**.

   A warning message appears.

4. Click **Proceed**. The **Set Password for postgres** appears.

5. Type the new password in the **New Password**. Retype the password in **Confirm password** for confirmation purpose.

6. Click **OK**.

4. Open the services window.

5. Right-click on HP_PMDB_Platform_PostgreSQL and select **Properties**.

   The HP_PMDB_Platform_PostgreSQL Properties page appears.

6. Click the Log On tab.

7. Provide the password provided in step 5 and retype it to confirm the same.

8. Click **OK**.

Linux:

1. Log on to the command line console.

2. Run the following command:

   ```
   passwd postgres
   ```

3. Type the new password and press **Enter**.

To change default password for *Postgres - pmdb_admin* user:

If you want to change the password for the default Management database user, perform the following steps:

1. In the Administration Console, click **Administration > System Configuration**.
   The System Configuration page appears.

2. On the **Management Database Configuration** tab, click **Reset Password**.
   The Reset Password dialog box appears.

3. In the **Reset Password** dialog box, type the database password details:

Field	Description
Old Password	Enter the existing management database administrator password.
New Password	Enter a new password. The password should be an alphanumeric value and less than 25 characters in length.
Confirm New Password	Retype the new password for confirmation purposes.

4. Click **OK**.
   A `Password Successfully Changed` message appears in the Information message panel indicating that the password has been successfully changed.

SAP BusinessObjects Database Password

SHR is installed with a default SAP BusinessObjects database password. Perform this task to change the default SAP BusinessObjects database password.

After installing SHR, follow these steps to modify the default password of the database embedded with SAP BusinessObjects:

For Windows:

1. Go to `<BusinessObejcts installed drive>:\Program Files (x86)\Business Objects\SQLAnyWhere12\bin`

2. Open the `dbisqlc` application.

3. Type the credentials as follows:

   User name = DBA.

   Password = pmdb_admin.

   Server name = BOE120SQLAW_<shrshorthostname>.

   Database name = BOE120.

4. Run the following command in the sql window:

   ALTER USER *<shrshorthostname>* **IDENTIFIED BY** *<new password>***;**

   ALTER USER DBA **IDENTIFIED BY** *<new password>***;**

5. Repeat the same steps for database BOE120_AUDIT.

After updating the password, follow these steps:

1. Go to CCM from **Start > All Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Configuration Manager**

2. Stop the Server Intelligence Agent (SIA); right-click and select **Properties**.

3. Go to the **Configuration** tab, you may see a error pop up click **OK** to proceed, and then click **Specify** of BOE120.

4. Click on the **Update Data Source Settings** .

5. Click **OK**.

6. Select **SQL Anywhere (ODBC)** and click **OK**.

7. The Select Datasource window appears. Select **Machine Data Source** tab.

8. Double-click DSN **BOE120** and provide the password that was changed and click **OK**.

9. Repeat from step 3 to 8 for BOE120_AUDIT database by selecting the **BOE120_AUDIT**.

10. Start the SIA.

To check if the password is modified, log in to the database using the new password.

SHR is installed with a default SAP BusinessObjects database password. Perform this task to change the default SAP BusinessObjects database password.

For Linux:

1. Log in to the system as root.

2. Run the following command to switch to SHRBOADMIN user:

   `su - SHRBOADMIN`

3. Go to `/opt/HP/BSM/BO/bobje/SQLAW/Bin/`.

4. Run the following command:

   `source /opt/HP/BSM/BO/bobje/setup/env.sh`

5. Run the following command:

   `./dbisqlc`

   The credentials window appears. Click **Cancel**.

6. Select **Command** tab, and then click **Connect...**. The Connect credentials window appears.

7. Type the following details:

   a. USER ID = DBA.

   b. Password = pmdb_admin.

   c. Database Name = <shrshorthostname>BOE120.

   d. Server = <shrshorthostname>BOE120_SHR.

8. Run the following command in the sql window:

   ALTER USER SHR **IDENTIFIED BY** *<new password>***;**

   ALTER USER DBA **IDENTIFIED BY** *<new password>***;**

9. To modify the default password for BOE120_AUDIT, from Menu, click **Command** tab, and then

click **Connect…**.

10. Type the following details:

    a. USER ID = DBA.

    b. Password = pmdb_admin.

    c. Database Name = <shrshorthostname>BOE120_AUDIT.

    d. Server = <shrshorthostname>BOE120_SHR.

11. Run the following command in the sql window:

    ALTER USER SHR **IDENTIFIED BY** *<new password>***;**

    ALTER USER DBA **IDENTIFIED BY** *<new password>***;**

After updating the password, follow these steps:

For BOE120 perform the following:

1. Go to `/opt/HP/BSM/BO/bobje`.

2. Run the following command:

   `./cmsdbsetup.sh`

3. Provide the SIA name as *PRD_SHR* and click on Enter.

4. The prompt shows stop SIA. Type *yes*, and then click on Enter.

5. The prompt asks you to update. Type *update*, and then click on Enter.

6. Type *yes* and click Enter.

7. Select *SQL Anywhere* or Type 2, and then click on Enter.

8. Type DSN as<shrshorthostname>BOE120, and then click on Enter.

9. Type user as SHR, and then click on Enter.

10. Type the new password, which you changed recently, and then click on Enter.

11. Run the following command:

    `./startservers`

For BOE120_AUDIT perform the following:

1. Go to `/opt/HP/BSM/BO/bobje`.

2. Run the following command:

   `./cmsdbsetup.sh`

3. Provide the SIA name as *PRD_SHR* and click on Enter.

4. The prompt shows stop SIA. Type *yes*, and then click on Enter.

5. Select *selectaudit* option, and then click Enter.

6. If you want to enable the Audit option Type *yes* in the command line.

   You can type *No* if you do not want to enable Audit now and want to enable the Audit at a later point of time.

7. Select *SQL Anywhere* or Type 2, and then click on Enter.

8. Type the DSN as <shrshorthostname>BOE120_AUDIT.

9. Type user as SHR, and then click on Enter.

10. Type the new password, which you changed recently, and then click on Enter.

11. Run the following command:

    `./startservers`

To check if the password is modified, log in to the database using the new password.

The new password must be updated in the *BobjEnterprise120* script that contains the default password. Perform the following steps:

1. Go to the location `/etc/init.d`

2. In the *BobjEnterprise120* script go to the following line:

   `$SU - "$BOBJEUSERNAME" -c "$BOBJEDIR/sawstop.sh DATABASEUID=SHR DATABASEPWD=pmdb_admin"`

3. Type the new password in place of `pmdb_admin`.

Integrating with Data Sources for HP Operations Smart Plug-ins

To show reports on the data collected from different enterprise applications, SHR relies on the metrics collected by collectors of HP Operations Smart Plug-ins (SPIs). SPI collectors store the data into the

data store provided by the HP Operations agent. SHR's integration with SPI data sources facilitate transfer of data from HP Operations agent's data store to SHR's database.

This integration is established when you deploy SHR in the HPOM deployment scenario.

SHR provides performance reports for the following enterprise applications:

- Microsoft Active Directory

- Microsoft Exchange 2007

- Microsoft Exchange 2010

- Microsoft SQL Server

- Oracle Database

- Oracle WebLogic Server

- IBM WebSphere Application Server

Working of the Integration

1. Installation and configuration of a SPI ensures that necessary instrumentation, scripts, programs, and policies are transferred to a node where the application is running and the HP Operations agent is already installed.

   > **Tip:** For successful installation and configuration of SPIs, follow the SPI documentation.

2. SPI collectors start collecting data on the node based on rules and specifications available with the policies deployed on the node.

3. SPI stores the collected data into HP Operations agent's data store. Each SPI creates at least one *data source* in agent's data store.

4. After configuring SHR to collect data from a data source and installing Content Packs, SHR starts collecting historical data from agent's data store.

   > **Tip:** Procedures to configure SHR to collect data from the SPI data sources and installing Content Packs are available in the *SHR Configuration Guide*.

Prerequisites for Generating SHR Reports from the HP Operations SPIs Data

Ensure the following prerequisites are met before integrating SHR with HP Operations SPIs. Otherwise, blank SHR reports will be generated:

- **Ensure data is logging into the HP Operations SPIs data store.**

  a. Ensure HP Operations SPIs is installed and configured. For further information on deploying and configuring HP Operations SPIs, see the reference documents mentioned for each HP Operations SPIs in individual chapters of this book.

  b. Ensure all necessary HP Operations SPIs policies are deployed correctly.

  c. Ensure HP Operations SPIs collector is logging metrics into HP Operations agent database. For details on verifying that HP Operations SPIs is logging metrics into database, see the *HP Service Health Reporter Troubleshooting Guide*.

  > **Note:** If any of the preconditions are not fulfilled by the HP Operations SPIs, SHR cannot gather the necessary information from the data source and reports will not generate.

- **Ensure SHR is configured for HP Operations SPIs data store.**

  a. Ensure the topology source (HPOM or RTSM) is configured to collect fact metrics from the data store of HP Operations SPIs. Verify this from the SHR Administration Console -> Topology Configuration -> Test Connection (which should be successful). For more information, see "*Configuring SHR*" in the *HP Service Health Reporter Configuration Guide*.

  b. Ensure the SHR Content Packs relevant to the HP Operations SPIs are installed. Verify this from the SHR Administration Console -> Administration -> Deployment Manager; you will see a column that indicates the deployment status of the content pack.

  > **Note:** If the HP Operations SPIs data store is not configured for SHR, it cannot gather the necessary information from the data source and reports will not generate.

Each SHR report uses a specific set of HP Operations SPIs metrics available in HP Operations agent's data store. Collection of metric data is governed by the HP Operations SPIs policies deployed on the node. In other words, to be able to view reports of your interest successfully, you must deploy all the prerequisite policies.

Prerequisite Policies for Oracle Database Reports

Policy Configuration Requirement: Not required; deploy the policy with default settings.

Report Name	Data Source	Data Class	SPI Policy

Database Oracle Executive Summary	DBSPI_ ORA_ REPORT	DBSPI_ ORA_ REPORT	• Scheduled task policy
			  ▪ DBSPI-Ora-05min-Reporter (for UNIX/Linux nodes)
			
			  ▪ DBSPI-Ora-05min-Reporter-NT (for Windows nodes)
			
			• Measurement threshold Policy
			
			  ▪ E201_InstUptime

Database Oracle Top 10 Instances and Tablespaces	DBSPI_ ORA_ REPORT	DBSPI_ ORA_ REPORT	• Scheduled task policy
			  ▪ DBSPI-Ora-05min-Reporter (for UNIX/Linux nodes)
			
			  ▪ DBSPI-Ora-1d-Reporter (for UNIX/Linux nodes)
			
			  ▪ DBSPI-Ora-05min-Reporter-NT (for Windows nodes)
			
			  ▪ DBSPI-Ora-1d-Reporter-NT (for Windows nodes)
			
			• Measurement threshold Policy
			
			  ▪ E201_InstUptime
			
			  ▪ E210_TblSpcSize
			
			  ▪ E212_Inst Size

Report Name	Data Source	Data Class	SPI Policy
Database Oracle Top 5 Instances Load and Efficiency	DBSPI_ ORA_ GRAPH	DBSPI_ ORA_ GRAPH	• Scheduled task policy ▪ DBSPI-Ora-05min-Favorites ▪ DBSPI-Ora-Add-Ons-05min ▪ DBSPI-Ora-05min-SQLNet ▪ DBSPI-Ora-1h-Favorites ▪ DBSPI-Ora-1h-SQLNet ▪ DBSPI-Ora-05min-Favorites • Measurement threshold Policy ▪ E021_BufferBusyPct ▪ E022_TotBufCacHitPct ▪ E039_LibCacGetHitPct ▪ E032_ REDOLGSPCREQCNT ▪ E019_SortDiskRate ▪ E020_SortMemoryPct ▪ E037_UserLogonCnt ▪ E049_USERCALLRATE

Report Name	Data Source	Data Class	SPI Policy
Database Oracle Archive Device Detail	DBSPI_ ORA_ GRAPH	DBSPI_ ORA_ GRAPH	• Scheduled task policy ■ DBSPI-Ora-15min-Favorites ■ DBSPI-Ora-05min-Favorites ■ DBSPI-Ora-05min-SQLNet ■ DBSPI-Ora-Add-Ons-15min ■ DBSPI-Ora-1h-SQLNet ■ DBSPI-Ora-Add-Ons-15min-NT (for Windows nodes) • Measurement threshold Policy ■ E058_ArchvFreeSpcPct ■ E060_RedoUnarchvdCnt ■ E062_BkgrDumpSpcePct ■ E063_TraceFileAddCnt ■ E064_UserDumpSpacPct ■ E065_CoreDumpSpacPct

Report Name	Data Source	Data Class	SPI Policy
Database Oracle Disk And Memory Sort Detail	DBSPI_ ORA_ GRAPH	DBSPI_ ORA_ GRAPH	- Scheduled task policy - DDBSPI-Ora-1h-Favorites - DBSPI-Ora-1h-SQLNet - DBSPI-Ora-Add-Ons-05min - DBSPI-Ora-05min-SQLNet - DBSPI-Ora-Add-Ons-1h - DBSPI-Ora-1h-SQLNet - DBSPI-Ora-Add-Ons-1h-NT - Measurement threshold Policy - E019_SortDiskRate - E020_SortMemoryPct - E052_SortTotalRate
Database Oracle Instance Availability Detail	DBSPI_ ORA_ REPORT	DBSPI_ ORA_ REPORT	- Scheduled task policy - DBSPI-Ora-05min-Reporter (for UNIX/Linux nodes) - DBSPI-Ora-05min-Reporter-NT (for Windows nodes) - Measurement threshold Policy - E201_InstUptime

Report Name	Data Source	Data Class	SPI Policy
Database Oracle Instance Space Utilization Detail	DBSPI_ ORA_ REPORT	DBSPI_ ORA_ REPORT	• Scheduled task policy ■ DBSPI-Ora-1d-Reporter (for UNIX/Linux nodes) ■ DBSPI-Ora-1d-Reporter-NT (for Windows nodes) • Measurement threshold Policy ■ E212_Inst Size
Database Oracle Segment Detail	DBSPI_ ORA_ GRAPH	DBSPI_ ORA_ GRAPH	• Scheduled task policy ■ DBSPI-Ora-15min-SQLNet ■ DBSPI-Ora-15min-Favorites ■ DBSPI-Ora-05min-Favorites ■ DBSPI-Ora-05min-SQLNet • Measurement threshold Policy ■ E016_SegmntExtendCnt ■ E017_SegMaxExtentCnt ■ E018_SegExtRapidCnt ■ E067_RBSegmntStatCnt

Report Name	Data Source	Data Class	SPI Policy
Database Oracle Shared Pool and Cache Performance Detail	DBSPI_ ORA_ GRAPH	DBSPI_ ORA_ GRAPH	• Scheduled task policy ■ DBSPI-Ora-05min-Favorites ■ DBSPI-Ora-Add-Ons-05min ■ DBSPI-Ora-05min-SQLNet ■ DBSPI-Ora-Add-Ons-05min-NT ■ DBSPI-Ora-05min-SQLNet • Measurement threshold Policy ■ E021_BufferBusyPct ■ E022_TotBufCacHitPct ■ E039_LibCacGetHitPct ■ E026_DictCacheHitPct ■ E040_LibCacPinHitPct ■ E045_ShrdPoolFreePct

Report Name	Data Source	Data Class	SPI Policy

Database Oracle SQL Performance Detail	DBSPI_ ORA_ GRAPH	DBSPI_ ORA_ GRAPH	• Scheduled task policy
			
			  ■ DBSPI-Ora-05min-Favorites
			
			  ■ DBSPI-Ora-05min-SQLNet
			
			  ■ DBSPI-Ora-Add-Ons-1h-NT
			
			  ■ DBSPI-Ora-1h-SQLNet
			
			  ■ DBSPI-0070
			
			  ■ DBSPI-0071
			
			  ■ DBSPI-0074
			
			  ■ DBSPI-0076
			
			• Measurement threshold Policy
			
			  ■ E030_FulLgTblScnRate
			
			  ■ E046_RowFetcByIdxPct
			
			  ■ E070_PQServrsBusyPct
			
			  ■ E071_PQSrvHighwtrPct
			
			  ■ E074_PQQueryRate
			
			  ■ E076_PQRangeScanPct

Report Name	Data Source	Data Class	SPI Policy

Database Oracle Tablespace Detail	DBSPI_ ORA_ GRAPH	DBSPI_ ORA_ GRAPH	• Scheduled task policy
			
			  ▪ DBSPI-Ora-05min-Favorites
			
			  ▪ DBSPI-Ora-05min-SQLNet
			
			  ▪ DBSPI-0006
			
			  ▪ DBSPI-Ora-1h-Favorites
			
			  ▪ DBSPI-Ora-Add-Ons-05min
			
			  ▪ DBSPI-Ora-Add-Ons-05min-NT
			
			• Measurement threshold Policy
			
			  ▪ E007_TblSpcStatusCnt
			
			  ▪ E006_TblSpFreePctCnt
			
			  ▪ E008_TSBReadRatioCnt
			
			  ▪ E004_UsersTmpDfltCnt
			
			  ▪ E005_ObjctsForignCnt
			
			  ▪ E011_TblSpcFrgmntCnt

Database Oracle Tablespace Space Utilization Detail	DBSPI_ ORA_ REPORT	DBSPI_ ORA_ REPORT	• Scheduled task policy
			
			  ▪ DBSPI-Ora-1d-Reporter (for UNIX/Linux nodes)
			
			  ▪ DBSPI-Ora-1d-Reporter-NT (for Windows nodes)
			
			• Measurement threshold Policy
			
			  ▪ E210_TblSpcSize

Prerequisite Policies for Oracle WebLogic Reports

The following table lists the Oracle WebLogic SPI policies required by each Oracle WebLogic report.

Policy Configuration Requirement: Not required; deploy the policy with default settings.

Report Name	Data Source	Data Class	Required SPI Policy
WebLogic Servlet Performance Summary	WLSSPI	WLSSPI_ METRICS	• WLSSPI_ 0011 • WLSSPI_ 0035 • WLSSPI_ 0036 • WLSSPI_ 0025 • WLSSPI_ 0026 • WLSSPI_ 0005 • WLSSPI_ 0012 • WLSSPI_ 0014 • WLSSPI_ 0061 • WLSSPI_ 0283 • WLSSPI_ 0284 • WLSSPI_ 0285 • WLSSPI_ 0286 • WLSSPI_ 0287

Report Name	Data Source	Data Class	Required SPI Policy
			• WLSSPI_ 0288
WebLogic JVM Utilization	WLSSPI	WLSSPI_ METRICS	• WLSSPI_ 0823 • WLSSPI_ 0819
WebLogic Top N Summary	WLSSPI	WLSSPI_ METRICS WLSSPI_ RPT_ METRICS	• WLSSPI_ 0011 • WLSSPI_ 0035 • WLSSPI_ 0036 • WLSSPI_ 0025 • WLSSPI_ 0026 • WLSSPI_ 0005 • WLSSPI_ 0012 • WLSSPI_ 0014 • WLSSPI_ 0061 • WLSSPI_ 0283 • WLSSPI_ 0284 • WLSSPI_ 0285 • WLSSPI_ 0286

Report Name	Data Source	Data Class	Required SPI Policy
			• WLSSPI_ 0287
			• WLSSPI_ 0288
			• WLSSPI_ 0823
			• WLSSPI_ 0819
			• WLSSPI_ 0072
			• WLSSPI_ 0073
			• WLSSPI_ 0074
			• WLSSPI_ 0075
			• WLSSPI_ 0079
			• WLSSPI_ 0263
			• WLSSPI_ 0265
			• WLSSPI_ 0238
			• WLSSPI_ 0278
			• WLSSPI_ 0251
			• WLSSPI_ 0252
			• WLSSPI_ 0253
			• WLSSPI_ 0254
			• WLSSPI_ 0224
			• WLSSPI_

Report Name	Data Source	Data Class	Required SPI Policy
WebLogic EJB Cache Hit	WLSSPI	WLSSPI_ METRICS WLSSPI_ RPT_ METRICS	
WebLogic Transaction Performance Details	WLSSPI	WLSSPI_ METRICS WLSSPI_ RPT_ METRICS	
WebLogic JDBC Connection Pool Summary	WLSSPI	WLSSPI_ RPT_ METRICS	• WLSSPI_ 0072 • WLSSPI_ 0073 • WLSSPI_ 0074 • WLSSPI_ 0075 • WLSSPI_ 0079 • WLSSPI_ 0263 • WLSSPI_ 0265 • WLSSPI_ 0238 • WLSSPI_ 0278 • WLSSPI_ 0251 • WLSSPI_ 0252 • WLSSPI_ 0253

Report Name	Data Source	Data Class	Required SPI Policy
			• WLSSPI_ 0254 • WLSSPI_ 0224
WebLogic Executive Summary	WLSSPI	WLSSPI_ RPT_ METRICS	• WLSSPI_ 0245 • WLSSPI_ 0001
WebLogic JMS Performance Details	WLSSPI	WLSSPI_ RPT_ METRICS	• WLSSPI_ 0070 • WLSSPI_ 0071 • WLSSPI_ 0240
WebLogic Server Availability Details	WLSSPI	WLSSPI_ RPT_ METRICS	• WLSSPI_ 0242 • WLSSPI_ 0260

Prerequisite Policies for Microsoft SQL Server Reports

The following table lists the Microsoft SQL Server SPI policies required by each Microsoft SQL Server report.

Note: See the SPI documentation for information on how the policies should be deployed and what additional configuration steps may be required.

Policy Configuration Requirement: Not required; deploy the policy with default settings.

Report Name	Data Source	Data Class	SPI Policy

MSSQL Database and Virtual Device Space Usage Top N	DBSPI_ MSS_ REPORT	DBSPI_ MSS_ REPORT	• Scheduled task policy
			  ■ DBSPI-MSS-1d-Reporter
			
			• Measurement threshold Policy
			
			  ■ M240_DBSize
			
			  ■ DBSPI-MSS-1h

MSSQL Performance Summary	DBSPI_ MSS_ GRAPH	DBSPI_ MSS_ GRAPH	• Scheduled task policy
			  ■ DBSPI-MSS-1d-Reporter
			
			  ■ DBSPI-MSS-05min
			
			• Measurement threshold Policy
			
			  ■ DBSPI-3001
			
			  ■ DBSPI-3025
			
			  ■ DBSPI-3013
			
			  ■ DBSPI-3009
			
			  ■ DBSPI-3008

MSSQL Table Space Usage Top N	DBSPI_ MSS_ GRAPH	DBSPI_ MSS_ GRAPH	• Scheduled task policy
			
			  ■ DBSPI-MSS-1d-Reporter
			
			• Measurement threshold Policy
			
			  ■ M241_TableSize

Report Name	Data Source	Data Class	SPI Policy

MSSQL Database Input and Output Statistics	DBSPI_ MSS_ GRAPH	DBSPI_ MSS_ GRAPH	• Scheduled task policy
			
			  ▪ DBSPI-MSS-1h
			
			• Measurement threshold Policy
			
			  ▪ DBSPI-3007
			
			  ▪ DBSPI-3008

MSSQL Database Locks Summary	DBSPI_ MSS_ GRAPH	DBSPI_ MSS_ GRAPH	• Scheduled task policy
			
			  ▪ DBSPI-MSS-1h
			
			  ▪ DBSPI-MSS-05min
			
			• Measurement threshold Policy
			
			  ▪ DBSPI-3013
			
			  ▪ DBSPI-3071
			
			  ▪ DBSPI-3070
			
			  ▪ DBSPI-3072
			
			  ▪ DBSPI-3075

Report Name	Data Source	Data Class	SPI Policy
MSSQL Database Performance Summary	DBSPI_ MSS_ GRAPH	DBSPI_ MSS_ GRAPH	• Scheduled task policy ■ DBSPI-MSS-1h • Measurement threshold Policy ■ DBSPI-3023 ■ DBSPI-3024 ■ DBSPI-3053 ■ DBSPI-3054 ■ DBSPI-3051 ■ DBSPI-3052
MSSQL Database Space Usage Details	DBSPI_ MSS_ REPORT	DBSPI_ MSS_ REPORT	• Scheduled task policy ■ DBSPI-MSS-1d-Reporter • Measurement threshold Policy ■ M240_DBSize
MSSQL Database Table Space Usage Details	DBSPI_ MSS_ REPORT	DBSPI_ MSS_ REPORT	• Scheduled task policy ■ DBSPI-MSS-1d-Reporter • Measurement threshold Policy ■ M241_DBSize

Report Name	Data Source	Data Class	SPI Policy
MSSQL Instance Availability Details	DBSPI_ MSS_ REPORT	DBSPI_ MSS_ REPORT	- Scheduled task policy - DBSPI-MSS-05min-Reporter - Measurement threshold Policy - M243_DBSize
MSSQL Server Transaction Summary	DBSPI_ MSS_ GRAPH	DBSPI_ MSS_ GRAPH	- Scheduled task policy - DBSPI-MSS-1h - Measurement threshold Policy - DBSPI-3064 - DBSPI-3066 - DBSPI-3067
MSSQL Users Connection Summary	DBSPI_ MSS_ GRAPH	DBSPI_ MSS_ GRAPH	- Scheduled task policy - DBSPI-MSS-1h - Measurement threshold Policy - M031_ NumUsersCnt - DBSPI-3032 - DBSPI-3026

Prerequisite Policies for Microsoft Exchange Server Reports

The following table lists the Microsoft Exchange SPI policies required by each Microsoft Exchange Server report.

Note: Not every policy should be deployed to every Microsoft Exchange Server node. See the SPI documentation to understand what each policy does and determine which policies are appropriate

for the role played by each server. Deploying the policies indiscriminately will result in incorrect messages originating from the node.

In addition, see the SPI documentation for information on how the policies should be deployed and what additional configuration steps may be required.

Policy Configuration Requirement: Not required; deploy the policy with default settings.

Report Name	Data Source	Data Class	Required SPI Policy
Exchange Mail Server Summary	EXSPI_ DATA	EXSPI_ MBSUMMARY	EXSPI-14X Get Mailbox IS Sum Data
		EXSPI_ PFSUMMARY	EXSPI-14X Get Public IS Sum Data
Exchange Site Executive Summary	EXSPI_ DATA	EXSPI_ AVAILABILITY	EXSPI-8X/14X Get Exchange Availability
		EXSPI_ HUBTRANSDSN	EXSPI-14X HUB Transport DSN
		EXSPI_TRANSQ	EXSPI-14X Dc Transport Queues
		EXSPI_ MBSUMMARY	EXSPI-14X Get Mailbox IS Sum Data
		EXSPI_ POP3PERF	EXSPI-14X Dc-POP3 Performance
		EXSPI_ IMAP4PERF	EXSPI-14X Dc-IMAP4 Performance
Exchange Source and Destination Mails Comparison	EXSPI_ DATA	EXSPI_DEST	EXSPI-14X Dc-Get Top Destination Details
		EXSPI_ SOURCE	EXSPI-14X Dc-Get Top Source Details

Report Name	Data Source	Data Class	Required SPI Policy
Exchange Top N Mail Senders and Recipients	EXSPI_ DATA	EXSPI_RECP	EXSPI-14X Dc-Get Top Recipient Details
		EXSPI_SENDER	EXSPI-14X Dc-Get Top Sender Details
Exchange Top N MailBox	EXSPI_ DATA	EXSPI_ MBDETAIL	EXSPI-14X Get Mailbox Details
		EXSPI_SENDER	EXSPI-14X Dc-Get Top Sender Details
		EXSPI_RECP	EXSPI-14X Dc-Get Top Recipient Details
Exchange Top N PubFolder	EXSPI_ DATA	EXSPI_ PFDETAIL	EXSPI-14X Get Public Folder Details
Exchange EdgeTransport Queue Details	EXSPI_ DATA	EXSPI_TRANSQ	EXSPI-14X Dc Transport Queues
Exchange EdgeTransport SMTP Details	EXSPI_ DATA	EXSPI_ SMTPRECV	EXSPI-14X Edge Dc-SMTP Perf Inbound Cnn
		EXSPI_ SMTPSEND	EXSPI-14X Edge Dc-SMTP Perf Outbound Cnn
Exchange HubTransport SMTP and DSN Details	EXSPI_ DATA	EXSPI_ SMTPRECV	EXSPI-14X Edge Dc-SMTP Perf Inbound Cnn
		EXSPI_ SMTPSEND	EXSPI-14X Edge Dc-SMTP Perf Outbound Cnn
		EXSPI_ HUBTRANSDSN	EXSPI-14X HUB Transport DSN

Report Name	Data Source	Data Class	Required SPI Policy
Exchange MailBox Details	EXSPI_ DATA	EXSPI_ MBDETAIL	EXSPI-14X Get Mailbox Details
		EXSPI_MBPERF	EXSPI-14X Dc- IS Mailbox Performance
Exchange MailBox Usage	EXSPI_ DATA	EXSPI_ PFDETAIL	EXSPI-14X Get Public Folder Details
		EXSPI_ MBDETAIL	EXSPI-14X Get Mailbox Details
Exchange PubFolder Details	EXSPI_ DATA	EXSPI_ PFDETAIL	EXSPI-14X Get Public Folder Details
		EXSPI_PFPERF	EXSPI-14X Dc- IS Public Folder Performance

Prerequisite Policies for Microsoft Active Directory Reports

The following table lists the Microsoft Active Directory SPI policies required by each Microsoft Active Directory report.

Note: Not every policy should be deployed to every Microsoft Active Directory node. See HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide and/or the HP Operations Smart Plug-in for Microsoft Active Directory Online Help to understand what each policy does and determine which policies are appropriate for the role played by each server. Deploying the policies indiscriminately will result in incorrect messages originating from the node.

In addition, see the SPI documentation for information on how the policies should be deployed and what additional configuration steps may be required.

Policy Configuration Requirement: Not required; deploy the policy with default settings.

Report Name	Data Source	Data Class	Required SPI Policy
AD Adhoc Comparison	ADSPI	ADSPI_DITDBSIZE	ADSPI-DIT_TotalDitSize
		ADSPI_ DITQUEUELENGTH	ADSPI-DIT_ DITQueueLength
		ADSPI_ LOGDISKSIZE	ADSPI-DIT_ LogFilesPercentFull
		ADSPI_ REPLATENCY	ADSPIRep_ MonitorIntraSiteReplication,
			ADSPI-Rep_ MonitorInterSiteReplication
AD Availability	ADSPI	ADSPI_ RESPONSETIME	ADSPI-Response_Logging
FSMO Role Holder	ADSPI	ADSPI_FSMO_ ROLEMVMT	ADSPI-FSMO_RoleMvmt
DC-GC Replication Delay	ADSPI	ADSPI_ REPLATENCY	ADSPIRep_ MonitorIntraSiteReplication
			ADSPI-Rep_ MonitorInterSiteReplication
DC Capacity	ADSPI	ADSPI_DITDBSIZE	ADSPI-DIT_TotalDitSize
		ADSPI_ DITQUEUELENGTH	ADSPI-DIT_ DITQueueLength
		ADSPI_ LOGDISKSIZE	ADSPI-DIT_ LogFilesPercentFull
		ADSPI_NTDSP	ADSPI_Logging
DC Health	ADSPI	ADSPI_DITDBSIZE	ADSPI-DIT_TotalDitSize
		ADSPI_ DITQUEUELENGTH	ADSPI-DIT_ DITQueueLength
		ADSPI_NTDSP	ADSPI_Logging
		ADSPI_ REPLATENCY	ADSPIRep_ MonitorIntraSiteReplication
			ADSPI-Rep_ MonitorInterSiteReplication

Prerequisite Policies for IBM WebSphere Reports

The following table lists the IBM WebSphere Smart Plug-in (SPI) policies required by each IBM WebSphere report in SHR:

Policy Configuration Requirement: Not required; deploy the policy with default settings.

Report Name	Data Source	Data Class	Required SPI Policy
WebSphere Top N summary	WBSSPI	WBSSPI_ METRICS WBSSPI_ RPT_ METRICS	WBSSPI_0040
			WBSSPI_0042
			WBSSPI_0026
			WBSSPI_0810
			WBSSPI_0811
			WBSSPI_0814
			WBSSPI_0807
			WBSSPI_0808
			WBSSPI_0809
			WBSSPI_0013
			WBSSPI_0812
			WBSSPI_0813
			WBSSPI_0045
			WBSSPI_0048
			WBSSPI_0074
			WBSSPI_0072
			WBSSPI_0073
			WBSSPI_0075
			WBSSPI_0077
			WBSSPI_0078
			WBSSPI_0076
			WBSSPI_0005
			WBSSPI_0807
			WBSSPI_0041

Report Name	Data Source	Data Class	Required SPI Policy
WebSphere Servlet Performance Overview	WBSSPI	WBSSPI_ METRICS WBSSPI_ RPT_ METRICS	WBSSPI_0260 WBSSPI_0261 WBSSPI_0262 WBSSPI_0265
WebSphere Thread Pool Performance Overview	WBSSPI	WBSSPI_ METRICS WBSSPI_ RPT_ METRICS	WBSSPI_0266 WBSSPI_0221 WBSSPI_0220
WebSphere JDBC Pool Throughput and Wait Time Details	WBSSPI	WBSSPI_ METRICS WBSSPI_ RPT_ METRICS	WBSSPI_0001 WBSSPI_0077 WBSSPI_0073 WBSSPI_0246
WebSphere EJB Performance Details	WBSSPI	WBSSPI_ METRICS WBSSPI_ RPT_ METRICS	WBSSPI_0245 WBSSPI_0263
WebSphere JDBC Utilization Details	WBSSPI	WBSSPI_ METRICS WBSSPI_ RPT_ METRICS	
WebSphere Executive Summary	WBSSPI	WBSSPI_ RPT_ METRICS	WBSSPI_0041 WBSSPI_0260 WBSSPI_0261 WBSSPI_0262 WBSSPI_0265 WBSSPI_0266 WBSSPI_0221 WBSSPI_0220 WBSSPI_0001 WBSSPI_0077 WBSSPI_0073 WBSSPI_0246

Report Name	Data Source	Data Class	Required SPI Policy
WebSphere Servlet Performance Details	WBSSPI	WBSSPI_ RPT_ METRICS	WBSSPI_0245 WBSSPI_0263
WebSphere Server Availability Details	WBSSPI	WBSSPI_ RPT_ METRICS	
WebSphere Transaction Performance Details	WBSSPI	WBSSPI_ METRICS	WBSSPI_0040 WBSSPI_0042 WBSSPI_0026 WBSSPI_0810 WBSSPI_0811 WBSSPI_0814 WBSSPI_0807 WBSSPI_0808 WBSSPI_0809 WBSSPI_0013 WBSSPI_0812 WBSSPI_0813
WebSphere JVM Utilization Details	WBSSPI	WBSSPI_ METRICS	WBSSPI_0045 WBSSPI_0048 WBSSPI_0074 WBSSPI_0072 WBSSPI_0073 WBSSPI_0075 WBSSPI_0077 WBSSPI_0078 WBSSPI_0076 WBSSPI_0005 WBSSPI_0807

Integrating with Data Sources for HP Operations Manager i Management Packs

To show reports on the data collected from different enterprise applications, SHR relies on the metrics collected by Operations Manager i Management Pack (OMi MP) .OMi MP collectors store the data into the data store provided by the HP Operations agent. SHR's integration with OMi MP data sources facilitates transfer of data from HP Operations agent's data store to SHR's database.

This integration is established when you deploy SHR views in the RTSM deployment scenario.

SHR provides performance reports for the following enterprise applications:

- OMi MP for Microsoft Active Directory

- OMi MP for Microsoft SQL Server

- OMi MP for Oracle Database

- OMi MP for Oracle WebLogic

- OMi MP for IBM WebSphere

Working of the Integration

1. Installation and configuration of an OMi MP ensures that necessary instrumentation, scripts, programs, and policies are transferred to a node where the application is running and the HP Operations agent is already installed.

   > **Tip:** For successful installation and configuration of OMi MPs, follow the *OMi MP* documentation.

2. OMi MP collectors start collecting data on the node based on rules and specifications available with the policies deployed on the node.

3. OMi MP stores the collected data into HP Operations agent's data store. Each OMi MP creates at least one *data source* in agent's data store.

4. After configuring SHR to collect data from a data source and installing Content Packs, SHR starts collecting historical data from agent's data store.

   > **Tip:** Procedures to configure SHR to collect data from the OMi MP data sources and installing Content Packs are available in the *SHR Configuration Guide*.

Prerequisites for Generating SHR Reports from the HP Operations Manager i Management Packs Data

Ensure the following prerequisites are met before integrating SHR with OMi MP. Otherwise, blank SHR reports will be generated:

- **Ensure data is logging into the HP Operations agent data store.**

  a. Ensure OMi MP is installed and configured. For further information on deploying and configuring OMi MPs, see the reference documents mentioned for each OMi MP in individual chapters of this book.

  b. Ensure all necessary OMi MP policies are deployed correctly.

  c. Ensure OMi MP collector is logging metrics into HP Operations agent database. For details on verifying that OMi MP is logging metrics into database, see the *HP Service Health Reporter Troubleshooting Guide*.

  > **Note:** If any of the preconditions are not fulfilled by the OMi MP, SHR cannot gather the necessary information from the data source and blank reports will be generated.

- **Ensure SHR is configured to connect to the Business Service Management (BSM) system where OMi MP is configured.**

  a. Ensure the topology source (RTSM) is configured to collect fact metrics from the data store of OMi MP. Verify this from the SHR Administration Console -> Topology Configuration -> Test Connection (which should be successful). For more information, see "*Configuring SHR*" in the *HP Service Health Reporter Configuration Guide*.

  b. Ensure the SHR Content Packs relevant to the OMi MP are installed. Verify this from the SHR Administration Console -> Administration -> Deployment Manager; you will see a column that indicates the deployment status of the content pack.

  > **Note:** If the OMi MP data store is not configured in BSM for SHR's use, it cannot gather the necessary information from the data source and blank reports will be generated.

Each SHR report uses a specific set of OMi MP metrics available in HP Operations agent's data store. Collection of metric data is governed by the OMi MP policies deployed on the node. In other words, to be able to view SHR reports of your interest successfully, you must deploy all the prerequisite policies.

Prerequisite Policies for IBM WebSphere Reports

The following table lists the IBM WebSphere Management Pack policies and aspects required for each IBM WebSphere report in SHR:

Report Name	Aspect Name	Policy Templates in Aspect	HP Operations agent	
			Data Source Name	Data Class Name
WebSphere Servlet Performance Overview	WebSphere Servlet Performance	WebSphere_ WebAppServletRespTime WebSphere_ WebAppServReqRtApp	WEBSPHERE_ DATA	WebSphere_ Servlet
WebSphere Thread Pool Performance Overview	WebSphere Thread Status	WebSphere_ ThreadPoolActThreads WebSphere_ ThreadPoolAveSize	WEBSPHERE_ DATA	WebSphere_ Thread
WebSphere Top N Summary	WebSphere JVM Heap Memory	WebSphere_ JVMMemUtilPct	WEBSPHERE_ DATA	WebSphere_ JVM_Perf
WebSphere Top N Summary	WebSphere Thread Status	WebSphere_ ThreadPoolActThreads WebSphere_ ThreadPoolAveSize	WEBSPHERE_ DATA	WebSphere_ Thread
WebSphere Top N Summary	WebSphere EJB Performance	WebSphere_EJBPoolSize WebSphere_ JDBCConnPoolUtil	WEBSPHERE_ DATA	WebSphere_ JDBC
WebSphere Top N Summary	WebSphere JDBC Connection Pool Status	WebSphere_ JDBCConnPoolSize WebSphere_ JDBCConnPoolUtil	WEBSPHERE_ DATA	WebSphere_ JDBC
WebSphere EJB Performance Details	WebSphere EJB Performance	WebSphere_EJBPoolSize WebSphere_ EJBPoolMissPctApp WebSphere_ EJBPoolUtilApp WebSphere_ EJBMethRespTime WebSphere_ EJBMethCallsRtApp	WEBSPHERE_ DATA	WebSphere_ EJB

Report Name	Aspect Name	Policy Templates in Aspect	HP Operations agent	
			Data Source Name	Data Class Name
WebSphere JDBC Pool Throughput and Wait Time Details	WebSphere JDBC Connection Pool Status	WebSphere_ JDBCConPoolThroughput WebSphere_ JDBCConPoolWtTime	WEBSPHERE_ DATA	WebSphere_ JDBC
WebSphere JDBC Utilization Details	WebSphere JDBC Connection Pool Status	WebSphere_ JDBCConnPoolUtil	WEBSPHERE_ DATA	WebSphere_ JDBC
WebSphere JVM Utilization Details	WebSphere JVM Heap Memory	WebSphere_ JVMMemUtilPct	WEBSPHERE_ DATA	WebSphere_ JVM_Perf
Websphere Executive Summary	WebSphere Server Status	WebSphere_ServerStatus	WEBSPHERE_ DATA	WebSphere_ SERVER
WebSphere Server Availability Details	WebSphere Server Status	WebSphere_ServerStatus	WEBSPHERE_ DATA	WebSphere_ SERVER
WebSphere Servlet Performance Details	WebSphere Servlet Performance	WebSphere_ WebAppServletRespTime WebSphere_ WebAppServReqRtApp	WEBSPHERE_ DATA	WebSphere_ Servlet
WebSphere Transaction Performance Details	WebSphere Transaction Status	WebSphere_TranCommitRt WebSphere_TranRollbackRt WebSphere_ TranTimeoutRte WebSphere_TranStartRt	WEBSPHERE_ DATA	WebSphere_ Transact

Note: When using the *IBMWebSphere_ETL_WebSphereMP* for gathering data from the IBM WebSphere Management Pack, the `NumServSession` measure of the *WebSphere Server Servlet* cube in the WebSphere Universe will not contain data.

Prerequisite Policies for Microsoft Active Directory Reports

The following table lists the OMi MP for Microsoft Active Directory policies and aspects required for each Microsoft Active Directory report.

> **Note:** Not every policy should be deployed to every Microsoft Active Directory node. See HP OMi MP for Microsoft Active Directory Online Help to understand what each policy does and determine which policies are appropriate for the role played by each server. Deploying the policies indiscriminately will result in incorrect messages originating from the node.
>
> In addition, see the OMi MP documentation for information on how the policies should be deployed and what additional configuration steps may be required.

Report Name	Aspect Name	Policy Templates in Aspect	Data Source Name	Data Class Name
			HP Operations agent	
AD Adhoc Comparison	MicrosoftAD DIT	MSAD_TotalDitSize	ADSPI	ADSPI_DITDBSIZE
	MicrosoftAD DIT	MSAD_DITQueueLength		ADSPI_DITQUEUELENGTH
	MicrosoftAD DIT	MSAD_LogFilesPercentFull		ADSPI_LOGDISKSIZE
	MicrosoftAD Replication Auto Baseline	MSAD_Rep_GC_Check_and_Threshold_Monitor_AT		ADSPI_GCREP
AD Availability	MicrosoftAD	MSAD_SCH_ResponseLogging	ADSPI	ADSPI_RESPONSE
DC-GC Replication Delay	MicrosoftAD Replication	MSAD_Rep_MonitorIntraSiteReplication	ADSPI	ADSPI_REPLATENCY
	MSAD_Rep_MonitorInterSiteReplication			
DC Capacity	MicrosoftAD DIT	MSAD_LogFilesPercentFull	ADSPI	ADSPI_LOGPERCENTFULL
	MicrosoftAD DIT	MSAD_DITPercentFull		ADSPI_DITPERCENTFULL

| Report Name | Aspect Name | Policy Templates in Aspect | HP Operations agent | |
			Data Source Name	Data Class Name
	MicrosoftAD Services	MSAD_ NTDSPROCDETAILS		ADSPI_NTDSP
DC Health	MicrosoftAD Replication	MSAD_Rep_ MonitorIntraSiteReplicati on MSAD_Rep_ MonitorInterSiteReplicati on	ADSPI	ADSPI_ REPLATENCY
	MicrosoftAD Services	MSAD_ NTDSPROCDETAILS		ADSPI_NTDSP
	MicrosoftAD DIT	MSAD_TotalDitSize		ADSPI_ DITDBSIZE
		MSAD_DITPercentFull		ADSPI_ DITPERCENTFUL L
		MSAD_DITQueueLength		ADSPI_ DITQUEUELENGT H

Prerequisite Policies for Microsoft SQL Server Reports

The following table lists the OMi MP for Microsoft SQL Server policies and aspects required for each Microsoft SQL Server report.

Note: See the OMi MP documentation for information on how the policies should be deployed and what additional configuration steps may be required.

For OMi MP for Microsoft SQL Server, Data Source Name is same as Data Class Name.

Report Name	Aspect Name	Policy Templates in Aspect	HP Operations agent Data Source Name
MSSQL Database and Virtual Device Space Usage Top N	Microsoft SQL Server Space	MSSQLServer_ 3242 MSSQLServer_ 3240	DBSPI_ MSS_ REPORT
MSSQL Performance Summary	Microsoft SQL Server Processes and Statistics	MSSQLServer_ 3001 MSSQLServer_ 3025	DBSPI_ MSS_ GRAPH
	Microsoft SQL Server Locks	MSSQLServer_ 3013	
	Microsoft SQL Server Transactions	MSSQLServer_ 3009	
	Microsoft SQL Server Input and Output Utilization	MSSQLServer_ 3008	
MSSQL Table Space Usage Top N	Microsoft SQL Server Space	MSSQLServer_ 3241	DBSPI_ MSS_ REPORT
MSSQL Database Input and Output Statistics	Microsoft SQL Server Input and Output Utilization	MSSQLServer_ 3007 MSSQLServer_ 3008	DBSPI_ MSS_ GRAPH
MSSQL Database Locks Summary	Microsoft SQL Server Locks	MSSQLServer_ 3071 MSSQLServer_ 3013 MSSQLServer_ 3070 MSSQLServer_ 3072 MSSQLServer_ 3075	DBSPI_ MSS_ GRAPH

Report Name	Aspect Name	Policy Templates in Aspect	HP Operations agent
			Data Source Name
MSSQL Database Performance Summary	Microsoft SQL Server Error	MSSQLServer_ 3023 MSSQLServer_ 3024	DBSPI_ MSS_ GRAPH
	Microsoft SQL Server Data Access Methods	MSSQLServer_ 3053 MSSQLServer_ 3054 MSSQLServer_ 3051 MSSQLServer_ 3052	DBSPI_ MSS_ GRAPH
MSSQL Database Space Usage Details	Microsoft SQL Server Space	MSSQLServer_ 3240	DBSPI_ MSS_ REPORT
MSSQL Database Table Space Usage Details	Microsoft SQL Server Space	MSSQLServer_ 3241	DBSPI_ MSS_ REPORT
MSSQL Instance Availability Details	Microsoft SQL Server Availability	MSSQLServer_ 3243	DBSPI_ MSS_ REPORT
MSSQL Server Transaction Summary	Microsoft SQL Server Transactions	MSSQLServer_ 3064 MSSQLServer_ 3066 MSSQLServer_ 3067	DBSPI_ MSS_ GRAPH
MSSQL Users Connection Summary	Microsoft SQL Server Processes and Statistics	MSSQLServer_ 3032 MSSQLServer_ 3026	DBSPI_ MSS_ GRAPH
MSSQL Virtual Device Space Usage Details	Microsoft SQL Server Space	MSSQLServer_ 3242	DBSPI_ MSS_ REPORT

Note: M031_NumUsersCnt is not available in the SQL list.

Prerequisite Policies for Oracle Database Reports

The following table lists the OMi MP for Oracle Database policies and aspects required for each Oracle database report.

> **Note:** For OMi MP for Oracle Database, Data Source Name is same as Data Class Name.

Report Name	Aspect Name	Policy Templates in Aspect	HP Operations agent Data Source Name
Database Oracle Executive Summary	Oracle Database Availability	OracleDB_0201	DBSPI_ORA_REPORT
Database Oracle Top 10 Instances and Tablespaces	Oracle Database Space Utilization Oracle Tablespace Health	OracleDB_0210 OracleDB_0212	DBSPI_ORA_REPORT
Database Oracle Top 5 Instances Load and Efficiency	Oracle Memory Performance	OracleDB_0021 OracleDB_0022 OracleDB_0039 OracleDB_0019 OracleDB_0020	DBSPI_ORA_GRAPH
	Basic Oracle Memory Performance	OracleDB_0032	
	Oracle Database Availability	OracleDB_0037	
	Oracle Transactions	OracleDB_0049	
Database Oracle Archive Device Detail	Oracle Archive Health	OracleDB_0058 OracleDB_0060	DBSPI_ORA_GRAPH
	Oracle Database Space Utilization	OracleDB_0062 OracleDB_0064 OracleDB_0065	
Database Oracle Disk And Memory Sort Detail	Oracle Memory Performance	OracleDB_0019 OracleDB_0020 OracleDB_0052	DBSPI_ORA_REPORT
Database Oracle Instance Availability Detail	Oracle Database Availability	OracleDB_0201	DBSPI_ORA_REPORT

Report Name	Aspect Name	Policy Templates in Aspect	HP Operations agent / Data Source Name
Database Oracle Instance Space Utilization Detail	Oracle Database Space Utilization	OracleDB_0212	DBSPI_ORA_ REPORT
Database Oracle Segment Detail	Oracle Segment Space	OracleDB_0016 OracleDB_0017 OracleDB_0018	DBSPI_ORA_ GRAPH
Database Oracle Shared Pool and Cache Performance Detail	Oracle Memory Performance	OracleDB_0021 OracleDB_0022 OracleDB_0039 OracleDB_0026 OracleDB_0040 OracleDB_0045	DBSPI_ORA_ GRAPH
Database Oracle SQL Performance Detail	Oracle Object Faults	OracleDB_0030 OracleDB_0046	DBSPI_ORA_ GRAPH
	Oracle Parallel Query Performance	OracleDB_0070 OracleDB_0071 OracleDB_0074 OracleDB_0076	
Database Oracle Tablespace Detail	Oracle Tablespace Health	OracleDB_0007 OracleDB_0006 OracleDB_0008 OracleDB_0011	DBSPI_ORA_ GRAPH
	Oracle Object Faults	OracleDB_0004 OracleDB_0005	
Database Oracle Tablespace Space Utilization Detail	Oracle Tablespace Health	OracleDB_0210	DBSPI_ORA_ REPORT

Note: The following metrics are deprecated in the MP:

- E063_TraceFileAddCnt

- E067_RBSegmntStatCnt

Prerequisite Policies for Oracle WebLogic Reports

The following table lists the OMi MP for Oracle WebLogic policies and aspects required for each Oracle WebLogic report.

Report Name	Aspect Name	Policy Templates in Aspect	HP Operations agent	
			Data Source Name	Data Class Name
WebLogic Servlet Performance Summary	Weblogic Servlet Performance	Weblogic_ ServletAverageExecutionTime Weblogic_ServletRequestRate	WEBLOGIC_DATA	WEBLOGIC_ SERVLETS
WebLogic JDBC Connection Pool Summary	Weblogic JDBC Connection Pool Status	Weblogic_ConnectionDelayTime Weblogic_ JDBCConnectionLeakRate Weblogic_ JDBCConnectionPoolThroughputRate Weblogic_ JDBCConnectionPoolUtilization	WEBLOGIC_DATA	WEBLOGIC_ JDBC
WebLogic Top N Summary	Weblogic JVM Heap Memory	Weblogic_JVMHeapUsage	WEBLOGIC_DATA	WEBLOGIC_ JVM
	Weblogic JDBC Connection Pool Status	Weblogic_ConnectionDelayTime Weblogic_ JDBCConnectionPoolThroughputRate	WEBLOGIC_DATA	WEBLOGIC_ JDBC
	Weblogic EJB Performance	Weblogic_ EJBCacheHitPercentage Weblogic_EJBPoolWaitCount	WEBLOGIC_DATA	WEBLOGIC_ EJB_TRANS WEBLOGIC_ EJB
WebLogic EJB Cache	Weblogic EJB	Weblogic_ EJBCacheHitPercentage	WEBLOGIC_DATA	WEBLOGIC_ EJB_TRANS

Report Name	Aspect Name	Policy Templates in Aspect	HP Operations agent	
			Data Source Name	Data Class Name
Hit	Performance			
WebLogic JMS Performance Details	Weblogic JMS Performance	Weblogic_ JMSServerThruByteRate Weblogic_ JMSServerThruMessageRate Weblogic_ JMSUtilizationByBytesPercentage Weblogic_ JMSUtilizationByMessagesPercentage	WEBLOG I C_DATA	WEBLOGIC_ JMS
WebLogic JVM Utilization	Weblogic JVM Heap Memory	Weblogic_JVMHeapUsage Weblogic_JVMHeapFreeMemory	WEBLOG I C_DATA	WEBLOGIC_ JVM
WebLogic Server Availability Details	Weblogic Server Status	Weblogic_ServerStatus	WEBLOG I C_DATA	WEBLOGIC_ SERVER
WebLogic Transaction Performance Details	Weblogic Transactions	Weblogic_ TransactionThroughputRate Weblogic_TransactionAverageTime	WEBLOG I C_DATA	WEBLOGIC_ TRANSACTIO N
WebLogic Executive Summary	Weblogic Server Status	Weblogic_ServerStatus	WEBLOG I C_DATA	WEBLOGIC_ SERVER

Note: All the other metrics that were part of this report are collected from the System Management and OM SHR Content Packs.

Send Documentation Feedback

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

Feedback on Administration Guide (Service Health Reporter 9.40)

Just add your feedback to the email and click send.

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

We appreciate your feedback!