

HP Service Health Reporter

Software Version: 9.40

Windows® and Linux operating systems

Configuration Guide

Document Release Date: July 2016
Software Release Date: January 2015



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 - 2016 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.

Documentation Updates

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

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

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

<https://softwaresupport.hp.com>

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

<https://hpp12.passport.hp.com/hppcf/createuser.do>

Or click the **the Register** link at the top of the HP Software Support 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: <https://softwaresupport.hp.com>

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:

<https://hpp12.passport.hp.com/hppcf/createuser.do>

To find more information about access levels, go to:

<https://softwaresupport.hp.com/web/softwaresupport/access-levels>

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

Part I: Configuring SHR	8
Chapter 1: Deployment Scenarios Supported by SHR	9
Business Service Management/Operations Manager i	9
HP Operations Manager	11
VMware vCenter	11
Other Sources of Data	12
Chapter 2: Planning to Configure SHR with BSM/OMi	14
Configuring RTSM Topology Source for SHR	14
List of Content Pack and Topology Views to Deploy	15
HP BSM Server	18
HP OMi 10 Server	20
Enabling CI Attributes for a Content Pack	22
Chapter 3: Planning to Configure SHR with HPOM	27
Authentication for SHR connection with HPOM	27
SHR connection with HPOM using NT authentication	28
SHR connection with HPOM using database authentication	28
Checking for the HPOM Server Port Number	36
Chapter 4: Primary Configuration	37
Task 1: Launching the Administration Console	38
Task 2: Configure the Database Connection	39
Task 3: Creating the Database Schema	40
Create DSN for Sybase IQ Database	46
Task 4: Creating the Management Database User Account	48
Task 5: Configuring the Collectors Installed on Remote Systems	50
Task 6: Selecting the Data Source	51
Data Sources for the HPOM Deployment Scenario	53
Data Sources for the BSM or OMi Deployment Scenario	54
OMi10 Topology Source with Integrated BSM	55
OMi10 Topology Source after BSM Upgrade	56
Data Source for the VMware vCenter Deployment Scenario	58
Data Sources for Other (Generic) Database Deployment Scenario	59
Task 7: Configuring the Topology Source	60
Configuring RTSM Service Definition Source	61
Supported Data Source Selections	62
Configuring HPOM Service Definition Source	62
Supported Data Source Selections	64
Configuring vCenter Service Definition	65
Supported Data Source Selections	66
Task 8: Summary	66
Chapter 5: Installing the Content Packs	67
Before You Begin	67

Check Availability and Integrity of Data Sources	67
Selecting the Content Pack Components	67
Installing the Content Pack Components	68
Chapter 6: Data Source Configuration	71
Configuring the HP Operations Agent Data Source	72
Configuring the HP Operations Manager Data Source	72
Configuring the Network Data Source (using Generic Database)	73
Configuring the VMware vCenter Data Source	74
Configuring the SiteScope Data Source	75
Configuring the Management and Profile Database Data Source	78
Configuring the HP OMi Data Source	82
Part II: Licensing	85
Chapter 7: Licensing SHR	86
Licenses to Use (LTUs)	86
Obtaining a Permanent License Key	88
Installing the Permanent License Key	89
SAP BusinessObjects License Reactivation	89
Part III: Migrating to Windows 2012 Environment	91
Chapter 8: Migration Scenarios	92
Method 1: Side-by-Side	92
Method 2: In-Place	97
Chapter 9: Migrating a Typical Installation to Custom Installation	101
Part IV: Additional Configurations	107
Chapter 10: Configuring the HP Operations Agent for Data Collection in Secure Mode	108
Chapter 11: Configuring the Report Drill Feature Settings	112
Chapter 12: Create Password for the Administrator Account	113
Chapter 13: Configuring the Internal Alerting Service	114
Chapter 14: Configuring Manual Restart of Tomcat Services	116
Chapter 15: Change Password for SybaseIQ Database User (dba)	117
Chapter 16: Configuring Secure Connection for SHR (HTTPS)	118
Creating a Keystore File	118
Configuring Secure Connection (HTTPS)	119
For the Administration console of SHR	119
For the InfoView Console and CMC of SHR	121
Deleting a Certificate from the Keystore	123
Chapter 17: Client Authentication Certificate for SHR	125
Authentication and Authorization	125
Prerequisites of Certificate Based Authentication	125
Configuring Username Extraction Method	128
Configuring SHR Administration Console	128
Configuring SAP BusinessObjects InfoView	131
Chapter 18: Database Backup and Recovery	135

Creating a Backup of SHR Databases on Windows	136
For Sybase IQ Database	136
For SAP BusinessObjects Database and File Store	147
For Management Database Table	153
Creating a Backup of SHR Databases on Linux	156
For Sybase IQ Database	157
For SAP BusinessObjects Database and File Store	159
For Management Database Tables	160
Restoring SHR Databases	161
Restoring SHR on Windows	161
For Sybase IQ Database	161
For SAP BusinessObjects Database and File Store	163
For Management Database Table	169
Restoring SHR on Linux	169
For Sybase IQ Database	170
For SAP BusinessObjects Database and File Store	171
For Management Database Table	179
Part V: References	180
Appendix A: SiteScope Monitors for SHR	181
Appendix B: Installing Xcelsius	187
Hardware and Software Requirements	187
Installing Xcelsius (Optional)	187
Appendix C: Listing of ETLs	188
Appendix D: Troubleshooting for Aggregation of Data Failed After Migration	193
Send Documentation Feedback	194

Part I: Configuring SHR

This section provides information about various deployment scenarios supported by SHR to generate reports corresponding to that environment.

Service Health Reporter (SHR) is a cross-domain historical infrastructure performance reporting solution. It leverages the topology information to show how the underlying infrastructure's health, performance, and availability are affecting your business services and business applications in the long term. SHR manages the relationship of infrastructure elements to the business services at run-time by using the same topology services that are used by the products that collect the performance data from the managed nodes.

Service Health Reporter collects data from different data sources, processes the data, and generates reports with the processed data. Service Health Reporter uses its components like the Sybase IQ database for storing performance data, SAP BusinessObjects for reporting and PostgreSQL database for storing management data. The collector component of SHR collects data from RTSM, HPOM, BSM Profile database, BSM Management database, Operations manager i (OMi), HP SiteScope, HP Network Node Manager i (NNMi) via the NNM iSPI Performance for Metrics and Network Performance Server (NPS), and HP Operations Agent.

All the components of Service Health Reporter can be installed on a single system. If a single system is not capable of supporting all the components of Service Health Reporter, the data collector, SAP BusinessObjects, and the Sybase IQ components can be installed on separate systems. If the data sources are distributed over a large area, there is an option to deploy Service Health Reporter collector on different systems. It reduces the network load and ensures connectivity to the data sources.

A topology model or view, logically maps and relates your business services to your IT elements. SHR enables you to define a topology service and collect the infrastructure data from the nodes that are part of the topology. In this way any change in topology information gets automatically reflected in the reports at run-time.

SHR provides support for the following topology sources:

- BSM/OMi
- HP Operations Manager (HPOM)
- VMware vCenter

SHR can connect to only one of the topology sources at a time.

Reference Documents:

For the latest SAP BusinessObjects documentation, see http://help.sap.com/businessobject/product_guides/

For information on Central management console(Administration of Business objects), go to:

http://<BO_FQDN>:8080/CmcApp/help/en/administration/html/default.htm

For information on Infoview (creation of reports, report functions and other admin tasks like scheduling), go to:

http://<BO_FQDN>:8080/InfoViewApp/BSMRHelp/en_US/WebHelp/Default.htm

For information on OMi Management Packs and other contents, see [HP Live Network Content Catalog](#).

Chapter 1: Deployment Scenarios Supported by SHR

Following are the deployment scenarios supported on SHR:

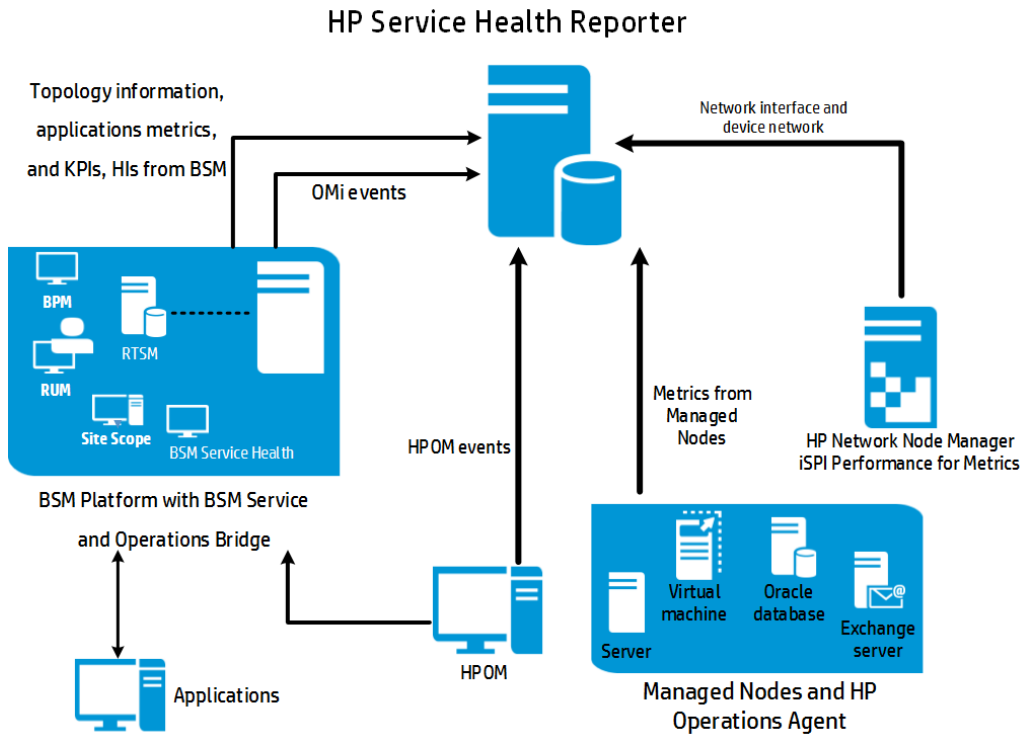
- [Deployment with BSM/OMi](#)
- [Deployment with HP Operations Manager](#)
- [Deployment with VMware vCenter](#)
- [Other deployments](#)

Business Service Management/Operations Manager i

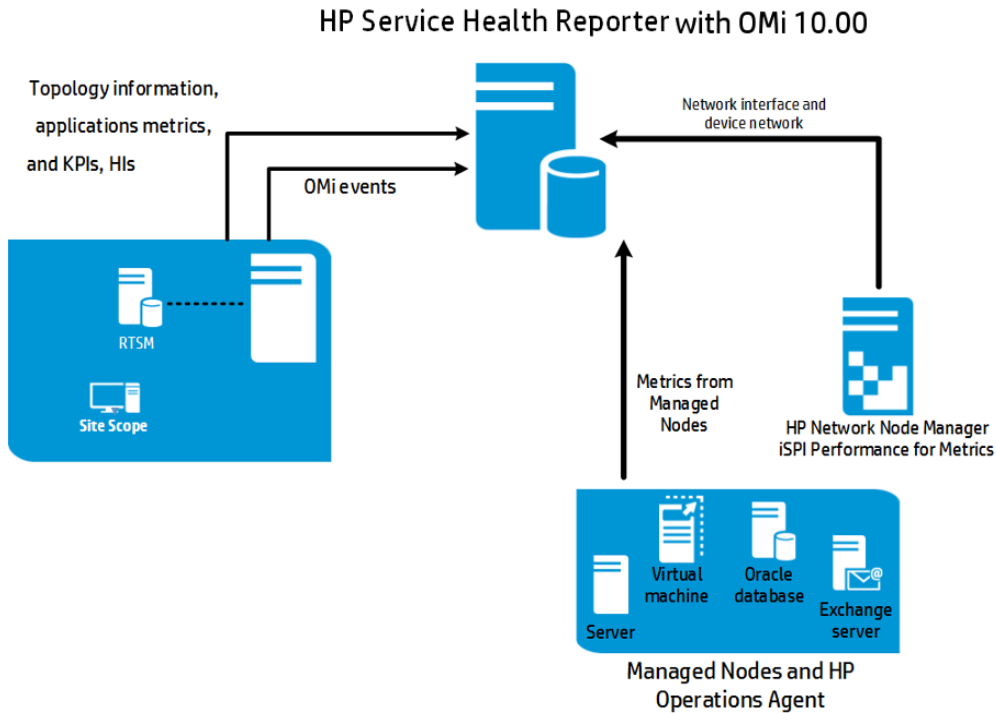
In this deployment, Run-time Service Model (RTSM) is the source of topology information. SHR discovers and synchronizes topology information from OMi. In a BSM environment with underlying HPOM servers, this synchronization technique receives discovered topology data from multiple HPOM systems and updates the Configuration Items (CIs) and CI relationships in the RTSM as soon as changes are discovered. However, you can also use the HPOM D-MoM dynamic topology synchronization technique to discover and synchronize the topology information in RTSM. In an environment with OMi 10.00, SHR uses RTSM to obtain topology information and metrics from HP Operations Agent or HP SiteScope systems that are configured with OMi.

Additionally, you can configure NPS with SHR to create reports with data collected by NNMI.

The following diagram shows the flow of data from HP Operations Agent, HPOM, NNM iSPI Performance for Metrics, and topology information from RTSM in a BSM environment with underlying HPOM servers.



The following diagram shows the flow of data from HP Operations Agent, HPOM, NNM iSPI Performance for Metrics, and topology information from RTSM in an OMi 10.00 environment.

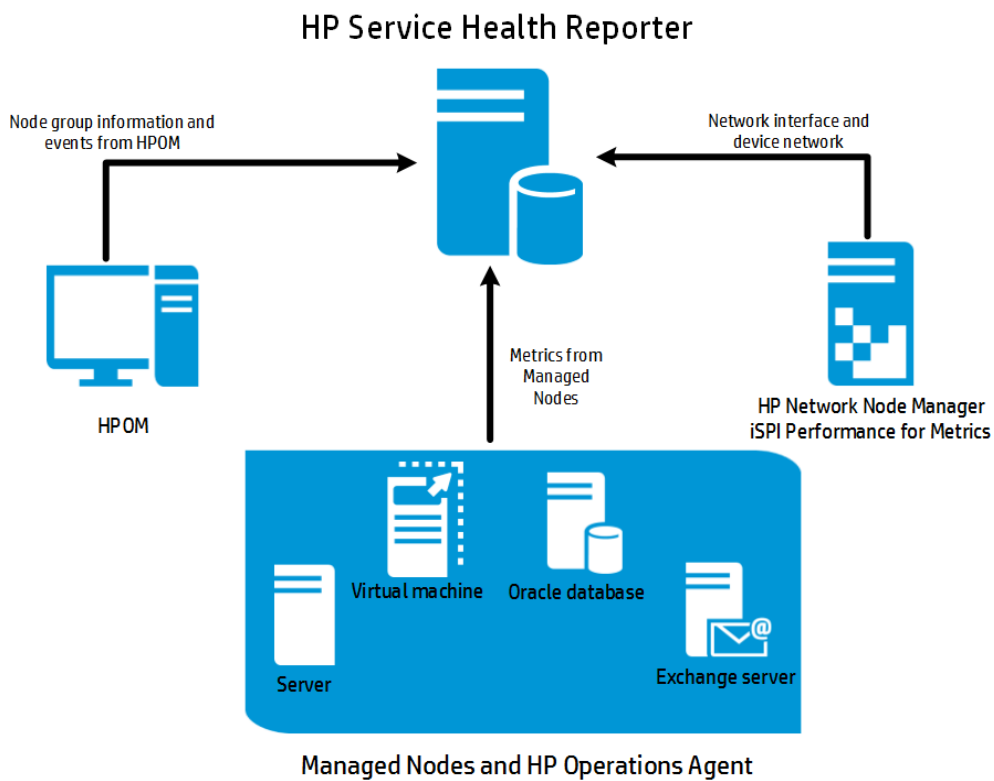


For information on OMi Management Packs and other contents, see [HP Live Network Content Catalog](#).

HP Operations Manager

In this deployment, the topology information is a group of managed nodes defined in HPOM that are logically combined for operational monitoring. These logical node groups are created by HPOM users to classify the nodes as specific organizations or entities within their enterprise. For example, a group called Exchange Servers can be created in HPOM to organize the specific Exchange Servers and Active Directory nodes for reporting or monitoring purposes. SHR uses the node groups from HPOM for its topology computation.

While SHR collects topology information only from HPOM in this environment, you can use VMware vCenter as a data source to create reports.



VMware vCenter

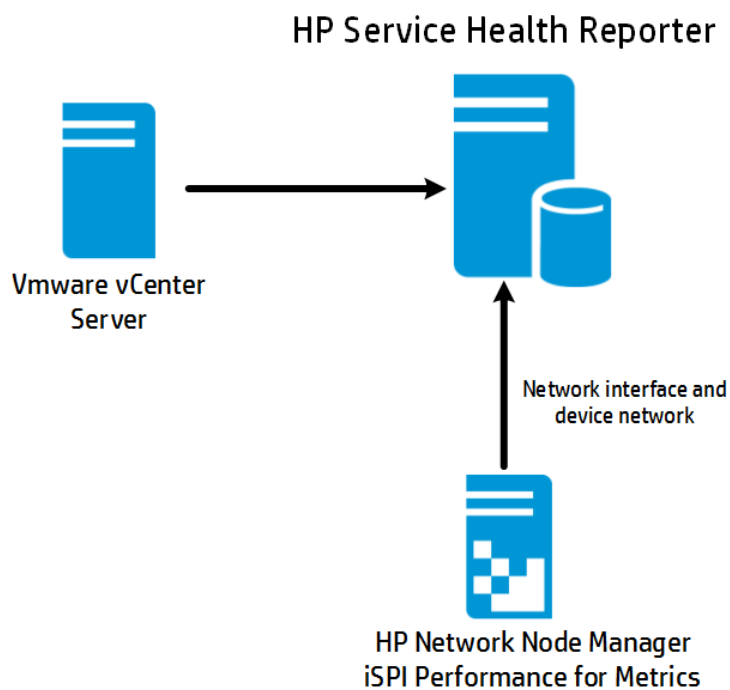
VMware vCenter is a distributed server-client software solution that provides a central and a flexible platform for managing the virtual infrastructure in business-critical enterprise systems. VMware vCenter centrally monitors performance and events, and provides an enhanced level of visibility of the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

In the VMware vCenter deployment scenario, the VMware vCenter server is the source of the topology information for SHR.

Note: It is recommended to set the VMware stats logging level to 2. However, if the logging level is

set to 1, then some of the metrics of logging level 2 may not be available in SHR reports. For information on logging levels and their corresponding metrics, use the following URL:

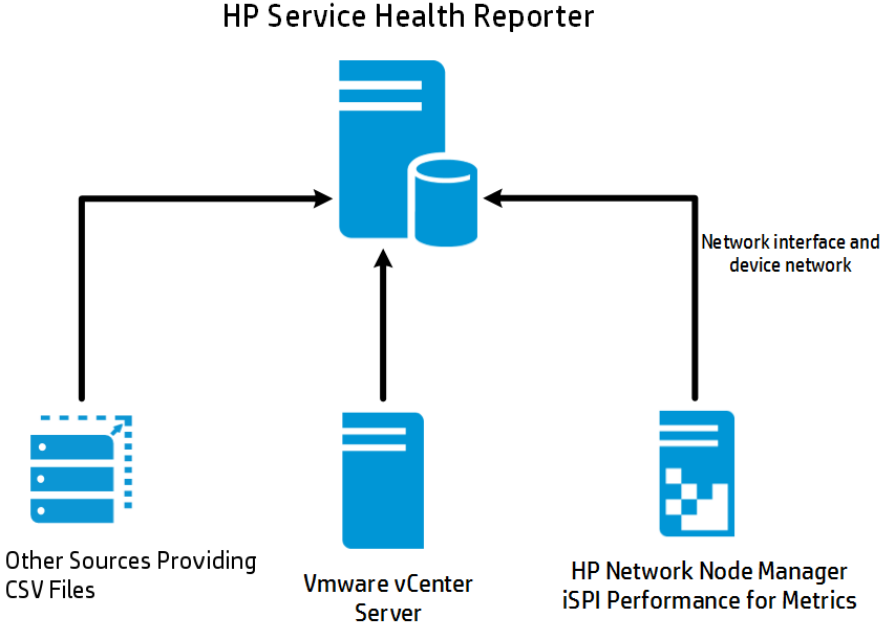
<https://communities.vmware.com/docs/DOC-5600>



Other Sources of Data

Apart from the basic deployment scenarios, you can collect data from the following sources independently:

- Deployment with NNMi
- Deployment with a generic database
- Deployment with other applications using CSV



Chapter 2: Planning to Configure SHR with BSM/OMi

If you plan to configure SHR to work with a BSM or OMi installation, you must make sure:

- BSM/OMi is installed and configured successfully.
- If you are monitoring systems and applications using the Monitoring Automation component of OMi and Management Packs, make sure that necessary Management Pack policies are deployed.
- If you are monitoring systems and applications using underlying HPOM servers and Smart Plug-ins (SPIs), make sure that necessary SPI policies are deployed.
- Make sure to deploy necessary OMi views. See [Configuring RTSM Topology Source for SHR](#).

Configuring RTSM Topology Source for SHR

RTSM is a source of the topology information for SHR. The topology information includes all CIs as modeled and discovered in RTSM. Node resource information is directly obtained from HP Operations Agent and HP SiteScope.

Note: Node resource is a local dimension in HP Operations Agent and HP SiteScope.

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
- Systems Infrastructure
- Virtualization Infrastructure

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

In the HP BSM environment, RTSM is used to discover the CIs and generate the topology views. To configure SHR to collect domain-specific data, you first need to deploy those topology views for each Content Pack.

These topology views contain specific CI attributes that Contents Packs use to collect the relevant data. However, these topology views can vary from one Content Pack to another.

For example, the Exchange Server Content Pack might require a topology view that lists exchange servers, mailbox servers, mailbox and public folder stores, and so on. A System Management Content Pack, however, might require a different topology view that lists all the Business Applications, business services, and system resource, such as CPU, memory, disk, within the infrastructure. Based on these views, the CI attributes for each Content Pack may vary.

List of Content Pack and Topology Views to Deploy

On Windows:

Content Pack	View Name	Location
BPM (Synthetic Transaction Monitoring)	EUM_BSMR.zip(BSM only) EUM_OMi.zip(OMi 10 only)	%PMDB_ HOME%\packages\EndUserManagement\ETL_BPM.ap\source\cldb_views %PMDB_ HOME%\packages\EndUserManagement\ETL_BPM_OMi.ap\source\cldb_views Note: If BSM is the deployment scenario, then deploy only EUM_BSMR.zip view in the BSM server. If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.
Real User Transaction Monitoring	EUM_BSMR.zip(BSM only) EUM_OMi.zip(OMi 10 only)	%PMDB_ HOME%\packages\EndUserManagement\ETL_RUM.ap\source\cldb_views %PMDB_ HOME%\packages\EndUserManagement\ETL_RUM_OMi.ap\source\cldb_views Note: If BSM is the deployment scenario, then deploy only EUM_BSMR.zip view in the BSM server. If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.
Network	SHR_Network_Views.zip	%PMDB_HOME%\packages\Network\ETL_Network_NPS92_RTSM.ap\source\cldb_views
System Management	SM_BSM9_Views.zip	%PMDB_ HOME%\packages\SystemManagement\ETL_SystemManagement_PA.ap\source\cldb_views
Oracle	SHR_DBOracle_	%PMDB_HOME%\Packages\DatabaseOracle\ETL_

Content Pack	View Name	Location
	Views.zip SHR_DBOracle_OM.zip	DBOracle_DBSPI.ap\source\cldb_views\SHR_DBOracle_Views.zip
Oracle WebLogic Server	J2EEApplication.zip J2EEApplication_OM.zip	For OM/SPI: %PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWLS_WLSSPI.ap\source\cldb_views For OMi/MP: %PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWLS_WLSMP.ap\source\cldb_views
IBM WebSphere Application Server	J2EEApplication.zip J2EEApplication_OM.zip	For OM/SPI: %PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWBS_WBSSPI.ap\source\cldb_views For OMi/MP: %PMDB_HOME%\packages\ApplicationServer\ETL_AppSrvrWBS_WBSMP.ap\source\cldb_views
Microsoft SQL Server	SHR_DBMSSQL_Views.zip SHR_DBMSSQL_OM.zip	%PMDB_HOME%\packages\DatabaseMSSQL\ETL_DBMSSQL_DBSPI.ap\source\cldb_views
Microsoft Exchange Server	SHR_Exchange_Business_View.zip SHR_Exchange_OM.zip	%PMDB_HOME%\packages\ExchangeServer\ETL_Exchange_Server2007.ap\source\cldb_views
Microsoft Active Directory	SHR_AD_Business_View.zip SHR_ActiveDirectory_OM.zip	%PMDB_HOME%\packages\ActiveDirectory\ETL_AD_ADSPI.ap\source\cldb_views
Virtual Environment Performance	SM_BSM9_Views.zip	%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_PA.ap\source\cldb_views
Health and Key Performance Indicators (Service Health)	All the views	
Cross-Domain Operations Events	All the views	
Operations Events	No views	

On Linux:

Content Pack	View Name	Location
BPM (Synthetic Transaction Monitoring)	EUM_BSMR.zip(BSM only) EUM_OMi.zip(OMi 10 only)	<p>Business view - \$PMDB_HOME/packages/EndUserManagement/ETL_BPM.ap/source/cmdb_views</p> <p>OM view - \$PMDB_HOME/packages/EndUserManagement/ETL_BPM_OMi.ap/source/cmdb_views</p> <p>Note: If BSM is the deployment scenario, then deploy only EUM_BSMR.zip view in the BSM server.</p> <p>If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.</p>
Real User Transaction Monitoring	EUM_BSMR.zip(BSM only) EUM_OMi.zip(OMi 10 only)	<p>Business view - \$PMDB_HOME/packages/EndUserManagement/ETL_RUM_OMi.ap/source/cmdb_views</p> <p>OM view - \$PMDB_HOME/packages/EndUserManagement/ETL_RUM_OMi.ap/source/cmdb_views</p> <p>Note: If BSM is the deployment scenario, then deploy only EUM_BSMR.zip view in the BSM server.</p> <p>If OMi 10 is the deployment scenario, then deploy only EUM_OMi.zip view in the OMi 10 server.</p>
Network	SHR_Network_Views.zip	\$PMDB_HOME/packages/Network/ETL_Network_NPS92_RTSM.ap/source/cmdb_views
System Management	SM_BSM9_Views.zip	\$PMDB_HOME/packages/SystemManagement/ETL_SystemManagement_PA.ap/source/cmdb_views
Oracle	SHR_DBOracle_Views.zip SHR_DBOracle_OM.zip	\$PMDB_HOME/Packages/DatabaseOracle/ETL_DBOracle_DBSPI.ap/source/cmdb_views/SHR_DBOracle_Views.zip
Oracle WebLogic Server	J2EEApplication.zip J2EEApplication_OM.zip	<p>For OM/SPI: \$PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWLS_WLSSPI.ap/source/cmdb_views</p> <p>For OMi/MP: \$PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWLS_WLSMP.ap/source/cmdb_views</p>

Content Pack	View Name	Location
IBM WebSphere Application Server	J2EEApplication.zip J2EEApplication_OM.zip	For OM/SPI: \$PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWBS_WBSMPI.ap/source/cmdb_views For OMi/MP: \$PMDB_HOME/packages/ApplicationServer/ETL_AppSrvrWBS_WBSMP.ap/source/cmdb_views
Microsoft SQL Server	SHR_DBMSSQL_Views.zip SHR_DBMSSQL_OM.zip	\$PMDB_HOME/packages/DatabaseMSSQL/ETL_DBMSSQL_DBSPI.ap/source/cmdb_views
Microsoft Exchange Server	SHR_Exchange_Business_View.zip SHR_Exchange_OM.zip	\$PMDB_HOME/packages/ExchangeServer/ETL_Exchange_Server2007.ap/source/cmdb_views
Microsoft Active Directory	SHR_AD_Business_View.zip SHR_ActiveDirectory_OM.zip	\$PMDB_HOME/packages/ActiveDirectory/ETL_AD_ADSPI.ap/source/cmdb_views
Virtual Environment Performance	SM_BSM9_Views.zip	\$PMDB_HOME/packages/SystemManagement/ETL_SystemManagement_PA.ap/source/cmdb_views
Health and Key Performance Indicators (Service Health)	All the views	
Cross-Domain Operations Events	All the views	
Operations Events	No views	

HP BSM Server

To deploy the topology model views for the Content Packs in the HP BSM server, follow these steps:

1. In the web browser, type the following URL:

`http://<BSM system FQDN>/bsm`

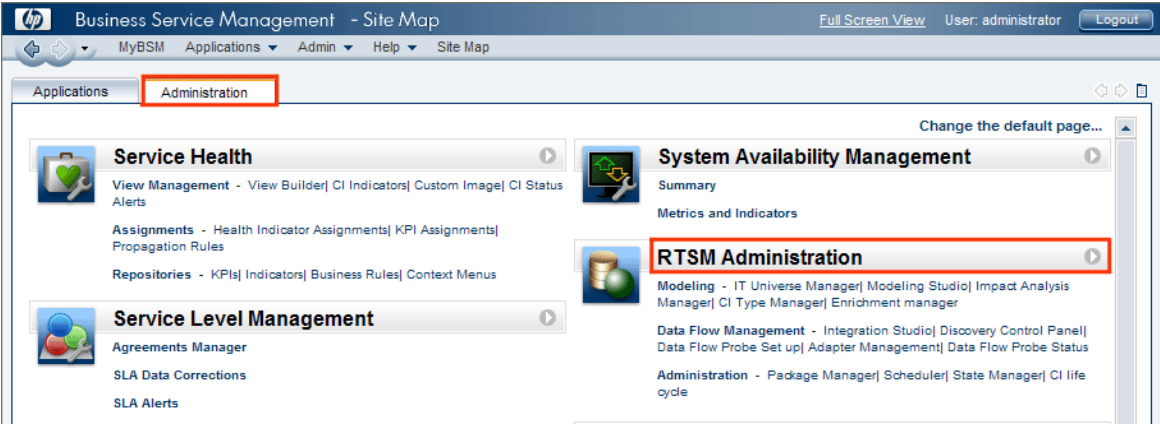
where, <BSM system FQDN> is the FQDN of the HP BSM server.

Note: You can launch the HP BSM server from a system where SHR is installed or any other local system. If you are launching from local system, ensure that you browse to the location mentioned in [List of Content Pack and Topology Views to Deploy](#) and copy the required views

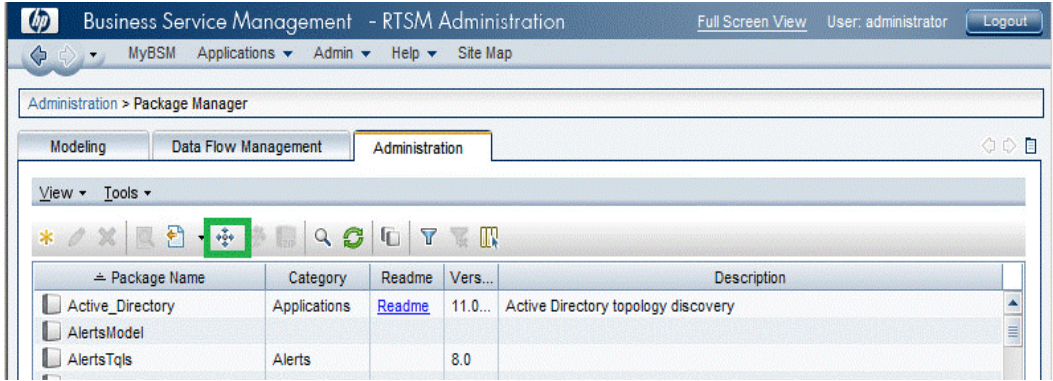
to your local system.

The Business Service Management Login page appears.

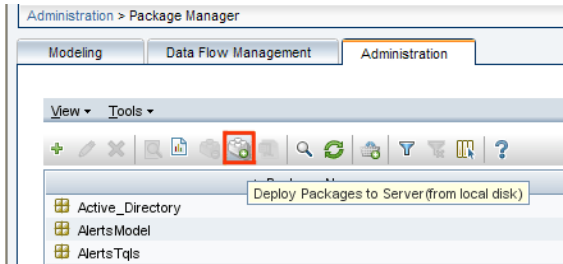
- 2. Type the login name and password and click **Log In**. The Business Service Management - Site Map appears.
- 3. Click **Administration > RTSM Administration**. The RTSM Administration page appears.



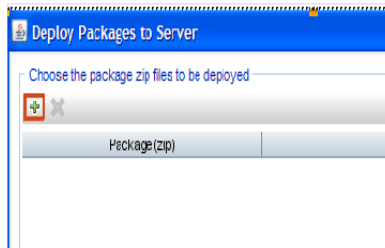
- 4. Click **Administration > Package Manager**. The Package Manager page appears.



- 5. Click the **Deploy Packages to Server (from local disk)** icon. The **Deploy Package to Server** dialog box appears.



- 6. Click the **Add** icon.



The **Deploy Package to Server (from local disk)** dialog box appears.

7. Browse to the location of the Content Pack zip files, select the required files, and then click **Open**.
You can view and select the TQL and ODB views that you want to deploy under **Select the resources you want to deploy** in the **Deploy Package to Server (from local disk)** dialog box. Ensure that all the files are selected.
8. Click **Deploy** to deploy the Content Pack views.

You have successfully deployed the Content Packs views based on the type of deployment scenario selected for SHR.

HP OMi 10 Server

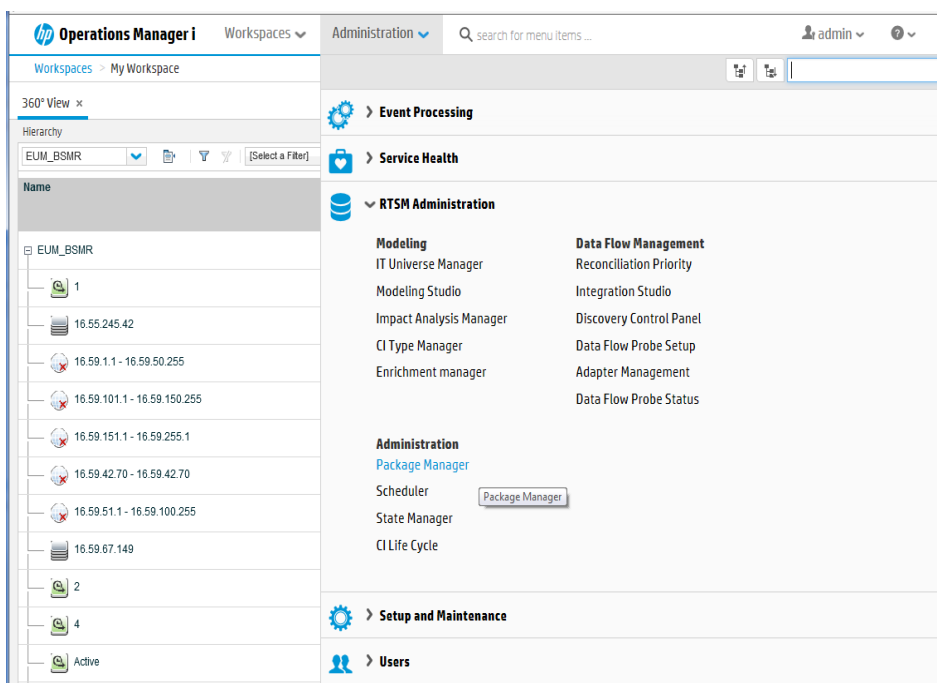
To deploy the topology model views for the Content Packs in the HP OMi 10 server, follow these steps:

1. In the web browser, type the following URL:
`http://<OMi system FQDN>/omi`
where, <OMi system FQDN> is the FQDN of the HP OMi server.

Note: You can launch the HP OMi server from a system where SHR is installed or any other local system. If you are launching from local system, ensure that you browse to the location mentioned in [List of Content Pack and Topology Views to Deploy](#) and copy the required views to your local system.

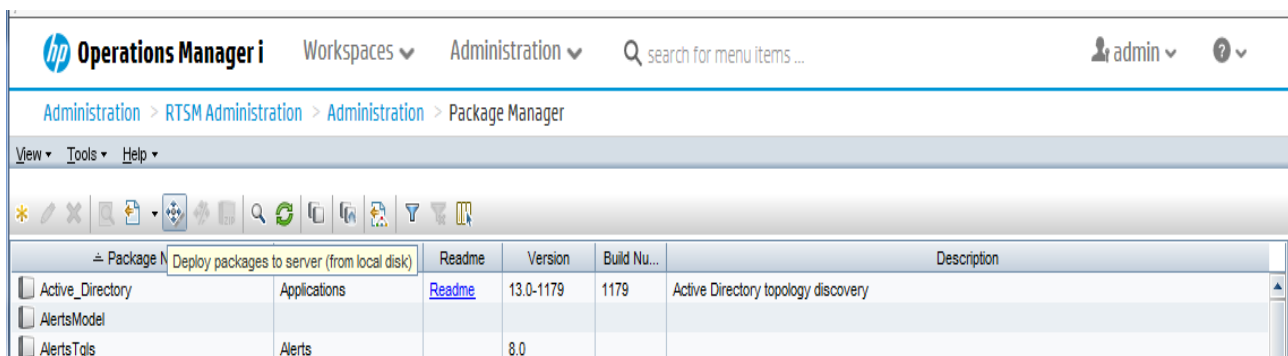
The Operations Manager i Login page appears.

2. Type the login name and password and click **Log In**. The Operations Manager i Workspace page appears.
3. Click **Administration > RTSM Administration > Package Manager**.

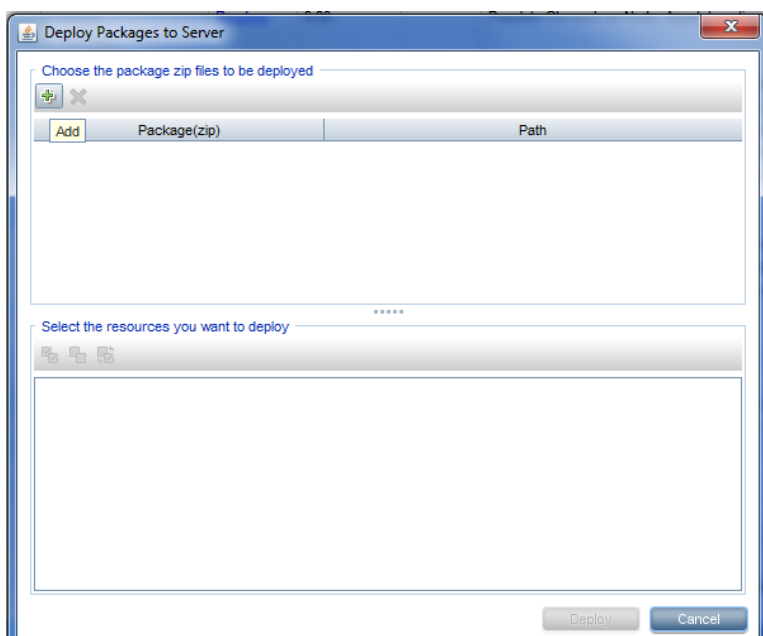


The Package Manager page appears.

4. Click the **Deploy Packages to Server (from local disk)** icon. The **Deploy Package to Server** dialog box appears.



5. Click the **Add** icon.



The **Deploy Package to Server (from local disk)** dialog box appears.

6. Browse to the location of the Content Pack zip files, select the required files, and then click **Open**.
You can view and select the TQL and ODB views that you want to deploy under **Select the resources you want to deploy** in the **Deploy Package to Server (from local disk)** dialog box. Ensure that all the files are selected.
7. Click **Deploy** to deploy the Content Pack views.

You have successfully deployed the Content Packs views based on the type of deployment scenario selected for SHR.

Enabling CI Attributes for a Content Pack

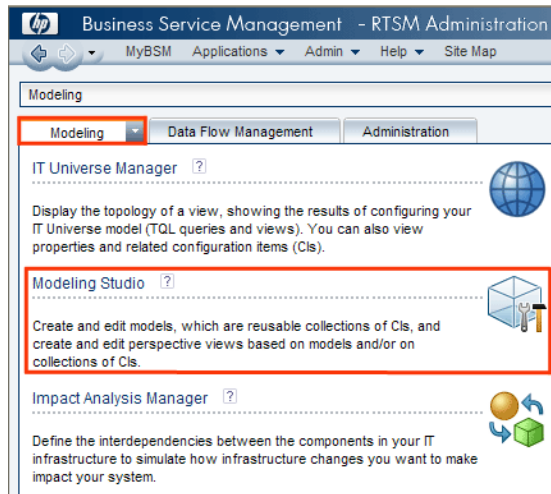
Note: To enable CI attributes for Content Pack in OMi 10 environment, follow the same configuration steps given in this section. However, use OMi server details instead of BSM server.

Each Content Pack view includes a list of CI attributes that are specific to that Content Pack. The CI attributes that are required for data collection are automatically enabled in each of the Content Pack views after you deploy them.

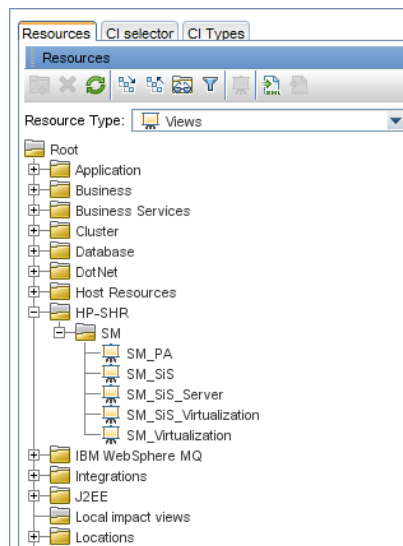
To enable additional CI attributes to collect additional information relevant to your business needs:

1. In the web browser, type the following URL:
`http://<server_name>.<domain_name>/HPBSM`
In this instance, `<server_name>` is the name of the HP BSM server, and `<domain_name>` is the name of the user's domain according to user's network configuration.
The Business Service Management Login page appears.
2. Type the login name and password and click **Log In**. The Business Service Management Site Map appears.
3. Click **Administration > RTSM Administration**. The RTSM Administration page appears.

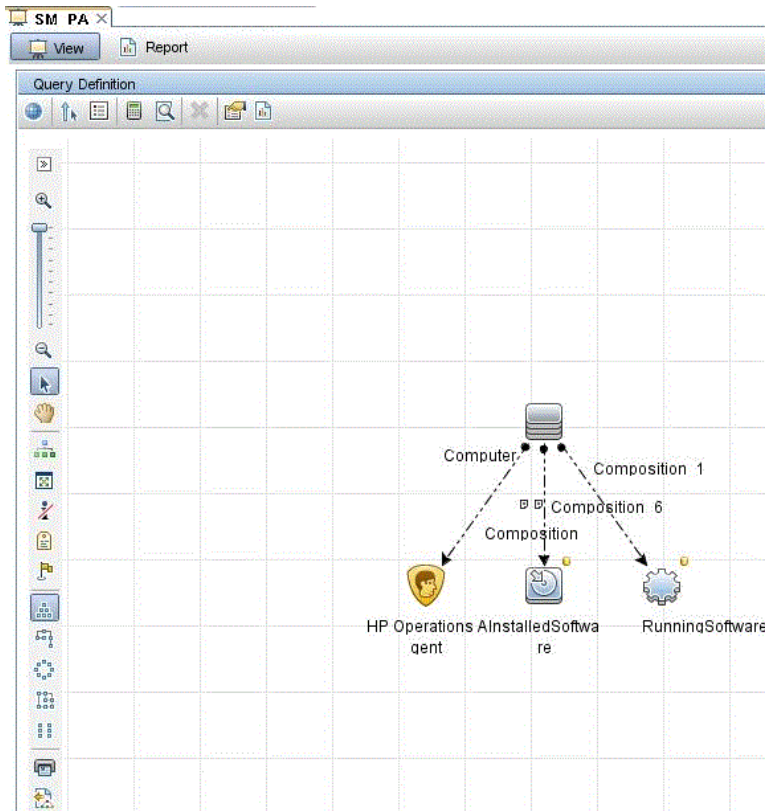
4. Click **Modeling > Modeling Studio**. The **Modeling Studio** page appears.



5. In the **Resources** pane, expand **HP-SHR**, expand a **Content Pack** folder and double-click a topology view to open it.

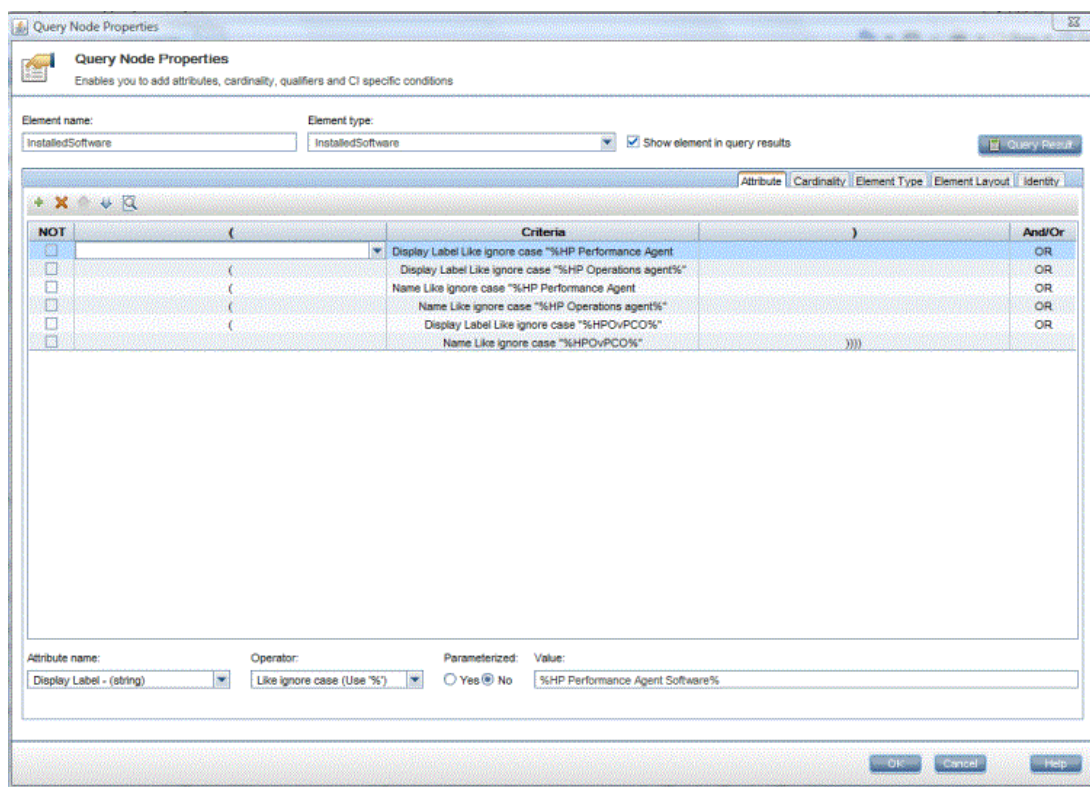


6. In the **Topology** pane, right-click any node in the topology diagram, and then click **Query Node Properties** to view the list of CI attributes for the selected node.



The **Query Node Properties** dialog box appears.

7. Click **Attributes**. Select the attributes that you want to enable and then click **OK**.



Configure SiteScope to integrate with SHR

HP SiteScope is an agent-less monitoring solution designed to ensure the availability and performance of distributed IT infrastructures—for example, servers, operating systems, network devices, network services, applications, and application components.

For SHR to collect data for the physical nodes from SiteScope, you must first create the monitors in SiteScope. Monitors are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems. These monitors collect data about the various IT components in your environment and are mapped to specific metrics that are used by SHR such as CPU usage, memory usage, and so on. After you create the monitors, you must also enable SiteScope to log data in HP Operations Agent/BSM profile database so that SHR can collect the required data from the agent. Perform this task only if you have SiteScope installed in your environment. Otherwise, proceed to the next task.

For the list of monitors (including the counters and measures) to be created in SiteScope, see ["Appendix A: SiteScope Monitors for SHR" on page 181](#).

For more information about creating monitors in SiteScope, see the *Using SiteScope* and the *Monitor Reference* guides. This document is available at the following URL:

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

Enable integration between SiteScope and BSM to transfer the collected topology data by the SiteScope monitors to BSM. For more information about SiteScope integration with BSM, see *Working with Business Service management (BSM)* of the *Using SiteScope* guide.

If HP BSM is the deployment scenario then you can integrate SiteScope with SHR using either [Configuring the Management and Profile Database Data Source](#) procedure or [Configuring the SiteScope Data Source](#) procedure.

If OMi10 is the deployment scenario then you can integrate SiteScope with SHR using [Configuring the SiteScope Data Source](#) procedure.

The SysPerf_ETL_SiS is deprecated in SHR 9.4. If you have already installed the SysPref_ETL_SiS_DB then to integrate SiteScope with SHR, follow these steps:

1. Log on to the host system that has SHR installed on it as administrator.
2. Access SiteScope by typing the SiteScope address in a Web browser. The default address is: `http://<SiteScope host name>:<port number>/SiteScope`.
3. Enable SiteScope to integrate with HP Operations Agent for data logging. For more information, see *Working with Operations Manager and BSM Using the HP Operations Agent* of the *Using SiteScope* guide.
4. Set the number of monitors and the frequency at which data is fed into the HP Operations Agent integration. While the default SiteScope configuration enables running thousands of monitors, sizing is important for planning the maximum number of monitors, metrics, and monitors types that can be stored within the SiteScope-HPOM metrics integration. For more information, see *Sizing Recommendations for SiteScope-Operations Manager Metrics Integration* of the *Using SiteScope* guide.

If you configured a remote collector with the service definition, make sure to restart the collector service on the collector system after installing Content Packs.

To restart the service manually on Windows:

1. Open the **Services** window, right-click **HP_PMDB_Platform_Collection** service, and then click **Restart**.

To restart the service manually on Linux:

1. Go to the `/etc/init.d` directory, and then run the following command:
`service HP_PMDB_Platform_Collection --full-restart`

Chapter 3: Planning to Configure SHR with HPOM

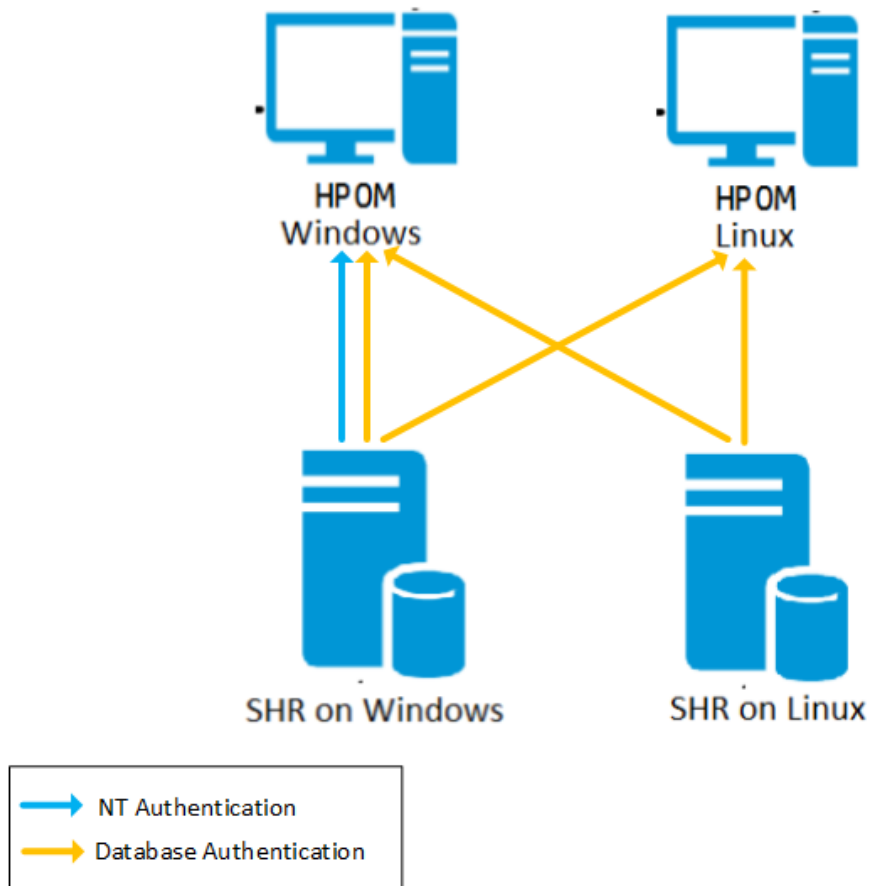
If you plan to configure SHR to work with an HPOM installation, you must:

- Install and configure HPOM successfully
- Deploy necessary SPI policies

Authentication for SHR connection with HPOM

SHR connects to HPOM to collect data. The NT authentication and database authentication are the two methods of authentication for SHR to connect to HPOM.

If SHR and HP OM are installed on Windows then both NT and database authentication is supported. For all the other deployment scenarios only database authentication is supported.



SHR connection with HPOM using NT authentication

If SHR is installed on a system which is part of a domain, and if you have logged into the system as a local user or domain user having administrator privileges (say DOMAIN\Administrator), start the *HP PMDB Platform Administrator* and *HP PMDB Platform Collection* service. You must configure the services for the domain before configuring the HPOM service definition source connection.

Task 1: Configure HP PMDB Platform Administrator Service for the Domain

1. Click **Start > Run**. The **Run** dialog box appears.
2. Type `services.msc` in the **Open** field, and then press **ENTER**. The **Services** window appears.
3. On the right pane, right-click **HP_PMDB_Platform_Administrator**, and then click **Stop**.
4. Right-click **HP_PMDB_Platform_Administrator** and then click **Properties**. The **SHR Service Properties** dialog box appears.
5. On the **Log on** tab, select **This account**.
6. Type **DOMAIN\Administrator** in the field (where Administrator is the local user having administrator privileges).
7. Type the user password in the **Password** field.
8. Retype the password in the **Confirm password** field.
9. Click **Apply** and then click **OK**.
10. On the right pane, right-click **HP_PMDB_Platform_Administrator**, and then click **Start**.

Task 2: Configure HP PMDB Platform Collection Service for the Domain

1. Click **Start > Run**. The **Run** dialog box appears.
2. Type `services.msc` in the **Open** field, and then press **ENTER**. The **Services** window appears.
3. On the right pane, right-click **HP_PMDB_Platform_Collection_Service**, and then click **Stop**.
4. Right-click **HP_PMDB_Platform_Collection_Service** and then click **Properties**. The **SHR Collection Service Properties** dialog box appears.
5. On the **Log on** tab, select **This account**.
6. Type **DOMAIN\Administrator** in the field (where Administrator is the local user having administrator privileges).
7. Type the user password in the **Password** field.
8. Retype the password in the **Confirm password** field.
9. Click **Apply** and then click **OK**.
10. On the right pane, right-click **HP_PMDB_Platform_Collection_Service**, and then click **Start**.

After performing the configuration steps, proceed with the HPOM service definition connection configuration.

SHR connection with HPOM using database authentication

Creating database user account depends on how Microsoft SQL Server is set up in the HPOM environment and how you configure SHR to communicate with the HPOM database server. The following are the two possible scenarios:

- **Scenario 1:** HPOM for Windows 8.x or 9.x is installed on one system with Microsoft SQL Server 2005 or Microsoft SQL Server 2008 installed on the same system or a remote system. SHR, which is installed on another system, can be configured to connect to SQL Server either through Windows authentication or SQL Server authentication (mixed-mode authentication). The authentication method defined in SQL Server can be used in SHR to configure the HPOM database connection.
- **Scenario 2:** HPOM for Windows 8.x uses Microsoft SQL Server 2005 Express Edition that is embedded with it by default. Similarly, HPOM for Windows 9.x uses the embedded Microsoft SQL Server 2008 Express Edition by default. The authentication mode in this scenario is Windows NT authentication. However, in this case, a remote connection between SQL Server and SHR is not possible. Therefore, you must create a user account for SHR so that mixed-mode authentication is possible in this scenario.

Before you create the user account, enable the mixed-mode authentication. For information on the steps to enable the mixed-mode authentication, see the following URL:

<http://support.microsoft.com>

To create a user name and password for authentication purposes on HPOM system with embedded Microsoft SQL Server 2005, follow these steps:

Task 1: Create a user name and password

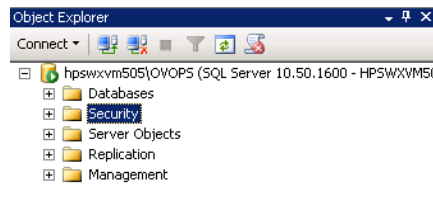
1. Log on to the HPOM system with embedded Microsoft SQL Server 2005.
2. Click **Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**. The **Microsoft SQL Server Management Studio** window opens.

Note: If SQL Server Management Studio is not installed on your system, you can download it from the relevant section of Microsoft web site using the following URL:
<http://www.microsoft.com>

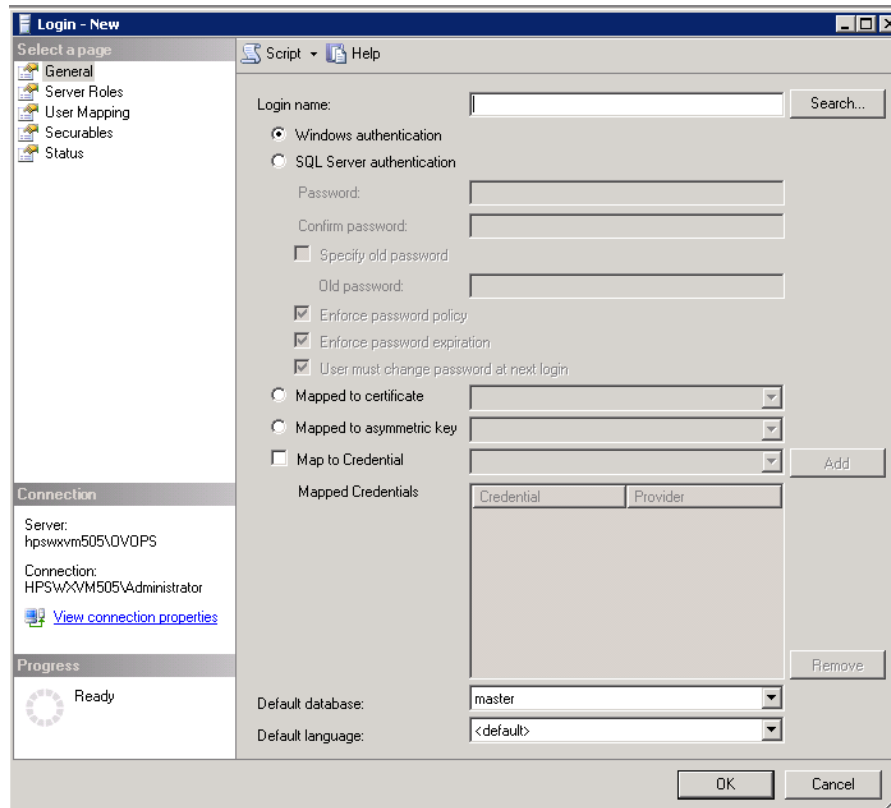
3. In the **Connect to Server** dialog box, select **NT Authentication** in the **Authentication** list, and then click **Connect**.



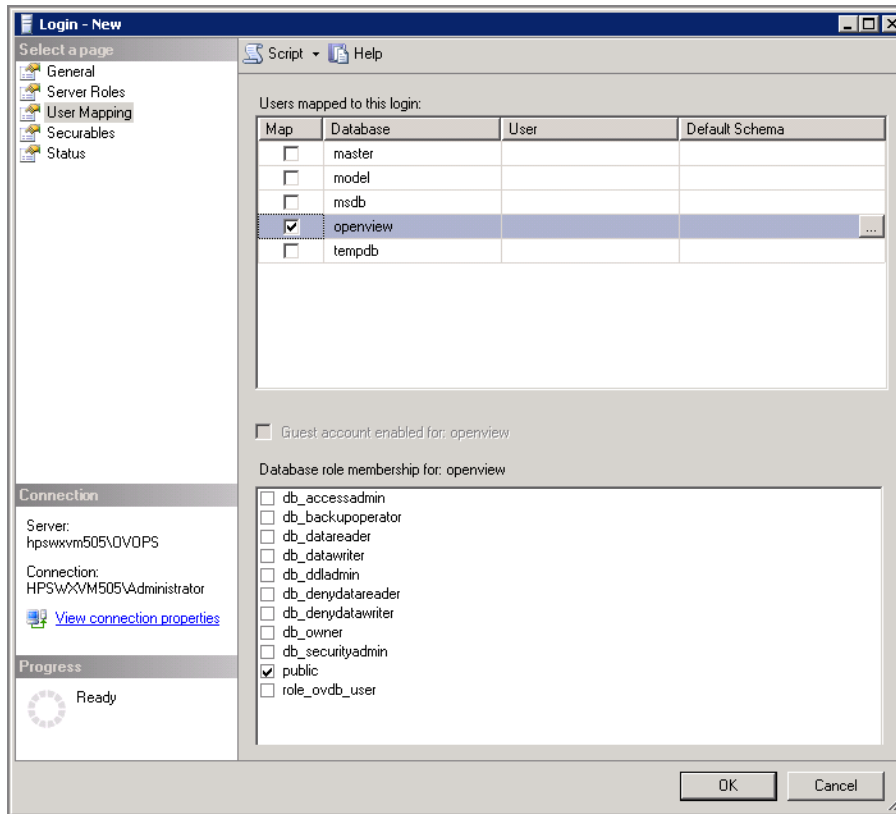
4. In the **Object Explorer** pane, expand **Security**.



5. Right-click **Login** and click **New Login**. The **Login - New** dialog box opens.



6. In **General**, type a user name for **Login name** field. Specify other necessary details.
7. Click **SQL Server authentication** option button.
8. In the **Password** field, type the password.
9. In the **Confirm password** field, retype the password. You can disable the password enforcement rules to create a simple password.
10. Click **User Mapping**.
11. In **Users mapped to this login**, select the **openview** check box.



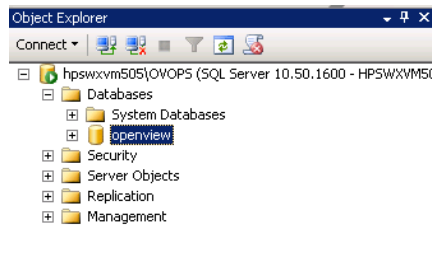
12. Click **OK** to create the user name and password.

Note: To create user name and password on HPOM system with embedded Microsoft SQL Server 2008, follow the same steps in [Task 1](#).

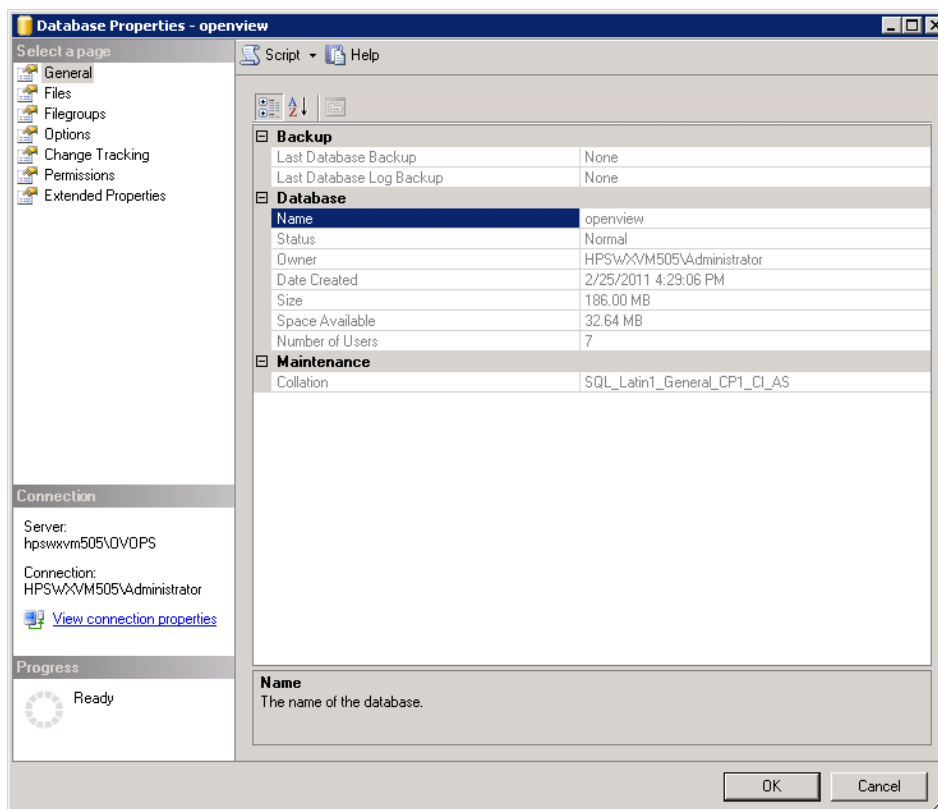
Task 2: Enable Connect and Select permissions

The database user must have at least the Connect and Select permissions. To enable Connect and Select permissions for the newly created user account, follow these steps:

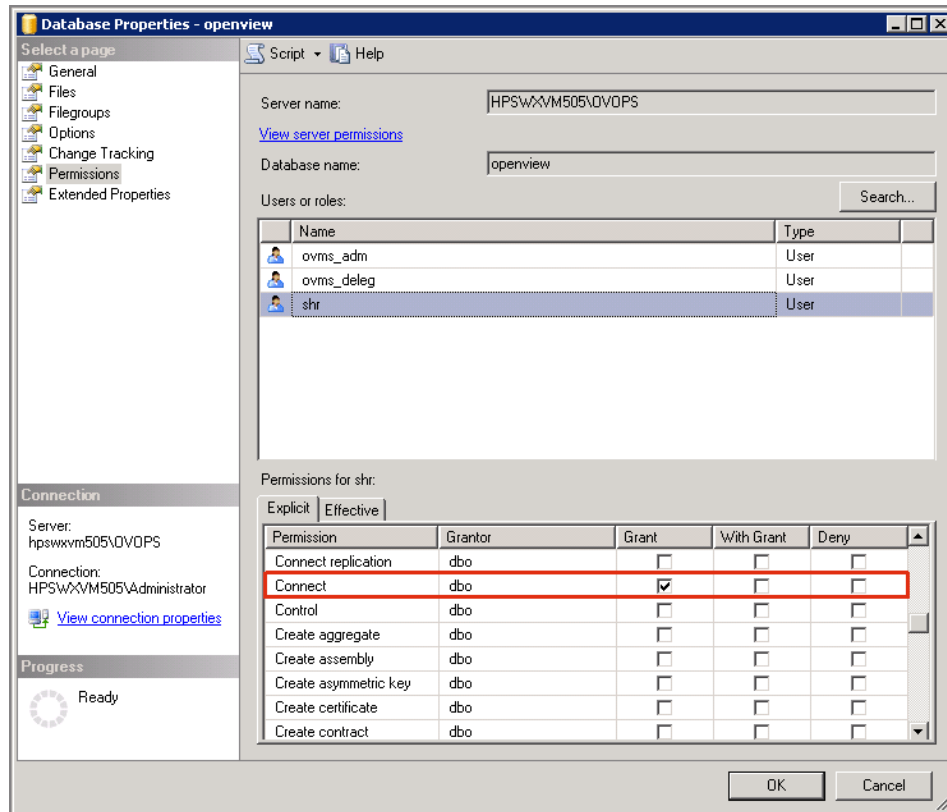
1. In the **Object Explorer** pane, expand Databases.



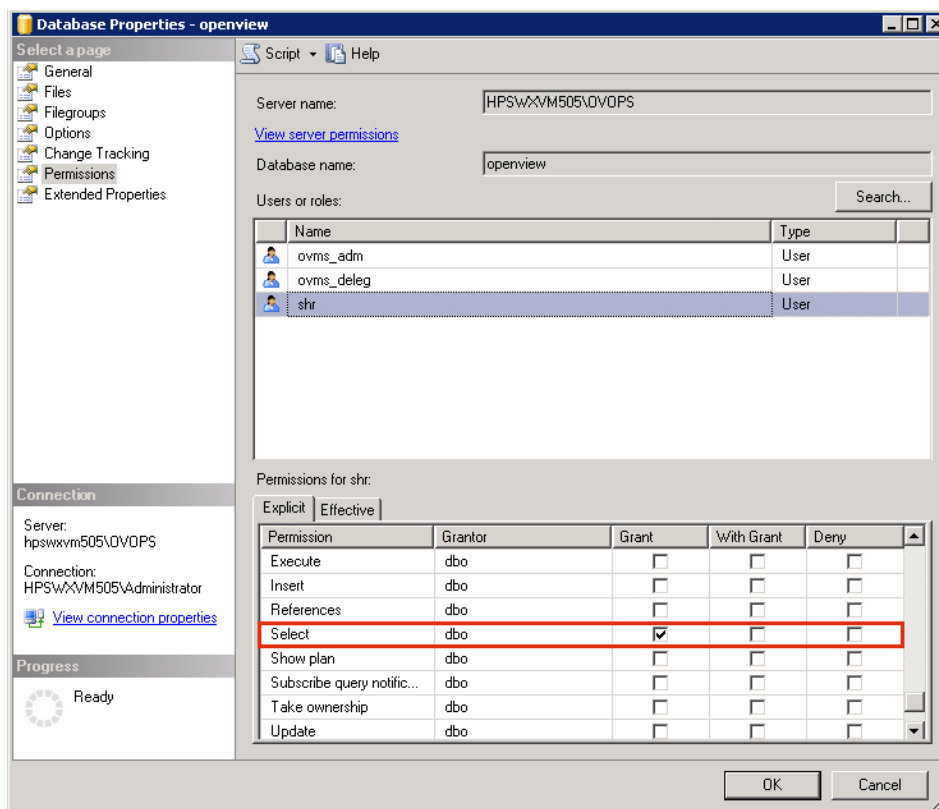
2. Right-click **openview** and then click **Properties**. The **Database Properties - openview** dialog box opens.



3. In the **Select a page** pane, click **Permissions**.
4. In the **Users or roles**, click the newly created user account.
5. In the **Explicit** tab of permissions for newly created user, scroll down to the **Connect** permission, and then select the **Grant** check box for this permission.



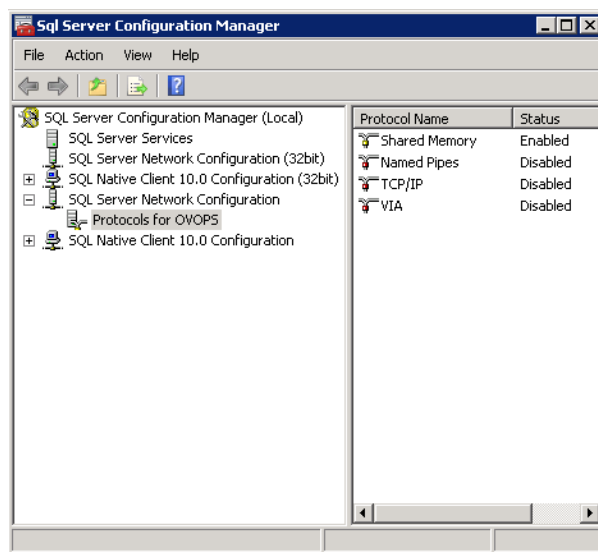
6. Scroll down to the **Select** permission and select the **Grant** check box for this permission.



7. Click **OK**.

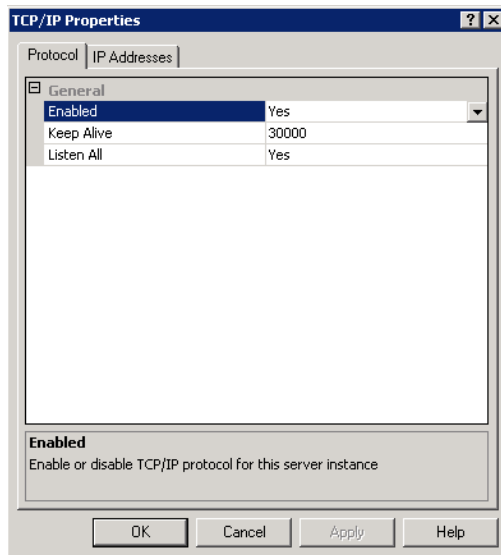
Task 3: Check for the HPOM server port number

1. Click **Start > Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**. The **SQL Server Configuration Manager** window is displayed.
2. Expand **SQL Server Network Configuration** and select **Protocols for OVOPS**. If the instance name has been changed, select the appropriate instance name.



3. On the right pane, right-click **TCP/IP**, and then click **Enable**.

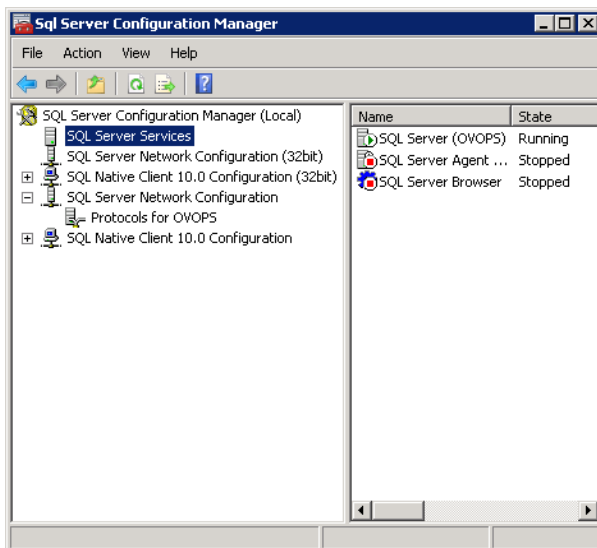
4. Right-click **TCP/IP** again, and click **Properties**. The **TCP/IP Properties** dialog box opens.



5. Click **IP Addresses** tab, under the IPAll, note down the port number.

Task 4: Restart the HPOM database server

1. In the **SQL Server Configuration Manager** window, click **SQL Server Services**.



2. On the right pane, right-click **SQL Server (OVOPS)**, and then click **Restart**.

You can use the newly created user name, password, and the observed instance name and port number when configuring the HPOM data source connection in the Administration Console.

Note: You can perform these steps by using the command prompt utility, `osql`. For more information, visit the Microsoft website at the following URL:

<http://support.microsoft.com>

Checking for the HPOM Server Port Number

If Microsoft SQL Server is the database type in HPOM, follow steps in [Task 3: Check for the HPOM server port number](#).

If Oracle is the database type in HPOM, follow these steps to check for the port number:

1. Log on the Oracle server.
2. Browse to the `$ORACLE_HOME/network/admin` or `%ORACLE_HOME%\NET80\Admin` folder.
3. Open the `listener.ora` file. The port number for the HPOM server is listed in the file.

Chapter 4: Primary Configuration

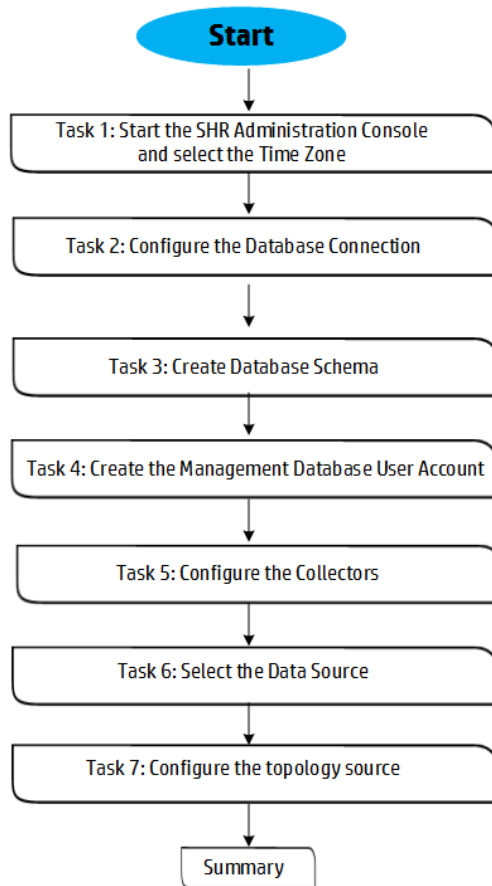
This section contains sub sections that describes tasks to complete primary or post-install configuration of SHR.

After SHR is installed and Administration Console is launched, the Configuration Wizard appears. Using the Configuration Wizard, you can configure SHR databases, collectors, and topology source. After completing tasks in Configuration Wizard, the Deployment Manager page is displayed. You can configure or install remaining package using the Pending Configuration page.

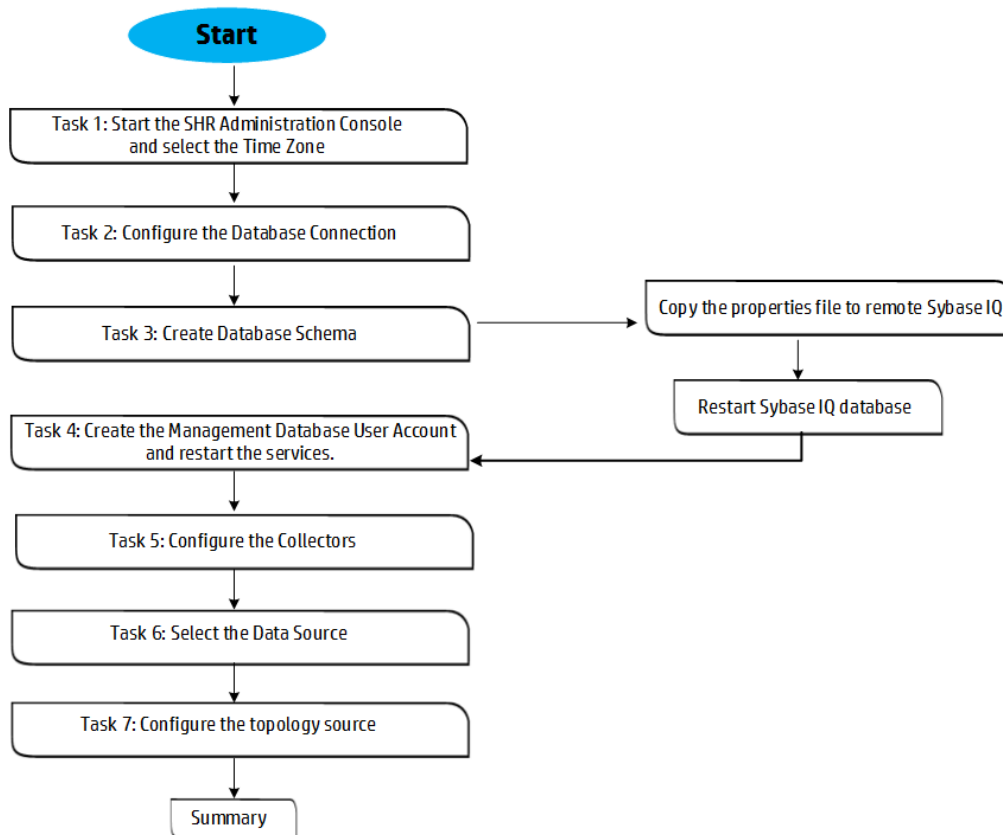
At this stage, if you do not configure the data sources using in Configuration Wizard, you can configure them later using the Collector Configuration page of the Administration Console.

Note: You must perform all the primary or post-install configuration tasks described in this chapter immediately after installing or upgrading SHR, and before installing the Content Packs through the Deployment Manager.

The following flowchart gives you an overview of the primary or post-install tasks for SHR where the SHR and Sybase IQ database are installed on the same system.



The following flowchart gives you an overview of the primary or post-install or post upgrade tasks for SHR with remote Sybase IQ database.



Task 1: Launching the Administration Console

1. Launch the Administration Console in a web browser using the following URL:

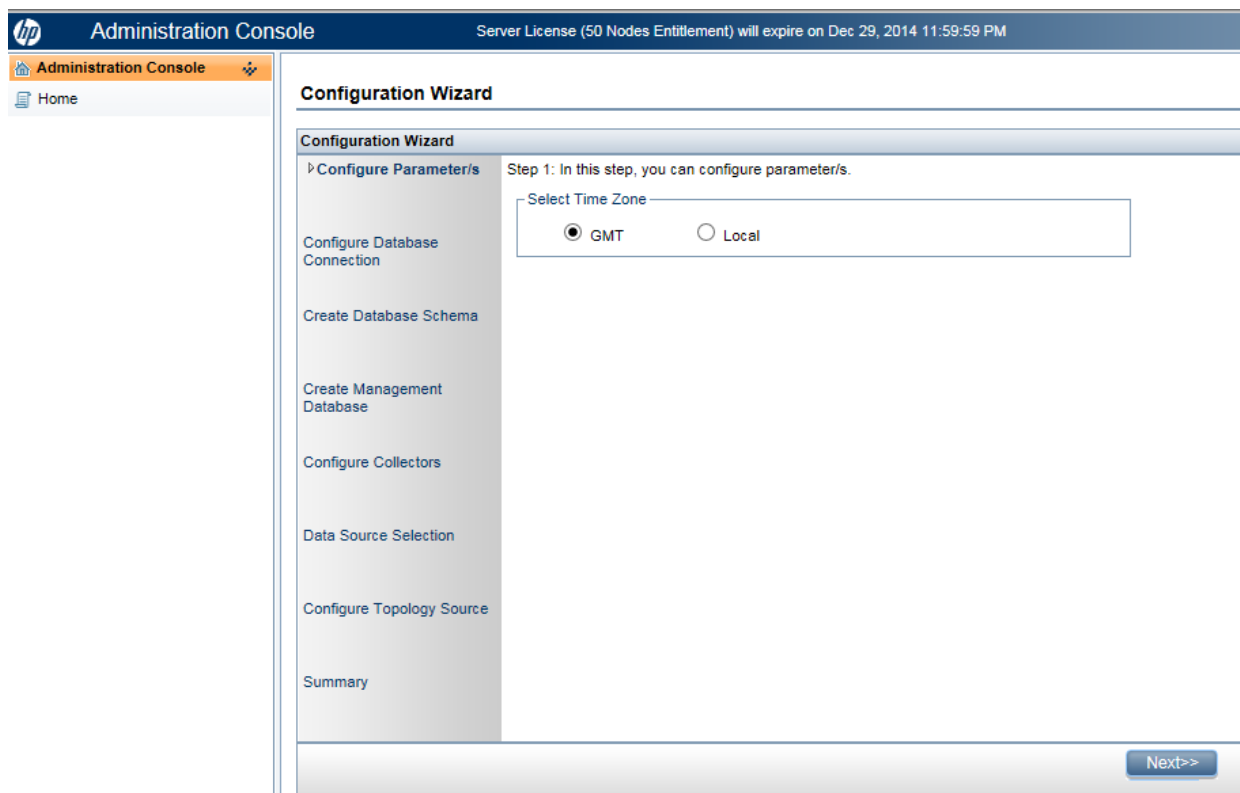
`http://<SHR_Server_FQDN>:21411`

2. Type **administrator** in the **Login Name** field and click **Log In** to continue. The **Home** page is displayed.

To set the password for the Administrator account, see [Create a Password for the Administrator Account](#).

Note: If you use any other user account to access the Administration Console, make sure that the user account has administrator privileges.

The following SHR Configuration Wizard appears only if you did not complete the post-install configuration tasks. The wizard supports session-state-persistence, which enables you to resume and continue a previously-interrupted configuration session.



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

Under Select HP Service Health Reporter Time Zone, perform any one of the following steps:

- Select **GMT** if you want SHR to follow the GMT time zone.
- Select **Local** if you want SHR to follow the local system time zone.

Note: The time zone that you select here applies to the SHR system and reports. However, the run-time information for processes like collection and work flow streams is always based on local time zone irrespective of selection.

4. Click **Next**. The **Configure Database Connection** page is displayed.

Task 2: Configure the Database Connection

In the **Configure Database Connection** page, provide the details of the database server where you want to create a database for SHR.

To configure a database connection, follow these steps:

1. On the **Configure Database Connection** page, for the Database Connection Parameter, type the following values:

Field	Description
Remote Database	Select Remote Database if SHR is installed with remote Sybase IQ.
Host name	Name or IP address of the host where the Sybase IQ database server is running.
Port	Port number to query the database server. The default port is 21424 .
Server name	Name of the Sybase IQ server. Ensure that the Sybase IQ server name is unique across the subnet. The server name displayed in this field is only for informational purposes. You must not change the server name at any time.

2. In **Enter Database User (DBA Privilege) and Password**, type the following values:

Field	Description
User name	Name of the Sybase IQ database user with DBA privileges. The default user name is <code>dba</code> .
Password	Password of the database user. The default password is <code>sql</code> . Once you complete the initial configuration, you can change the default password for the database user. To change the password for Database User (dba), see " Chapter 15: Change Password for SybaseIQ Database User (dba) " on page 117.

3. In **Enter Password For PMDB Database User**, type the following values:

Field	Description
Admin Password	Enter the new password for the PMDB Database User.
Confirm Admin Password	Retype the new password to confirm it.

4. Click **Next**. The **Create Database Schema** page is displayed.

Task 3: Creating the Database Schema

On the **Create Database Schema** page, specify the database deployment size. Based on your selection, SHR calculates and displays the recommended database size.

If Sybase IQ database is embedded with SHR, complete the task mentioned under [Creating Database Schema for Co-located Sybase](#).

If Sybase IQ database is located remotely, complete the task mentioned under [Creating Database Schema for Remote Sybase](#).

Creating Database Schema for Co-located Sybase

To create the database schema for Sybase IQ database that is installed on the SHR server, follow these steps:

1. In **Select Deployment Size**, select one of the following data volumes based on your requirements:

Note: You can use the *Licensing and Sizing Calculator* tool to calculate the deployment size from the following URL: <https://hpln.hp.com/group/service-health-reporter>.

Field	Description
Small	This option enables SHR to support data collection from 500 to 5,000 nodes.
Medium	This option enables SHR to support data collection from 5,000 to 10,000 nodes.
Large	This option enables SHR to support data collection from 20,000 nodes.

You can decide upon the deployment size based on the node count, content packs to be installed and the CI count. For more information on deployment size selection, see *HP Service Health Reporter Performance, Sizing, and Tuning Guide*.

2. In **Recommended IQ Configuration**, based on the deployment size you selected, the default values are set in the IQ fields:

Note: You can change the default values of IQ DBSpace Size (MB) and IQ Temporary DBSpace Size (MB) fields. As per the requirement you can set the values to more than the default values. However, it is recommended that you retain at least the default values and not to modify the values to less than the default values.

Field	Description
IQ Main Cache (MB)	The recommended size of the main buffer cache for the Sybase IQ main store. This value is set by default and depends on the deployment size selected.
IQ Temporary Cache(MB)	The recommended size of the temporary buffer size for the Sybase IQ temporary store. This value is set by default and depends on the deployment size selected.
IQ DBSpace Size (MB)	The recommended size for the IQ_System_Main dbspace, which stores the main database files. This size can be modified depending on the deployment size selected. <div style="border: 1px solid gray; padding: 5px; background-color: #f0f0f0;"> <p>Note: SHR adds additional database space in the same location as the space utilization reaches 80%. Ensure that sufficient free space is available in the file system to create new database files, if required.</p> </div>
IQ Temporary DBSpace Size (MB)	The recommended size for the IQ_System_Temp dbspace, which stores the temporary database files. This size can be

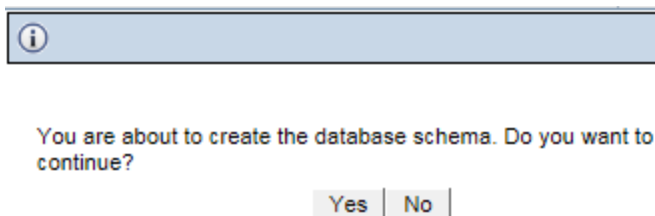
Field	Description
	modified. Note: Unlike IQ DBSpace Size, SHR does not add additional database space for IQ Temporary DBSpace Size. Ensure that you mention at least the recommended size for temporary database space and not reduce the value than what is recommended. You cannot customize this size and may lead to insufficient temporary database space issues.

3. In the **Database File Location** field, type the location where the database files will be stored.

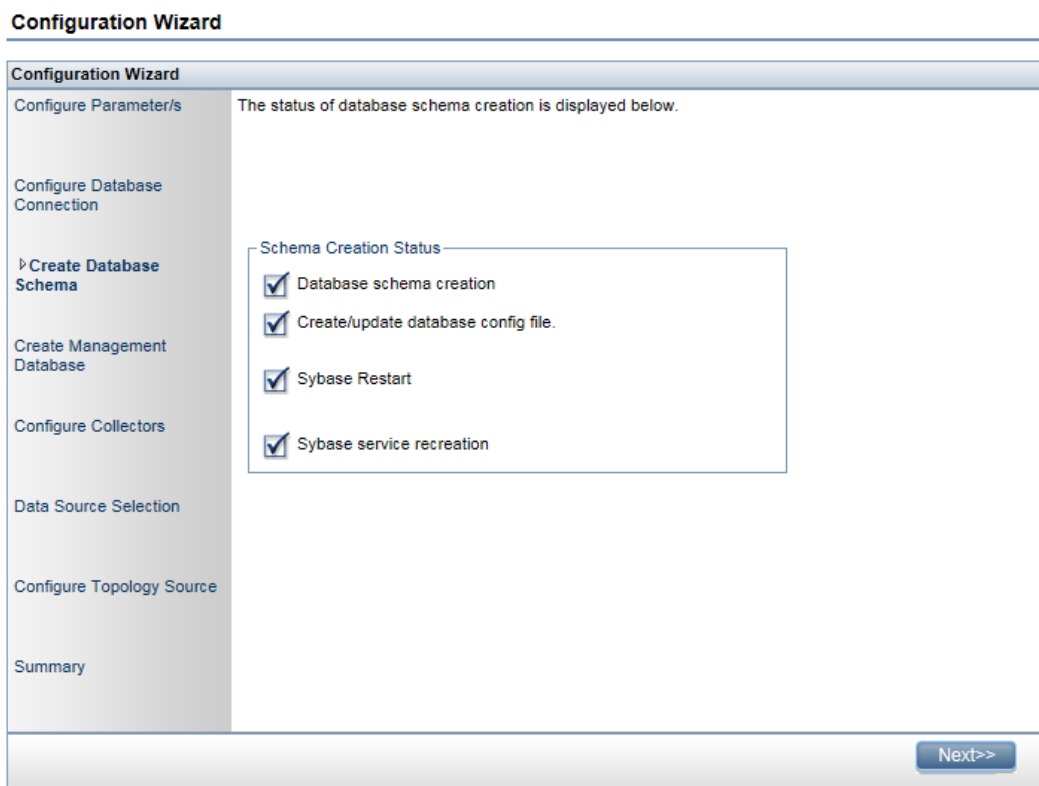
Example, for Windows C:\HP-SHR\Sybase\db and for Linux /opt/HP/BSM/Sybase/db.

Caution: Ensure that you have sufficient system resources to support the SHR data collection volume that you select. For information about the resource requirements for the selected volume, see the *HP Service Health Reporter Performance, Sizing, and Tuning Guide* and *HP Service Health Reporter Support Matrix*.

- a. Click **Next**. A confirmation dialog box is displayed.



- b. Click **Yes**. If the database connection and schema creation is successful, a confirmation page appears with the schema creation status.



- c. Click **Next** to continue.
- d. If the database connection and schema creation fails, click the **Previous** button to check the values provided.

Creating Database Schema for Remote Sybase

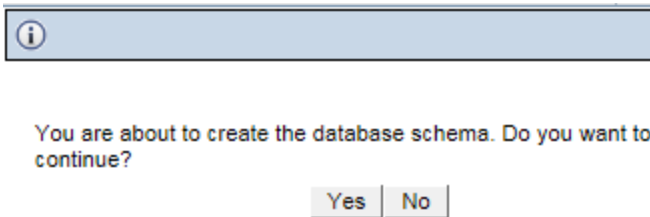
If SHR is installed with remote Sybase IQ, follow these steps:

1. Complete steps 1 and 2 mentioned under "[Creating Database Schema for Co-located Sybase](#)" on [page 40](#).
2. In the Database File Location field, type the location where the database files will be stored. For example, for Windows C:\HP-SHR\Sybase\db and for Linux /opt/HP/BSM/Sybase/db.

You must manually create the database folder before typing the path in the Database File Location field.

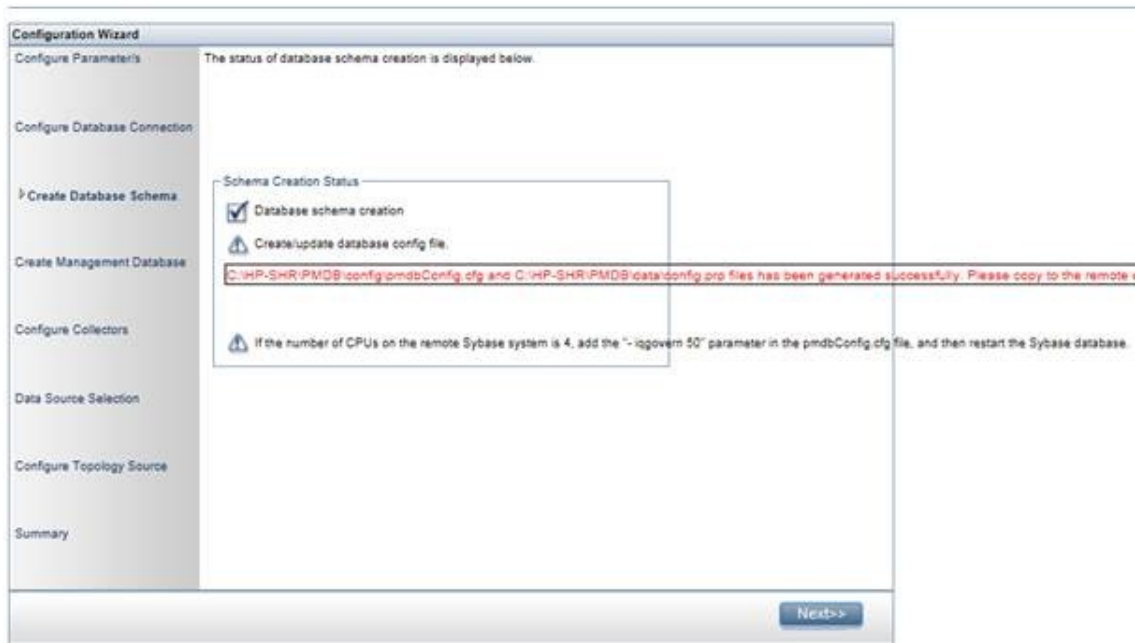
Caution: Ensure that you have sufficient system resources to support the SHR data collection volume that you select. For information about the resource requirements for the selected volume, see the *HP Service Health Reporter Support Matrix*.

3. Click **Next**. A confirmation dialog box opens.



Validate the existence of the database folder on the remote database host machine.

4. Click **Yes**. If the database connection and schema creation is successful, a confirmation page opens with the schema creation status.



5. Copy the newly created `pmdbConfig.cfg` file and the `config.prp` file to the corresponding folder in the remote system, and then restart the database. To copy the files to the remote system, follow the instructions on the Configuration Wizard.

Note: If SHR and SAP BusinessObjects are installed on the Windows operating system while SAP Sybase IQ is installed on the Linux operating system, run the following commands from the command line console of the Sybase IQ system after creating the Sybase database schema:

- `dos2unix $PMDB_HOME/data/config.prp`
- `dos2unix $PMDB_HOME/config/pmdbConfig.cfg`

6. To recreate the `HP_PMDB_Platform_Sybase` service, follows these steps:

On Windows:

Task 1: Stop and delete the `HP_PMDB_Platform_Sybase` service

- a. Click **Start > Run**. The **Run** dialog box appears.
- b. Type `services.msc` in the **Open** field, and then press **ENTER**. The **Services** window appears.

- c. On the right pane, right-click **HP_PMDB_Platform_Sybase**, and then click **Stop**.

Note: Go to Task Manager and ensure that `iqsrv` is not running.

- d. Open the command prompt and run the following command to delete the `HP_PMDB_Platform_Sybase` service:

```
sc delete "SQLANYs_HP_PMDB_Platform_Sybase"
```

Task 2: Create the HP_PMDB_Platform_Sybase service

- a. Open the command prompt and go to `%PMDB_HOME%/bin`.
- b. Run the following command to create the `HP_PMDB_Platform_Sybase` service:

```
sybaseServiceCreation.bat -install %PMDB_HOME%\..\ %PMDB_HOME%\..\
```

On Linux:

- a. Run the following command:

```
service HP_PMDB_Platform_Sybase restart
```

7. Click **Next** to continue.

Note: If the database connection and schema creation fails, click the **Previous** button to check the values provided.

Validating Remote Sybase Database Schema Creation

You must validate the following after successfully creating the Sybase database schema:

- **Check if Sybase IQ database is created.**

Verify if the following files are available in the database folder (that you entered in the Database File Location field).

- `pmdb.db`
- `pmdb.iq`
- `pmdb.iqmsg`
- `pmdb.iqtmp`
- `pmdb.lmp`
- `pmdb.log`
- `pmdb_user_main01.iq`

- **Check if the Sybase IQ database is running.**

- **On Windows:**

- Verify that `IQSRV15.exe` is visible in the **Process** tab of the **Task Manager**.

- **On Linux:**

- Run the `ps -ef|grep iqsrv15` command and verify if a `<process_id>` is returned.

- **Check connection to the Sybase IQ server.**

- **On Windows:**

- On the SHR system, click **Start > Run**. The Run dialog box opens.
- Type `dbisql` in the Open field and press **ENTER**. The **Connect** dialog box on Interactive SQL program opens.
- Type the following:
 - In the **User ID** field, type `pmdb_admin`
 - In the **Password** field, type the password you entered during post-install Sybase IQ database creation.
 - In **Action**, select **Connect to a database running on a different computer** or **Use an ODBC data source** from the drop down.
 - In the **Server Name** field, type the name of the server where the SHR Sybase IQ database is installed.

Tip: Open the `pmdbConfig.cfg` file. The server name is the text following `-n`.

- **On Linux:**

Run the following command:

```
dbisql -nogui -c "uid=pmdb_admin;pwd=<Password entered during Sybase IQ DB creation>;dbn=pmdb;eng=<server_name>;commlinks=tcpip(host=<host_name>;port=21424)"
```

Example

```
dbisql -nogui -c "uid=pmdb_admin;pwd=<Password entered during Sybase IQ DB creation>;dbn=pmdb;eng=abc;commlinks=tcpip(host=abc.com;port=21424)"
```

Create DSN for Sybase IQ Database

You have to create DSN to connect to Sybase IQ database if you have installed SAP BusinessObjects and SHR on different systems.

Note: You have to create the DSN on the system where SAP BusinessObjects is installed.

To create DSN to connect to Sybase IQ database, follow these steps:

On Windows:

Create 64-bit DSN (SHRDB)

1. Log on to the system where SAP BusinessObjects is installed with administrator privileges.
2. From the command prompt, type the following commands to navigate to the `Bin64` directory of Sybase.

```
cd %SYBASE%  
cd IQ-16_0\Bin64
```

3. Enter the following command to establish connection with the Sybase IQ database:

```
iqdsn -y -ws SHRDB -c "uid=pmdb_admin;pwd=<Sybase_db_password>;eng= <Sybase_server_engine>;dbf='<Sybase_db_path>\pmdb.db';links=tcpip{host= <Sybase_system_hostname>;port=21424}" -v -pe
```

Example

```
C:\HP-SHR\Sybase\IQ-16_0\Bin64>iqdsn -y -ws SHRDB -c "uid=pmdb_admin;pwd=pmdb_admin;eng= abc123;dbf='C:\ShrDB\pmdb.db';links=tcipip{host=abc123.example.com;port=21424}" -v -pe
```

where, *<Sybase_server_engine>* - short host name of the Sybase IQ database server.

<Sybase_db_password> - password given while configuring the Sybase database.

<Sybase_db_path> - database file location to store the database files provided while creating the database schema in [step 3](#).

<Sybase_system_hostname> - Sybase IQ database hostname.

Note: If you change the password of the Sybase IQ database, you must recreate the data source name (DSN).

Create 32-bit DSN (BSMR)

1. Log on to the system where SAP BusinessObjects is installed with administrator privileges.
2. Enter the following commands into the command prompt to navigate to the *Bin32* directory of Sybase:

```
cd %SYBASE%  
cd IQ-16_0\Bin32
```

3. Enter the following command to establish connection with the Sybase IQ database:

```
iqdsn -y -ws BSMR -c "uid=pmdb_admin;pwd=<Sybase_db_password>;eng= <Sybase_server_engine>;dbf='<Sybase_db_path>\pmdb.db';links=tcipip{host= <Sybase_system_hostname>;port=21424}" -v -pe
```

Example

```
C:\HP-SHR\Sybase\IQ-16_0\Bin32>iqdsn -y -ws BSMR -c "uid=pmdb_admin;pwd=pmdb_admin;eng= abc123;dbf='C:\ShrDB\pmdb.db';links=tcipip{host=abc123.example.com;port=21424}" -v -pe
```

<Sybase_server_engine> - short host name of the Sybase IQ database server.

<Sybase_db_password> - password given while configuring the Sybase database.

<Sybase_db_path> - database file location to store the database files provided while creating the database schema in [step 3](#).

<Sybase_system_hostname> - Sybase IQ database hostname.

On Linux:

Create 64-bit DSN (SHRDB)

1. Open a new Command Line Interface (CLI) session; close any existing CLI sessions.
2. Log on to the system where SAP BusinessObjects is installed as a root user.
3. Enter the following command into the command line to navigate to the *Bin64* directory of Sybase:

```
cd /opt/HP/BSM/Sybase/IQ-16_0/bin64/
```

4. Enter the following command to establish connection with the Sybase IQ database:

```
[root@<BusinessObjects_system_hostname> bin64] ./iqdsn -y -w SHRDB -c "uid=pmdb_admin;pwd=<Sybase_db_password>;eng=<Sybase_server_engine>;dbf='<Sybase_db_path>/pmdb.db';links=tcipip{host=<Sybase_system_hostname>;port=21424}" -v -pe
```

Example

```
[root@alpha1 bin64]./iqdsn -y -w SHRDB -c "uid=pmdb_admin;pwd=pmdb_admin;eng=abc123;dbf='/db/pmdb.db';links=tcPIP {host=abc123.example.com;port=21424}" -v -pe
```

<Sybase_server_engine> - short host name of the Sybase IQ database server.

<Sybase_db_password> - password given while configuring the Sybase database.

<Sybase_db_path> - database file location to store the database files provided while creating the database schema in [step 3](#).

<Sybase_system_hostname> - Sybase IQ database hostname.

Create 32-bit DSN (BSMR)

1. Open a new command line interface (CLI) session; close any existing CLI sessions.
2. Log on to the system where SAP BusinessObjects is installed as a root user.
3. Enter the following command into the command line to navigate to the *Bin32* directory of Sybase:

```
cd /opt/HP/BSM/Sybase/IQ-16_0/bin32/
```

4. Enter the following command to establish connection with the Sybase IQ database:

```
[root@<BusinessObjects_system_hostname> bin32]# su SHRBOADMIN  
[SHRBOADMIN@<BusinessObjects_system_hostname> bin32]-c "iqdsn -y -w BSMR -c \"uid=pmdb_admin;pwd=<Sybase_db_password>;eng=<Sybase_server_engine>;dbf=' /<Sybase_db_path>/pmdb.db';links=tcPIP {host=<Sybase_system_hostname>;port=21424}\" -v -pe"
```

Example

```
[root@alpha1 bin32]# su SHRBOADMIN  
[SHRBOADMIN@alpha1 bin32]-c "iqdsn -y -w BSMR -c \"uid=pmdb_admin;pwd=pmdb_admin;eng=abc123;dbf='/db/pmdb.db';links=tcPIP {host=abc123.example.com;port=21424}\" -v -pe"
```

<Sybase_server_engine> - short host name of the Sybase IQ database server.

<Sybase_db_password> - password given while configuring the Sybase database.

<Sybase_db_path> - database file location to store the database files provided while creating the database schema in [step 3](#).

<Sybase_system_hostname> - Sybase IQ database hostname.

Note: If you change the password of the Sybase IQ database, you must recreate the data source name (DSN).

Task 4: Creating the Management Database User Account

The management database refers to the Online Transaction Processing (OLTP) store used by SHR to store its run-time data such as data process job stream status, changed tables status, and data source information.

On the **Create Management Database** page, provide the user details for the management database.

To create the management database user account:

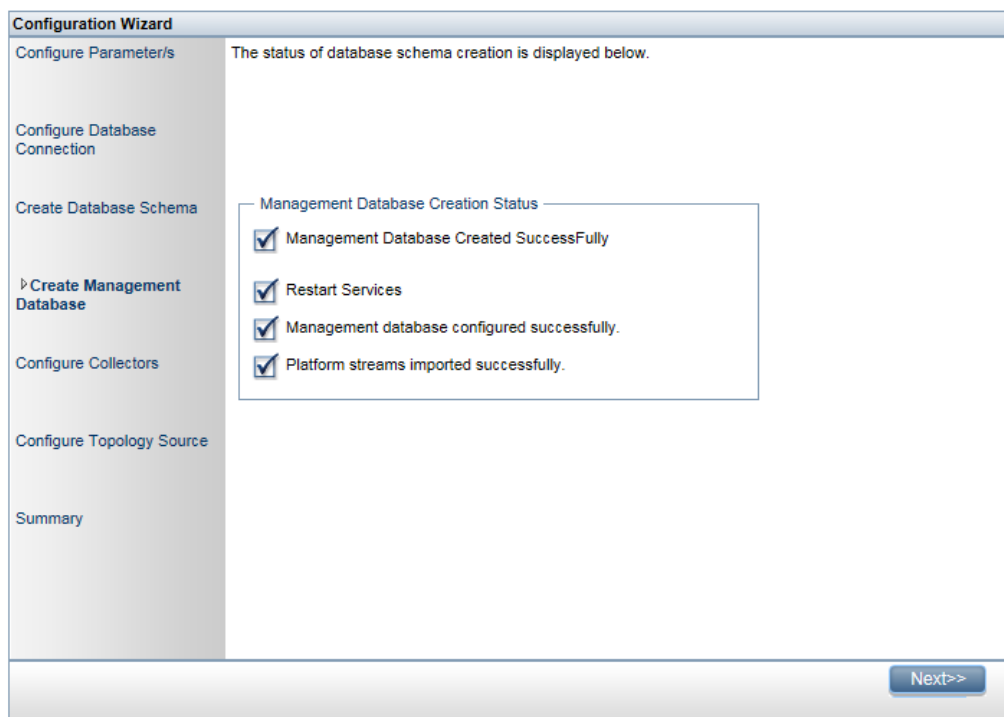
1. In the **Enter Management Database User (DBA Privilege) and Password**, type the following values:

Field	Description
User name	Name of the PostgreSQL database administrator. The default value is <i>postgres</i> .
Password	Password of the PostgreSQL database administrator. The default is <i>PMDB92_admin@hp</i> .

2. In the **Enter SHR Management Database User Information**, type the following values if you want to change the password of the management database user:

Field	Description
User name	Name of the management database user. <i>pmdb_admin</i> is the default password if the SAP BusinessObjects database password is not changed.
New Password	Password of the management database user.
Confirm New Password	Retype the same password to confirm it.

3. Click **Next**. The **Management Database Creation Status** page is displayed.
4. Review the tasks completed as part of database connection and management database details and then click **Next**. The **Configure Collectors** page is displayed.



Task 5: Configuring the Collectors Installed on Remote Systems

Before you proceed to configure the collector, it is mandatory to run the following command on the remote system. The command ensures that a certificate is exchanged between the SHR system and the collector system; this exchange sets up the communication channel between SHR and the collector:

Note: Run the following command only if only if HP Operations Agent does not coexist with SHR.

On Windows:

```
"perl %PMDB_HOME%\bin\scripts\configurePoller.pl <SHR system's fully qualified hostname>"
```

On Linux:

```
"perl $PMDB_HOME/bin/scripts/configurePoller.pl <SHR system's fully qualified hostname>"
```

Note: You can configure an instance of collector to use only one instance of SHR. Configuring a collector with multiple instances of SHR is not supported.

On the **Configure Collectors** page, you can create new collector, delete existing or connect application to the existing collectors.

1. On the **Configure Collectors** page, click **Create New**.

The **Configuration Parameters** section appears, type the following values:

Field	Description
Name	Display name of the collector that is installed on a remote system. The name must not contain spaces or special characters.
Host name	Collector host name

2. Click **OK** to complete the creation of the collector, and then click **Save**.
3. Click **Test Connection** to check the status of the connection.

If the status report shows Test Connection Failed, follow these steps:

- a. Log on to the collector system.
- b. Check that the **HP_PMDB_Platform_Collection** is started.
If the service is not started, manually start the service.
- c. To start the service manually, follow these steps:

On Windows:

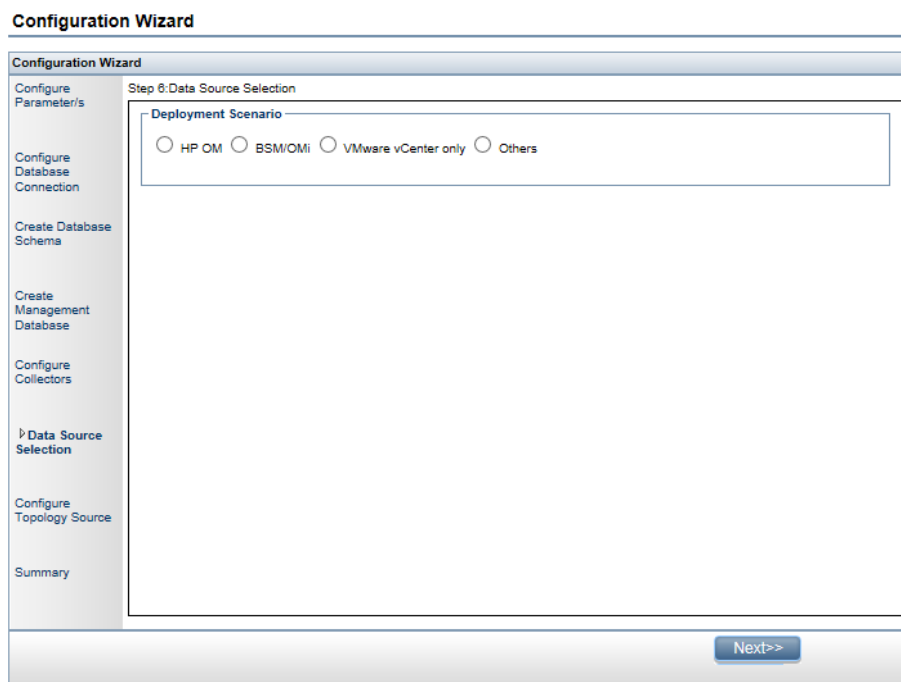
- o Open the **Services** window, right-click the **HP_PMDB_Platform_Collection** service, and then click **Start**.

On Linux:

- Go to the /etc/init.d directory, and then run the following command:
 service HP_PMDB_Platform_Collection start

Task 6: Selecting the Data Source

On the **Data Source Selection** page, specify the deployment scenario for which the data sources and other options are selected.



Select one of the **Deployment Scenarios** - **HP OM**, **BSM/OMi**, **VMWare vCenter only**, or **Others**.

The following table provides areas that can be monitored in each deployment scenario:

Deployment Scenario	Areas of Monitoring
HP OM	<ul style="list-style-type: none"> • System Performance <ul style="list-style-type: none"> • HP Operations Agent • Virtual Environment Performance <ul style="list-style-type: none"> • HP Operations Agent • VMware vCenter • Network Performance • Operations Events <ul style="list-style-type: none"> • HPOM Events • Enterprise Application Performance <ul style="list-style-type: none"> • Microsoft SQL Server

Deployment Scenario	Areas of Monitoring
	<ul style="list-style-type: none"> • Microsoft Exchange Server • Microsoft Active Directory • Oracle • Oracle Weblogic Server • IBM Webshpere Application Server
<p>BSM/OMi BSM 9.2x or OMi 10</p>	<ul style="list-style-type: none"> • System Performance <ul style="list-style-type: none"> • HP Operations Agent • SiteScope • Virtual Environment Performance <ul style="list-style-type: none"> • HP Operations Agent • SiteScope • VMware vCenter • Network Performance <ul style="list-style-type: none"> • NNMi integrated with BSM/OMi • Operations Events and KPI <ul style="list-style-type: none"> • HPOM Events • OMi Events • HP Service Health • HP End User Monitoring <ul style="list-style-type: none"> • HP Real User Monitor • HP Business Process Monitor • Enterprise Application Performance <ul style="list-style-type: none"> • Microsoft SQL Server • Microsoft Exchange Server • Microsoft Active Directory • Oracle • Oracle Weblogic Server • IBM Webshpere Application Server

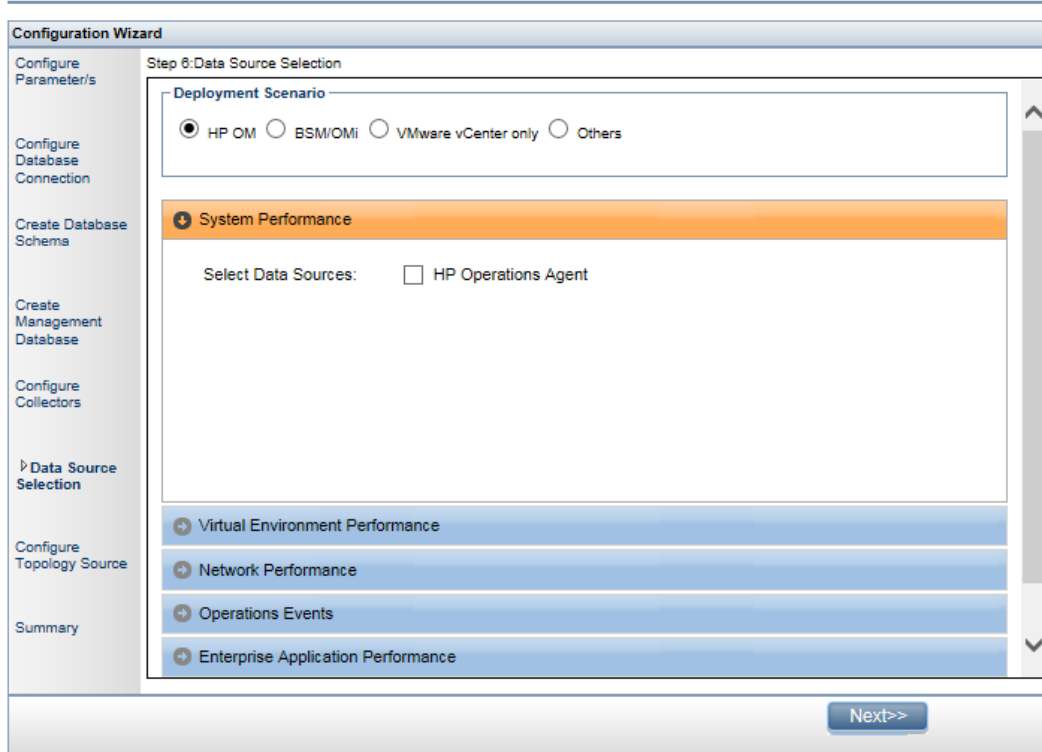
Deployment Scenario	Areas of Monitoring
VMware vCenter only	<ul style="list-style-type: none"> Virtual Environment Performance Network Performance
Others	<ul style="list-style-type: none"> Network Performance

Data Sources for the HPOM Deployment Scenario

To collect data for HPOM, follow these steps:

1. In the **Deployment Scenario**, click **HP OM**.

Configuration Wizard



2. In the **System Performance**, select **HP Operations Agent**.
3. (Optional). In the **Virtual Environment Performance**, select the data source for virtual environment.
4. (Optional). In the **Network Performance**, select **NNMi integrated with BSM/OMi** if NNMi and the NNMi SPI Performance is available in your environment.
5. In the **Operations Event**, select **HPOM Events** for events.
6. In the **Enterprise Application Performance**, select the data source for the Smart Plug-in (SPI) monitored by HPOM.

Note: If you select Microsoft Exchange Server, the **Select Version of MS Exchange Server** section appears. You must select the version of the Exchange Server.

7. Click **Save**. A summary of all the selection is displayed.
8. Click **Next**. The **Configure Topology Sources** page appears.

Data Sources for the BSM or OMi Deployment Scenario

You must configure the following data collectors in SHR:

- **Database collector** - to collect historical Synthetic Transaction Monitoring (BPM) and Real User Monitoring (RUM) data from the BSM database. It also collects events, messages, availability, and performance Key Performance Indicators (KPIs) from the databases of data sources such as Profile database, HPOM, and HP OMi databases.
- **HP Operations Agent collector** - to collect system performance metrics and data related to applications, databases, and system resources. The data is collected by the HP Operations Agents that are installed on the managed nodes.

To collect data for BSM or OMi, follow these steps:

1. In the **Deployment Scenario**, click **BSM/OMi**.

Configuration Wizard

Step 6: Data Source Selection

Deployment Scenario

HP OM BSM/OMi VMware vCenter only Others

Version of BSM/OMi

Version of BSM/OMi: BSM 9.2x OMi 10.x

System Performance

Select Data Sources: HP Operations Agent SiteScope

Virtual Environment Performance

Network Performance

Next>>

2. In the **Version of BSM/OMi**, select the version of the application.

You can select either **BSM 9.2x** or **OMi 10.x** or both **BSM 9.2x** and **OMi 10.x** together. For additional deployment configurations using BSM and OMi, see:

- ["OMi10 Topology Source with Integrated BSM"](#)
- [" OMi10 Topology Source after BSM Upgrade"](#)

3. In the **System Performance**, select the required data source for the system.
 - a. If you select **SiteScope** for system performance, then **SiteScope Metric Channel** section appears.
 - b. You must select either **Profile DB** or **Direct API** as the metric channel for SiteScope.

Note: If SiteScope is used to monitor system or virtual environment performance in OMi 10.x, the metric channel for SiteScope is through Direct API.

4. (Optional). In the **Virtual Environment Performance**, select the data source for the virtual environment. Select the technology for the data source.

Data Source	Select Technology
HP Operations Agent	VMware IBM LPAR Microsoft Hyper-V Solaris Zones
SiteScope	VMware Note: For virtual environment performance, you must also select the metric channel. For OMi 10.x, you can collect data for SiteScope only through Direct API.
VMware vCenter	VMware

5. (Optional). In the **Network Performance**, select **NNMi integrated with BSM/OMi** if NNMi and the **NNMi SPI Performance** is available in your environment.
6. In the **Operations Event and KPI**, select the data sources for required events.
7. In the **HP End User Monitoring**, select the data source for the components monitored by BSM.

Note: If the deployment is for OMi 10.x, this parameter is disabled.

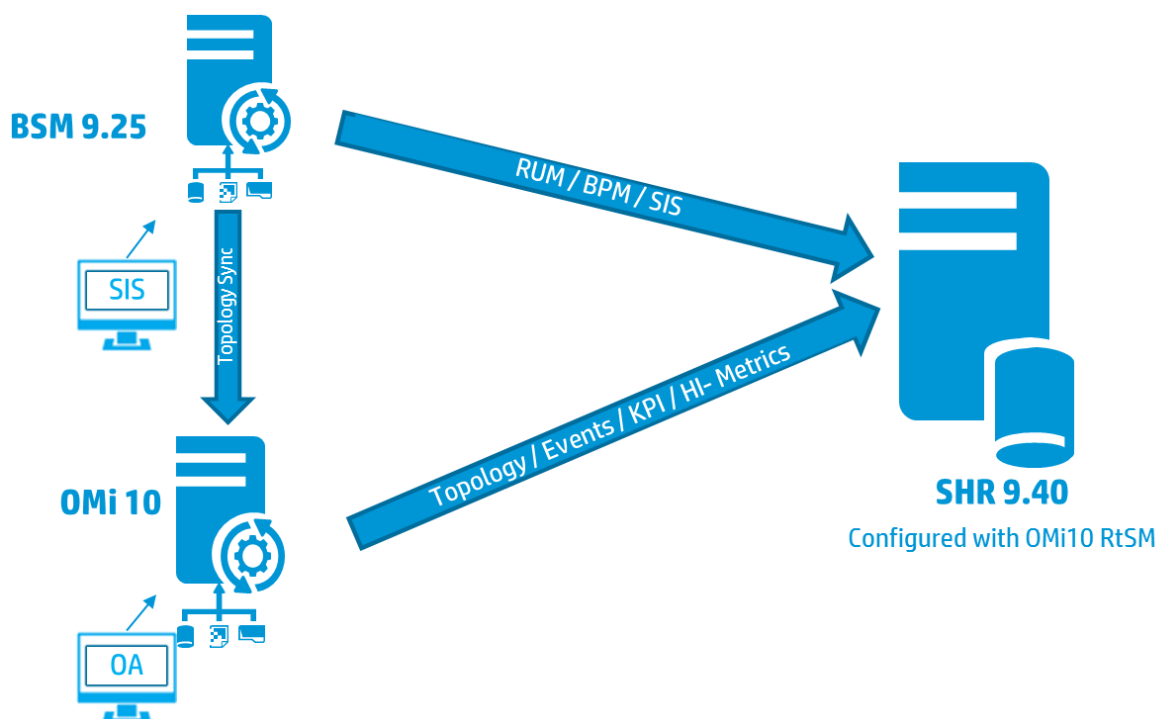
8. In the **Enterprise Application Performance**, select the data source for the Management Packs monitored by OMi.
9. The **Select Technology** section appears after selecting required Management Pack, select the **Management Pack** check box.

Note: If you select Microsoft Exchange Server Management Pack, the **Select Version of MS Exchange Server** section opens. You must select the version of the Exchange Server.

10. Click **Save**. A summary of all the selection appears.
11. Click **Next**. The **Configure Topology Sources** page is displayed.

OMi10 Topology Source with Integrated BSM

While you can configure BSM and OMi10 as standalone topology and data sources, you can also setup BSM to synchronize topology data with the OMi10 system.



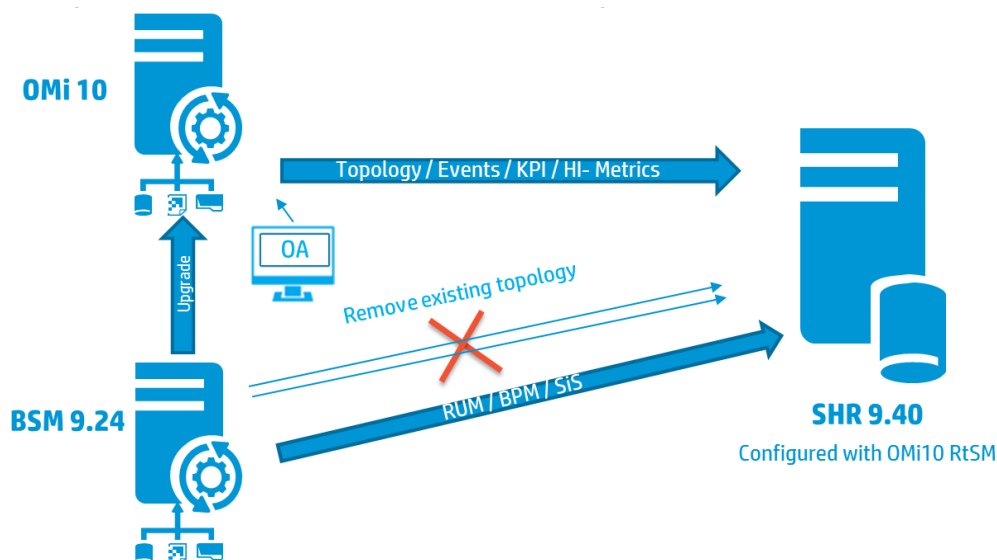
In this configuration, the OMi10 system provides topology data for all nodes and fact data for Operations Events and KPI. The BSM system provides fact data from RUM, BPM, and SiteScope that are directly monitored by BSM. For enabling topology sync between BSM and OMi10, see the respective documentation.

Note: Use the NPS RTSM ETL (**NetworkPerf_ETL_PerfiSPI_RTSM**) Content Pack component, if NNMI is integrated to OMi RTSM. Otherwise, use the non NPS RTSM ETL (**NetworkPerf_ETL_PerfiSPI_NonRTSM**) Content Pack component.

To configure the topology source in SHR, see ["Configuring RTSM Service Definition Source"](#) on page 61

OMi10 Topology Source after BSM Upgrade

While you can configure BSM and OMi10 as standalone topology and data sources, you can also upgrade your BSM system to an OMi10 system.



In this configuration, the existing topology synchronized between BSM system and SHR system is removed and the OMi10 system provides topology data for all nodes and fact data for Operations Events and KPI. The BSM system provides fact data from RUM, BPM, and SiteScope that are directly monitored by BSM.

Note: In this scenario, if you are already using NPS RTSM ETL (**NetworkPerf_ETL_PerfiSPI_RTSM**) when SHR was connected to BSM 9.2x then ensure that NNMI is integrated to OMi 10 RTSM after BSM is upgraded to OMi 10 and BSM 9.24.

In this configuration, after the BSM system is upgraded to OMi, all topology and fact data is collected from it. To perform the upgrade, follow these steps:

1. Stop data collection from the BSM and OMi systems.
Wait until all data is loaded into SHR tables.
2. Complete the BSM to OMi10 upgrade process.
3. From the **Administration Console > Administration > Deployment Manager** page:
 - a. Uninstall the older ETL component of BPM (**SynTrans_ETL_BPM**) and install the newer (**SynTrans_ETL_BPM_OMi10**) ETL component.
 - b. Uninstall the older ETL component of RUM (**RealUsrTrans_ETL_RUM**) and install the newer (**RealUsrTrans_ETL_RUM_OMi10**) ETL component.
 - c. Uninstall the older ETL component of OMi (**CrossOprEvent_ETL_OMi**) and install the newer (**CrossOprEvent_ETL_OMi10**) ETL component.

Note: You may also choose to install the OMi Extended ETL to generate customized reports that involves Event detail attributes.

- d. Uninstall the older ETL component of Service Health (**HIKPI_ETL_ServiceHealth**) and install the newer (**HIKPI_ETL_ServiceHealth_OMi10**) ETL component.

- e. Optionally, uninstall the SiteScope Profile database ETL (SysPerf_ETL_SiS_DB ETL) and install the SiteScope Direct API (SysPerf_ETL_SiS_API) ETL.
4. To modify the RTSM topology source for OMi, use the below update statement in Postgres DB:

```
update dict_cmdb_ds set hostname='<omi10hostname>';
```


where *<omi10hostname>*, is the hostname of your OMi10.
5. Log in to **SHR Administration Console > Topology Source**, and click **Configure** to modify the user name, password, and port as relevant for OMi10.
6. Add Operations database connection of OMi in **SHR Administration Console > Collection Configuration > BSM/OMi** page. For more details, see ["Configuring the Management and Profile Database Data Source" on page 78](#).
7. Enable HI/KPI Data Collection and optionally SiteScope.
8. Start the collection service.

Note: Ensure to configure the topology source to OMi10 in SHR soon after the upgrade and before starting the collection service. Otherwise SHR will continue to point and collect the data from BSM system even after upgrading to OMi10. During this period, if a new CI is discovered in BSM and this new CI is collected by SHR, it will end up being a duplicate in SHR when the topology is changed to OMi10. If you come across such situation, then use DLC to clean up the duplicates.

Data Source for the VMware vCenter Deployment Scenario

To collect data for VMware vCenter, follow these steps:

1. In the **Deployment Scenario**, click **VMware vCenter only**.

Configuration Wizard

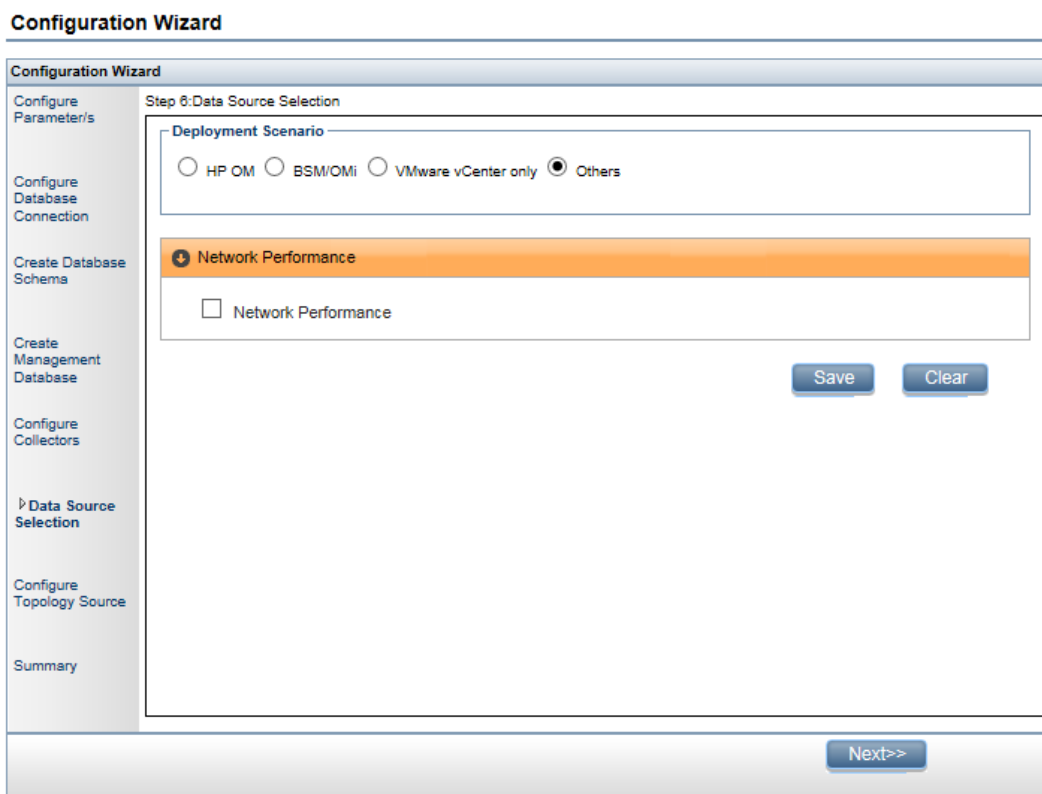
The screenshot shows the Configuration Wizard interface. On the left is a navigation pane with the following items: Configure Parameter/s, Configure Database Connection, Create Database Schema, Create Management Database, Configure Collectors, Data Source Selection (highlighted), Configure Topology Source, and Summary. The main content area is titled 'Step 6: Data Source Selection'. It contains a 'Deployment Scenario' section with four radio buttons: HP OM, BSM/OMI, VMware vCenter only (selected), and Others. Below this are two expandable sections: 'Virtual Environment Performance' (expanded, highlighted in orange) and 'Network Performance' (expanded, highlighted in blue). Under 'Virtual Environment Performance', there is a checkbox for 'VMware'. At the bottom right of the main content area are 'Save' and 'Clear' buttons. At the bottom right of the wizard is a 'Next>>' button.

2. In the **Virtual Environment Performance**, select **VMware**.
3. (Optional). In **Network Performance**, select **Network Performance** if NNMi and the NNMi SPI Performance is available in your environment.
4. Click **Save**. The **Saved Successfully** message is displayed.
5. Click **Next**. The **Configure the Topology Sources** page appears.

Data Sources for Other (Generic) Database Deployment Scenario

To collect data for other databases, follow these steps:

1. In the **Deployment Scenario**, click **Others**.



2. In the **Network Performance**, select **Network Performance** to collect metrics on your network environment.
3. Click **Save**. A summary of your selections is displayed.
4. Click **Next**. The **Configure Topology Sources** page appears.

Task 7: Configuring the Topology Source

Before you can configure SHR for data collection, you must configure the topology source. The topology source configuration tasks are organized into the following categories:

- If SHR is deployed in the BSM Service and Operations Bridge or Application Performance Management environment, see ["Configuring RTSM Service Definition Source" on the next page](#).
- If SHR is deployed in the HPOM environment, see ["Configuring HPOM Service Definition Source" on page 62](#).
- If SHR is deployed in the VMware vCenter environment, see ["Configuring vCenter Service Definition" on page 65](#).

Note: SHR uses the identifier of the Configuration Items (CI) from the topology source to uniquely identify them for reporting. Changing the topology source can result in duplicate CIs because different topology sources do not use the same identifier for a certain CI. So, once a certain topology source (RTSM, HPOM, or VMware vCenter) is configured, you cannot change it later.

Configuring RTSM Service Definition Source

To configure RTSM service definition source, follow these steps on the **Configure Topology Source** page:

1. In the **Service Definition Source**, click **RTSM**.
2. Click **Create New**. The **Connection Parameter** appears.
3. In the **Connection Parameter**, type the following details:

Field	Description
Host name	IP address or FQDN of the BSM or OMi server. If your HP BSM installation is distributed, type the name of the gateway server in the 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 default port number is 80. If the port number has been changed, contact your BSM administrator for more information.
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	If you installed collectors on remote systems, you can choose either the local collector or a remote collector. To configure a remote collector with this service definition source, select one of the available remote systems in the drop down list. To use the collector that was installed by default on the SHR system, select local.

4. Click **OK**.
5. Click **Save** to save the information.
6. Click **Test Connection**.

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

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

You can configure additional RTSM data sources by performing [step 2](#) to [step 7](#).

For more information about configuring RTSM service definition sources, see *Managing the enterprise topology* section in *HP Service Health Reporter Online Help for Administrators*.

8. Click **Next** to continue. The **Summary** page appears.
9. Click **Finish** to complete the post-install configuration tasks. The **Deployment Manager** page appears.

Configure Data Collection When HTTPS is Enabled for RTSM

If RTSM is HTTPS enabled, follow these steps:

1. Set the port to 443 when RTSM is HTTPS enabled during topology source configuration.
2. Import the BSM/OMi 10 root CA certificate into SHR cacerts trust store. To import the CA certificates, follow these steps:
 - **On Windows**

```
keytool -import -trustcacerts -keystore C:\HP-SHR\JRE64\lib\security\cacerts  
-file "<filename with path>"
```

- **On Linux**

```
keytool -import -trustcacerts -keystore  
/opt/HP/BSM/JRE64/lib/security/cacerts -file "<filename with path>"
```

where, *<filename with path>* is the location and file name of the BSM/OMi CA certificates.

Note: The password is changeit.

3. Add the following field in `config.prp`, located at `%PMDB_HOME%\data` (**on Windows**) `$PMDB_HOME/data` (**on Linux**):

Field	Value
ucmdb.protocol	https

Supported Data Source Selections

In this deployment scenario, you can configure the following data sources to collect fact data:

- ["Configuring the Management and Profile Database Data Source" on page 78](#)
- ["Configuring the HP OMi Data Source" on page 82](#)
- ["Configuring the HP Operations Manager Data Source" on page 72](#)
- ["Configuring the HP Operations Agent Data Source" on page 72](#)
- ["Configuring the Network Data Source \(using Generic Database\)" on page 73](#)
- ["Configuring the VMware vCenter Data Source" on page 74](#)
- ["Configuring the SiteScope Data Source" on page 75](#)

Configuring HPOM Service Definition Source

To configure HPOM service definition source, follow these steps on the **Configure Topology Source** page:

1. In the **Service Definition Source**, click **HP OM**.
2. Click **Create New**. The **Connection Parameter** section appears.
3. In the **Connection Parameter**, type the following details:

Caution: 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.

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. <div style="background-color: #f0f0f0; padding: 10px;"> <p>Note: The tables that queried by SHR are as follows:</p> <ul style="list-style-type: none"> • For OML: <ul style="list-style-type: none"> ◦ sto_ov_managednode ◦ sto_ov_nodegroup • For OMW: <ul style="list-style-type: none"> ◦ opc_node_names ◦ opc_nodes ◦ opc_node_groups </div>
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 in the data source. The default database instance is OVOPS. If MSSQL Server is configured to use default (unnamed) database instance, leave this field empty.
Port	Port number to query the HPOM database server. To check the port number for the database instance, such as OVOPS, see "Checking for the HPOM Server Port Number" on page 36 .

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. This option only appears if HPOM for Windows is selected as the data source type.
User name	Name of the HPOM database user. For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled and appears empty.
Password	Password of the HPOM database user. For the HPOM for Windows data source type, if the Windows Authentication option is selected, this field is disabled and appears empty.
Collection station	<p>If you installed collectors on remote systems, you can choose either the local collector or a remote collector.</p> <p>To configure a remote collector with this service definition source, select one of the available remote systems in the drop down list.</p> <p>To use the collector that was installed by default on the SHR system, select local.</p>

4. Click **OK**.
5. Click **Save** to save the information.
6. Click **Test Connection**.
7. In the message box, click **Yes**. A *Saved Successfully* message appears in the information message panel.

You can configure additional HPOM data sources by performing [step 2](#) to [step 7](#).

For more information about configuring HPOM service definition sources, see *Managing the enterprise topology* section in the *HP Service Health Reporter Online Help for Administrators*.

Note: To collect data from non-domain hosts, appropriate DNS resolutions must be made by the HPOM administrator for these hosts so that they are reachable by SHR, which is installed in the domain.

8. Click **Next** to continue. The **Summary** page appears.
9. Click **Finish** to complete the post-install configuration tasks. The **Deployment Manager** page appears.

Supported Data Source Selections

In this deployment scenario, you can configure the following data sources to collect fact data:

- ["Configuring the HP Operations Manager Data Source" on page 72](#)
- ["Configuring the HP Operations Agent Data Source" on page 72](#)

- ["Configuring the Network Data Source \(using Generic Database\)" on page 73](#)
- ["Configuring the VMware vCenter Data Source" on page 74](#)

Configuring vCenter Service Definition

To configure vCenter service definition, follow these steps on the **Configure Topology Source** page:

1. In the **Service Definition Source**, click **VMware vCenter**.
2. Click **Create New**. The **Connection Parameter** section appears.
3. In the **Connection Parameter**, type the following details:

Field	Description
Host name	IP address or FQDN of the vCenter server.
User name	Name of the vCenter web service user. The <code>administration@vsphere.local</code> is the default user name.
Password	Password of the vCenter web service user.
Collection station	If you installed collectors on remote systems, you can choose either the local collector or a remote collector. To configure a remote collector with this service definition source, select one of the available remote systems in the drop down list. To use the collector that was installed by default on the SHR system, select local.

4. Click **OK**.
5. Click **Save** to save the information.
6. Click **Test Connection**.
7. In the message box, click **Yes**. A `Saved Successfully` message appears in the information message panel.

You can configure additional vCenter data sources by performing [step 2](#) to [step 7](#).
8. Click **Next** to continue. The **Summary** page appears.
9. Click **Finish** to complete the post-install configuration tasks. The **Deployment Manager** page appears.

Restart the collector service

If you configured a remote collector with the service definition, make sure to restart the collector service on the collector system after installing Content Packs.

To restart the service manually, follow these steps:

On Windows:

- Open the Services window, right-click the **HP_PMDB_Platform_Collection** service, and then click **Restart**.

On Linux:

- Go to the `/etc/init.d` directory, and then run the following command:
`service HP_PMDB_Platform_Collection -restart`

Supported Data Source Selections

In this deployment scenario, you can configure the following data sources to collect fact data:

- ["Configuring the Network Data Source \(using Generic Database\)" on page 73](#)
- ["Configuring the VMware vCenter Data Source" on page 74](#)

Task 8: Summary

The **Summary** page presents a summary of all selections. Click **Finish**. The **Deployment Manager** page is displayed with Content Packs selected based on the selections made in the [data source configuration](#).

Chapter 5: Installing the Content Packs

For installing the required Content Packs, SHR provides the Deployment Manager utility through the Administration Console. This web-based interface simplifies the process of installation by organizing the Content Packs based on the domain, the data source applications from where you want to collect data, and the specific Content Pack components you want to install to collect the data.

Note: Stop the HP PMDB Platform Timer Service before updating Content packs when you upgrade SHR to the latest version. If Content pack update fails, it will roll back to previous state.

Customizing out-of-the-box reports is not supported; such reports are overwritten by default reports after you upgrade Content Packs.

Creating reports by modifying a Content Pack's universe is also not supported and such reports will not work after you update the Content Pack.

Before You Begin

Before you begin installing Content Packs, make sure that:

- Post-installation configuration and data source selection are complete.
- Data collection configuration is complete.

Check Availability and Integrity of Data Sources

SHR enables you to check the availability and integrity of data sources prior to installing Content Packs.

1. Launch the following page:

`http://<SHR Server FQDN>:<port>/BSMRApp/dscheck.jsf`

2. To check the data sources related to RTSM, click **RTSM**.

Click **View** to see the results. Results include the list of missing mandatory CI types and attributes.

3. To check the data sources in the HP Operations Agent, click **PA**.

Click **View** to see the results. Results include a status summary of nodes and missing policies.

Selecting the Content Pack Components

A Content Pack is a data mart—a repository of data collected from various sources—that pertains to a particular domain, such as system performance or virtual environment performance, and meets the specific demands of a particular group of knowledge users in terms of analysis, content presentation, and ease of use. For example, the system performance content provides data related to the availability and performance of the systems in your IT infrastructure. Content Packs also include a relational data

model, which defines the type of data to be collected for a particular domain, and a set of reports for displaying the collected data.

Content Packs are structured into the following layers or components:

- **Domain 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 (Extract, Transform, and Load) 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 Operations Agent, you must install the `SysPerf_ETL_PerformanceAgent` component. If you want to collect system performance data from HP SiteScope, you must install either `SysPerf_ETL_SiS_API` (sourcing data logged in API) or `SysPerf_ETL_SiS_DB` (sourcing data logged in BSM Profile database).

A single data source application can have multiple ETL components. For example, you can have one ETL component for each virtualization technology supported in Performance 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 component:** The Report Content Pack component defines the application-specific aggregation rules, business views, SAP BOBJ universes, and the reports for a particular domain. Report components can be dependent on one or more Domain components. This component also provides the flexibility to extend the data model that is defined in one or more Domain components.

The list of Content Pack components that you can install depends on the topology source that you configured during the post-install configuration phase of the installation. Once the topology source is configured, the Deployment Manager filters the list of Content Pack components to display only those components that can be installed in the supported deployment scenario. For example, if RTSM is the configured topology source, the Deployment Manager only displays those components that can be installed in the SaOB and APM deployment scenarios.

For more information about each Content Pack and the reports provided by them, see the *HP Service Health Reporter Online Help for Users*.

Installing the Content Pack Components

Use the Deployment Manager utility to install the Content Pack components.

To install the Content Packs, follow these steps:

1. Launch the Administration Console in a web browser:
 - a. Launch the following URL:
`http://<SHR_Server_FQDN>:21411`

- b. Type **administrator** in the **Login Name** field and click **Log In** to continue. The **Home** page appears.

Note: If you use any other user account to access the Administration Console, make sure that the user account has administrator privileges.

- 2. On the left pane, click **Administration**, and then click **Deployment Manager**. The **Deployment Manager** page appears.

The Deployment Manager displays the Content Pack components that can be installed in the supported deployment scenario. You can modify the selection by clearing the selected content, the data source application, or the Content Pack components from the list. The following table lists the content that is specific to each deployment scenario:

List of Content Packs

Content	BSM/OMi	HP Operations Manager	Application Performance Management	VMware vCenter
Default	✓	✓	✓	✓
Cross-Domain Operations Events	✓			
Health and Key Performance Indicators	✓		✓	
IBM WebSphere Application Server	✓	✓		
Microsoft Active Directory	✓	✓		
Microsoft Exchange Server	✓	✓		
Microsoft SQL Server	✓	✓		
MSAppCore	✓	✓		
Network Performance ¹	✓	✓		
Operations Events	✓	✓		

¹You must use the NetworkPerf_ETL_PerfiSPI_NonRTSM ETL content in an RTSM deployment of SHR when Network Node Manager i (NNMi) is not integrated with BSM.

Content	BSM/OMi	HP Operations Manager	Application Performance Management	VMware vCenter
Oracle	✓	✓		
Oracle WebLogic Server	✓	✓		
Real User Transaction Monitoring	✓		✓	
Synthetic Transaction Monitoring	✓		✓	
System Performance	✓	✓		✓
Virtual Environment Performance	✓	✓		✓

3. Click **Install/Upgrade**.

The Deployment Manager starts installing the selected Content Pack components.

The Status column displays the progress of the installation. The **Deployment Manager** page automatically refreshes itself to display the updated status.

After the installation completes, *Installation Successful* is displayed in the **Status** column for each Content Pack component.

Note: If some work flow streams are running, the Deployment Manager displays the following message:

All the required services are stopped but a few jobs are still active.
 Please try after some time.

If you get this message, wait until all work flow streams are completed.

Chapter 6: Data Source Configuration

After installing Content Packs, you must configure SHR to collect required data from various data collectors. The 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.

You can configure the data source based on the following deployment scenarios:

1. **BSM/OMi 9.2x deployment scenario**
 - a. [Configuring the Management and Profile Database Data Source](#)
 - b. [Configuring the HP OMi Data Source \(Events database\)](#)
 - c. [Configuring the HP Operations Agent Data Source](#)
 - d. [Configuring the HP Operations Manager Data Source](#)
 - e. [Configuring the Network Data Source \(using Generic Database\)](#)
 - f. [Configuring the VMware vCenter Data Source](#)
 - g. [Configuring the SiteScope Data Source](#)
2. **OMi 10 deployment scenario**
 - a. [Configuring the HP OMi Data Source \(Operations database\)](#)
 - b. [Configuring the HP Operations Agent Data Source](#)
 - c. [Configuring the Network Data Source \(using Generic Database\)](#)
 - d. [Configuring the VMware vCenter Data Source](#)
 - e. [Configuring the SiteScope Data Source](#)
3. **HP Operations Manager deployment scenario**
 - a. [Configuring the Management and Profile Database Data Source](#)
 - b. [Configuring the HP Operations Agent Data Source](#)
 - c. [Configuring the HP Operations Manager Data Source](#)
 - d. [Configuring the Network Data Source \(using Generic Database\)](#)
 - e. [Configuring the VMware vCenter Data Source](#)
4. **VMware vCenter deployment scenario**
 - a. [Configuring the VMware vCenter Data Source](#)
5. **Other deployment scenarios**
 - a. [Configuring the Network Data Source \(using Generic Database\)](#)

For information on listings of ETLs for Content Pack, see [Appendix C](#).

Configuring the HP Operations Agent Data Source

In the RTSM deployment scenario, you do not have to create new HP Operations Agent data source connections. Because, by default, all the nodes on which HP Operations Agent is installed are automatically discovered when the topology information is collected. These data sources or nodes are listed in the HP Operations Agent Data Source page of the Administration Console.

To view the list of HP Operations Agent data sources, follow these steps:

1. In the **Administration Console**, click **Collection Configuration > HP Operations Agent**. The **HP Operations Agent Data Source** page appears.
2. To view detailed information about the HP Operations Agent data sources, click the Domain name or the number in the **HP Operations Agent Data Source Summary** table. The **HP Operations Agent Data Source Details** table appears.
3. To change the data collection schedule for one or more hosts, specify a polling time between 1 and 24 hours in the **Hrs** box in the **Schedule Polling Frequency** column.
4. Click **Save** to save the changes. A **Saved Successfully** message appears in the Information message panel.

For more information about configuring HP Operations Agent data source connections, see the *HP Service Health Reporter Online Help for Administrators*.

Configuring the HP Operations Manager Data Source

If you have installed the HP Operations Manager (HPOM) Content Pack and created the topology source connection for HPOM on the Service Definition page, the same data source connection appears on the HP Operations Manager page. You need not create a new data source connection. You can test the existing connection and save it.

However, updating the data source connection on the Service Definition page does not update the connection details on the Operations Manager page.

To configure the database connection, follow these steps:

1. In the **Administration Console**, click **Collection Configuration > HP Operations Manager**. The **HP Operations Manager** page appears.
2. Select the check box next to the host name and then click **Test Connection** to test the connection.
3. Click **Save** to save the changes. A **Saved Successfully** message appears in the Information message panel.

You can configure additional HPOM data sources by clicking the **Create New** button. You can modify a specific data source connection by clicking **Configure**.

4. To change the HPOM data collection schedule for one or more hosts, in the **Schedule Frequency** column, specify a collection time between 1 and 24 hours in the **Hrs** box.
5. Click **Save** to save the changes. A **Saved Successfully** message appears in the Information message panel.

Configuring the Network Data Source (using Generic Database)

If you have install the Network Content Pack, you must configure SHR (Local Data Collector) or Remote Collector to collect network-related data from NNMi. NNMi uses the NPS as the repository for network performance data. Using the Generic Database page in the Administration Console, you can configure SHR to collect the required data from the NPS. This page also allows you to configure connections to generic databases that use Sybase, Oracle, or SQL Server as the database system.

To configure the NPS data source connection, follow these steps:

1. In the **Administration Console**, click **Collection Configuration > Generic Database**. The **Generic Database** page appears.
2. Click **Create New** to create the NPS data source connection. The **Connection Parameters** dialog box appears.
3. Specify or type the following values in the **Connection Parameters** dialog box:

Field	Description
Host name	Address (IP or FQDN) of the NPS database server.
Port	Port number to query the NPS database server.
TimeZone	The time zone in which the database instance is configured.
Database type	The type of database engine that is used to create the NPS database.
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.
User name	Name of the NPS database user.
Password	Password of the NPS database user.
Collection Station	To specify whether it is a Local / Remote Collector.

Note: The Domain name Network_Core appears for selection only after the installation of NetworkPerf_ETL_PerfiSPI_RTSM or NetworkPerf_ETL_PerfSPI9.20 Content Pack or NetworkPerf_ETL_PerfiSPI_NonRTSM.

4. Click **OK**.
5. Click **Test Connection** to test the connection.
6. Click **Save** to save the changes. A Saved Successfully message appears in the Information message panel.
7. To change the data collection schedule for one or more hosts, in the **Schedule Frequency** column, specify a collection time between 1 and 24 hours in the **Hrs** box.

8. Click **Save** to save the changes. A *Saved Successfully* message appears in the Information message panel.

Data collection for all the newly created data source connections is enabled by default. For more information about configuring network data source connections, see the *HP Service Health Reporter Online Help for Administrators*.

Configuring the VMware vCenter Data Source

You can configure VMware vCenter as the data collection source to collect virtualization metrics in the HPOM deployment scenario.

To configure VMware vCenter, follow these steps:

1. In the **Administration Console**, click **Collection Configuration > VMware vCenter**. The **VMware vCenter Data Source** page appears.
2. Click **Create New** to test the connection. The **Connection Parameters** dialog box appears.
3. In the **Connection Parameters** dialog box, type the following values:

Field	Description
Host name	IP address or FQDN of the VMware vCenter application server.
User name	Name of the VMware vCenter application user.
Password	Password of the VMware vCenter application user.
Collection Station	To specify whether it is a Local / Remote Collector.

Note: You can configure additional VMware vCenter data sources using [step 2 on page 109](#) for each VMware vCenter connection that you wish to create.

4. To change the VMware vCenter data collection schedule for one or more hosts, in the **Schedule Frequency** column, specify a collection time between 5 and 60 minutes in the **Mins** box.
5. Click **Save** to save the changes. A *Saved Successfully* message appears in the Information message panel.
6. In the VMware vCenter server, grant the user the following permissions:
 - Set the datastore permission to **Browse Datastore**.
 - Set the datastore permission to **Low Level File Operations**.
 - Set the sessions permission to **Validate session**.
7. In the VMware vCenter server, set the Statistics Level:
 - a. In the vSphere Client, click **Administration > vCenter Server Settings**.
 - b. In the **vCenter Server Settings** window, click **Statistics**. The **Statistics Interval** page is displayed. This page displays the time interval after which the vCenter Server statistics will be saved, the time duration for which the statistics will be saved and the statistics level.
 - c. Click **Edit**.

- d. In the **Edit Statistics Interval** window, set the Statistics Interval from the drop-down list. For the statistics level that you select, the **Edit Statistics Interval** window appears. This displays the type of statistics which will be collected for that level. You must set the minimum statistic level as 2.

Configuring the SiteScope Data Source

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. If Profile database is selected as the channel for metrics in Configuration Wizard, you must create a collector for the SiteScope data source.

If you have enabled SSL for SiteScope, perform the steps mentioned in ["SiteScope with SSL enabled" on page 77](#).

To create a new SiteScope data source connection, follow these steps:

1. In the **Administration Console**, click **Collection Configuration > SiteScope**. The **SiteScope** page appears.
2. Click **Create New**. The **Connection Parameters** dialog box appears.
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. Note: The port number 8080 is the default port to connect to SiteScope server.
Use SSL	<i>(Optional)</i> . If selected, you must enable the SiteScope server to support communication over Secure Sockets Layer (SSL). If you have enabled SSL for SiteScope, perform the steps mentioned in "SiteScope with SSL enabled" on page 77 .
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. Note: To obtain the Init String, log in to SiteScope server with your credentials and click on General Preferences > LW SSO .
Collection Station	This option is use for a collector installed on a remote system.
General Data Integration Settings:	

Field	Description
	<p>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.</p> <p>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.</p>
Integration name	<p>Enter the name of the integration.</p> <p>Note: You cannot change it later.</p>
Encoding	<p>The encoding type for communication between SHR and SiteScope.</p>
Use SSL	<p><i>(Optional).</i> If selected, you must enable the SiteScope server to support communication over Secure Sockets Layer (SSL).</p> <p>If you have enabled SSL for SiteScope, perform the steps mentioned in "SiteScope with SSL enabled" on the next page.</p> <p>For SHR to obtain the data from SiteScope in HTTPs mode, perform the steps "Configuring SHR server to get data from SiteScope in HTTPs mode" on the next page, after completing the SiteScope data source configuration.</p>
Reporting interval (seconds)	<p>Frequency at which SiteScope pushes data to SHR. This is a configurable parameter.</p>
Request timeout (seconds)	<p>The time to wait before the connection times out. Value of zero (0) gives you infinite timeout period. This is a configurable parameter.</p>
Connection timeout (seconds)	<p>Timeout until connection is reestablished. Value of zero (0) means timeout is not used. This is a configurable parameter.</p>
Number of retries	<p>Number of retries that SiteScope server attempts during connection error with SHR.</p>
Authentication when requested	<p><i>(Optional).</i> If selected, authentication is performed using the Web server user name and password.</p>
Authentication user name	<p>If SHR is configured to use basic authentication, specify the user name to access the server.</p>
Authentication password	<p>If SHR is configured to use basic authentication, specify the password to access the server.</p>
Proxy address	<p>If proxy is enabled on SiteScope, enter the proxy address.</p>
Proxy user name	<p>Enter user name of the proxy server.</p>
Proxy password	<p>Enter password of the proxy server.</p>
Create tag	<p>Select it to create a tag for the SiteScope monitors that you must manually apply from the SiteScope server.</p>

Field	Description
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.

SiteScope with SSL enabled

If you have enabled SSL for SiteScope, perform these steps:

1. Copy the certificate from Sitescope server to SHR server `{PMDB_HOME}/config` folder.
2. Rename the certificate extension with `.pem`.
3. Run the command `keytool -v -list -keystore <certificate name.pem>` to verify the certificate.

Note: The password is changeit.

4. The certificate should display the parameter `Owner: CN=<Sitescope Server name>`.
5. Perform the steps "[Configuring the SiteScope Data Source](#)" on page 75.
6. Go to the location `{PMDB_HOME}/stores` and verify if `cacert.jks` file is created.

Configuring SHR server to get data from SiteScope in HTTPs mode

Perform these steps to configure the SHR server to get the data from SiteScope server in HTTPs mode after "[Configuring the SiteScope Data Source](#)" on page 75:

1. From the location `{PMDB_HOME}/config`, open the file `collection.properties`.
2. Edit the following parameter values from `false` to `true`:
`sis.gdi.http.server.use.ssl=true`
`sis.https.server.enable=true`
Also, change the following parameter from `true` to `false`:
`sis.http.server.enable=false`
3. On the SHR Collector system, run the following command to export the Collector CA certificate from keystore:
`ovcert -exporttrusted -file <filename> -ovrg server`
4. Copy the exported CA certificate to the SiteScope server.
5. On the SiteScope server, log on to the SiteScope user interface, click **Preferences > Certificate Management** and click **Import Certificates** button. Select **File** or **Host**, and enter the details of the source server.
From the Loaded Certificates table, select the server certificates to import and click **Import**. The imported certificates are listed on the Certificate Management page.
6. On the SHR server, restart the **HPE_PMDB_Platform_Collection** service.

Configuring the Management and Profile Database Data Source

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 HPOM, OMi, BPM, RUM, and Service Health.

In your HP BSM deployment, you might have to set up multiple Profile databases for scaling because one database might not be enough to store all the data. You may also require multiple Profile database to store critical and non-critical data. The information on different Profile databases deployed in your environment is stored in the Management database.

To configure the multiple Profile database connections, you also need to configure the Management database on the BSM/OMi page.

Configure New Management Database

To configure a new Management Database, follow these steps:

1. In the **Administration Console**, click **Collection Configuration > BSM/OMi > Management Database**.
2. Click **Create New**. The **Connection Parameters** dialog box appears.
3. Based on the topology source, select **Data Source** as **BSM** or **OMi**.
4. Type the following values in the **Connection Parameters** dialog box:

Field	Description
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. If you have selected the Data Source as BSM then the database type can either be Oracle or MSSQL . If you have selected the Data Source as OMi then the database type can 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.

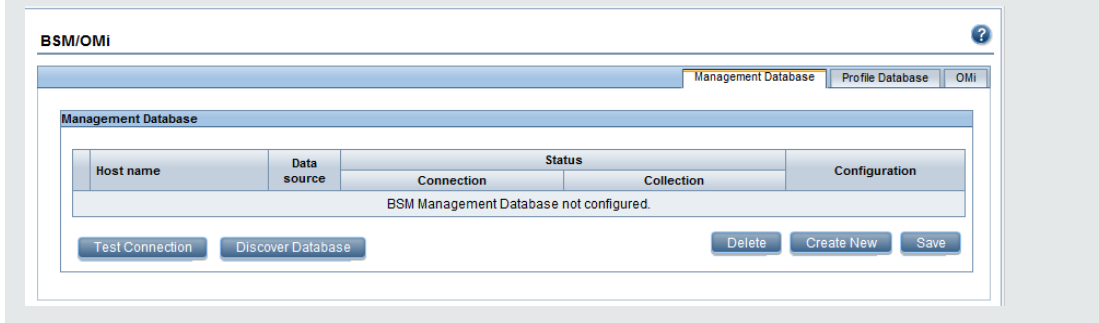
Field	Description
Database instance	System Identifier (SID) of the Management Database instance. Not displayed when Database in Oracle RAC is selected. Note: For information about the database host name, port number, and SID, contact your HP Business Service Management administrator.
Database name	Name 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 (available at \${PMDB.HOME}/config folder) 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.

5. Click **OK**.
6. Click **Test Connection** to test the connection.
7. 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.



8. Click **Save** to save the changes. A **Saved Successfully** message appears in the Information message pane.

Configure New Profile Database

To configure a new Profile database, follow these steps:

1. In the **Administration Console**, click **Collection Configuration > BSM/OMi > Profile Database**.
2. Click **Create New**. The **Connection Parameters** dialog box appears.
3. Type the following values in the **Connection Parameters** dialog box:

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, or MSSQL.
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. <div style="background-color: #f0f0f0; padding: 5px;"> <p>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.</p> <ul style="list-style-type: none"> • RUM • BPM • ServiceHealth </div>

Field	Description
	<ul style="list-style-type: none"> • SM • SM_VMware_SiS
Database instance	<p>System Identifier (SID) of the Profile Database instance. Not displayed when Database in Oracle RAC is selected.</p> <p>Note: For information about the database host name, port number, and SID, contact your HP Business Service Management administrator.</p>
Windows Authentication	<p>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.</p>
Database name	<p>Name of the database. This field appears only if MSSQL is selected as the database type.</p>
Database in Oracle RAC	<p>This option appears only if you have selected Oracle as the database type.</p>
Service name	<p>Name of the service. This option appears only if Database in Oracle RAC is selected.</p>
ORA file name	<p>The ORA file that contains connection information to the Oracle Real Application Cluster. This option appears only if Database in Oracle RAC is selected.</p>
User name	<p>Name of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.</p> <p>Note: If the Windows Authentication option is selected, this field is disabled.</p>
Password	<p>Password of the Profile Database user, which was specified in the BSM Configuration Wizard when setting up the Profile Database.</p> <p>Note: If the Windows Authentication option is selected, this field is disabled.</p>
Collection Station	<p>This option is used for a collector installed on a remote system.</p>

4. Click **OK**.
5. Click **Test Connection** to test the connection.
6. Click **Save** to save the changes made on this page. A *Saved Successfully* message appears in the Information message pane.

After you save the newly created Management database connection, SHR (local collector or remote collector) retrieves the Profile database information from the Management database data source and lists all the existing Profile database data sources under the Profile Database section of the page.

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

In case of a Remote Collector, the collection station has to be selected from the Database type drop down box provided in the Profile Database section of the page.

For more information about configuring Profile database data source connections, see the *HP Service Health Reporter Online Help for Administrators*.

Enable KPI Data Collection for Service Health CIs

KPIs are high-level indicators of a CI's performance and availability. The KPI data pertaining to certain logical Service Health CIs, such as Business Service, Business Application, Business Process, and Host, are logged by default in the Profile database. SHR collects this data from the database for reporting.

However, the KPI data for other CI types are not automatically logged in the Profile database. To enable the logging of the KPI data for these CI types, you must configure the CIs in the HP BSM. For more information, see the *Persistent Data and Historical Data* section of the *HP Business Service Management - Using Service Health* guide. This guide is available for the product, *Application Performance Management (BAC)*, at the following URL:

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

Configuring the HP OMi Data Source

If you install the HP OMi Content Pack, you must configure the HP OMi database connection for data collection. You can configure SHR to collect data from the following OMi data repositories:

- **Events database:** The events database stores data obtained from OMi (9.x versions) data source.
- **Operations database:** The operations database stores data obtained from OMi10 (and later versions) data source.

Before you create a new HP OMi data source connection, make sure that a data source connection for the Management database exists on the Management DB / Profile DB page. This data connection is required to retrieve Assigned User/Group information for HP OMi, which is stored in 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 BSM RTSM that was configured as the topology source.

To configure the HP OMi data source connections, follow these steps:

1. In the **Administration Console**, click **Collection Configuration > BSM/OMi > OMi**.
2. Click **Create New** to create a new HP OMi data source connection. The **Connection Parameters** dialog box appears.
3. Specify or type the following values in the **Connection Parameters** dialog box:

Field	Description
Data Source	Event or Operations <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;"> Note: Select Event for OMi 9.x version and Operations for OMi 10.x and later versions. </div>
Host name	Address (IP 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. If MSSQL Server is configured to use default (unnamed) database instance, leave this field empty. 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. If you have selected the Data Source as Event then the database type can either be Oracle or MSSQL . If you have selected the Data Source as Operations then the database type can be Oracle , MSSQL , or PostgreSQL .
Windows Authentication	If you 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. If the Windows Authentication option is selected, this field is disabled and appears empty.
Password	Password of the HP OMi database user. If the Windows Authentication option is selected, this field is disabled and appears empty.
Collection Station	To specify whether it is a Local / Remote Collector

4. Click **OK**.

Note: You can create only one HP OMi data source connection. After the connection is created, the **Create New** button is disabled by default. Make sure that you type in the correct values.

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

6. Click **Save** to save the changes. A *Saved Successfully* message appears in the Information message panel.

7. To change the HP OMi data collection schedule for one or more hosts, in the **Schedule Frequency** column, specify a collection time between 1 and 24 hours in the **Hrs** box.

8. Click **Save** to save the changes. A **Saved Successfully** message appears in the **Information** message panel.

Part II: Licensing

This section provides information about licensing SHR. It lists the licenses to use for SHR. It provides procedure to obtain a permanent license key and install it. It also provides procedure to reactivate license for SAP Business Objects.

Chapter 7: Licensing SHR

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 a base license and an additional node license as follows:

- **HP Service Health Reporter Software (Base License)**

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 50 nodes.

- **Additional Scalability Packs of 50 Nodes (Node License)**

A node is a real or virtual computer system, or a device (for example a printer, router, or bridge) on a network or an entity defined in custom content (for example software instance, port). 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.

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.

Note: If you have obtained the node license, you must also obtain and install the base license with it.

Licenses to Use (LTUs)

Table 1 presents all the LTUs available for SHR.

Table 1: Licenses to Use

LTU	Stock-keeping Unit (SKU)	Description
HP Service Health Reporter Standard Edition 50 Service Health Nodes SW E-LTU	TD905AAE	This LTU includes the following Content Packs: <ul style="list-style-type: none">• Systems/Virtualization Management Content Pack• SPI Content Packs• Event Content Packs (OM, OMi) The BSM EUM and Network Content Packs are not available

Table 1: Licenses to Use, continued

LTU	Stock-keeping Unit (SKU)	Description
		with this LTU.
HP Service Health Reporter Advanced 50 Service Health Nodes SW E-LTU	TJ756AAE	This LTU entitles the user to use all out-of-the-box Content Packs available with SHR.
HP Service Health Reporter Upgrade from Standard to Advanced 50 Service Health Nodes SW E-LTU	TD906AAE	This Upgrade LTU entitles the user to upgrade from the Standard Edition to the Advanced Edition of SHR.
HP Service Health Reporter add 50 Nodes for Standard or Advanced Service Health Nodes SW E-LTU	TJ757AAE	This is an add-on pack to add entitlement for 50 additional nodes for SHR.
Performance Insight to Service Health Reporter Advanced Core for Migration Software E-LTU	TJ773AAE	This is a migration pack for Performance Insight users to migrate to the HP Service Health Reporter Advanced Core LTU (50 Nodes).
Performance Insight to Service Health Reporter Advanced Migration 250 Service Health Software E-LTU	TJ774AAE	This is a migration pack for Performance Insight users to migrate to the HP Service Health Reporter Advanced 250 Nodes LTU.
Performance Insight to Service Health Reporter Advanced Migration 1000 Service Health Software E-LTU	TJ775AAE	This is a migration pack for Performance Insight users to migrate to the HP Service Health Reporter Advanced 1000 Nodes LTU.
Performance Insight to Service Health Reporter Advanced Migration 5000 Service Health Software E-LTU	TJ776AAE	This is a migration pack for Performance Insight users to migrate to the HP Service Health Reporter Advanced 5000 Nodes LTU.
Performance Insight to Service Health Reporter Advanced Migration Unlimited Service Health Software E-LTU	TJ777AAE	This is a migration pack for Performance Insight users to migrate to the HP Service Health Reporter Advanced Core LTU (Unlimited Nodes).

Note: A node is a real or virtual computer system, or a device (for example a printer, router, or bridge) on a network or an entity defined in custom content (for example software instance, port).

For information on custom content license, see *HP Service Health Reporter Content Development Guide*.

Obtaining a Permanent License Key

To obtain a permanent license key, follow these steps:

1. Open the SHR Administration Console by launching the following URL:
`http://<server name>:21411`
In this instance, *<server name>* is the fully qualified domain name of the system where SHR was installed.
2. Click **Administration > Licensing**. The HP License Key Delivery Service page opens.
3. Click **Launch HP Password Center**.
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 then type in 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.

Note: If you are setting up SHR in a high availability cluster environment, you must provide the logical IP address of the SHR host system. For more information on the high-availability setup, see the *HP Service Health Reporter High Availability Guide*.

9. Type in 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.

Installing the Permanent License Key

To install the permanent license, follow these steps:

On Windows:

1. Log on to the SHR system as administrator.
2. Click **Start > Programs > HP Software > Service Health Reporter > License Manager**. The **Retrieve/Install License Key** window appears.
3. Click **Install/Restore License Key from file**. The **Install/Restore License Key from file** page appears.
4. Browse to the location of the saved license certificate, click **View file content**, select **PERM**, and then click **Install**.

On Linux:

1. Log on to the SHR system as root.

Note: While using an X client application to remotely connect to the Linux system, do not use the BROADCAST mode and make sure that the DISPLAY environment variable on the Linux system is correctly configured.

2. The name of the license file (that you saved in "[Review the license certificate information, save the license to your system, and then close the License certificate page.](#)" on the previous page) starts with a . (dot) character. You must rename this file by removing the(.) (dot) character.
3. Run the following command:

```
$PMDB_HOME/bin/LicenseManager.sh
```

The **Retrieve/Install License Key** window appears.
4. Click **Install/Restore License Key from file**. The **Install/Restore License Key from file** page appears.
5. Browse to the location of the saved license certificate, click **View file content**, select **PERM**, and then click **Install**.

SAP BusinessObjects License Reactivation


The SAP BusinessObjects license depends on the validity of the SHR license. If the SHR license expires, the SAP BusinessObjects license is automatically deactivated and all the SAP BusinessObjects servers are disabled. After you renew the SHR license and access the Administration Console, SHR automatically reactivates the SAP BusinessObjects license. However, the SAP BusinessObjects servers remain in the disabled state. To ensure that SAP BusinessObjects works, you must manually enable the servers by performing the following steps:

On Windows:

1. Log on to the SHR system as administrator.
2. Click **Start > Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Configuration Manager**. The **Central Configuration Manager** window appears.

3. In the **Display Name** column, select **Server Intelligence Agent (HOMLO1GEATON)**.
4. On the main tool bar, click the **Manage Servers** icon. The **Log On** dialog box appears.
5. In the **System** list, select the system on which SAP BusinessObjects is installed.
6. In the **User name** and **Password** field, type the user credentials of the SAP BusinessObjects server. The default user name is **Administrator** and the Password field should be left blank.
7. Click **Connect**. The **Manage Servers** window appears.
8. Click the **Refresh** icon to refresh the server list.
9. Click **Select All** to select all the listed servers, and then click the **Enable** icon to restart the servers.
10. Click **Close** to close the window.
11. Close all open windows.

On Linux:

1. Log on to the **Central Management Console** by launching the following URL:
`http://<SHR_System_FQDN>:8080/CmcApp`
where, *<SHR_System_FQDN>* is the fully qualified domain name of the SHR system.
2. Log on as Administrator.
3. Click  **Servers**.
4. Hold down the **Shift** or **Ctrl** key and click on serve to select multiple servers.
5. Right-click on the selected group of servers and then click **Enable Server**.

Note: There are two pages of server listings. Proceed to the second page to enable all the servers.

Note: If the SAP BusinessObjects servers are still not enabled, restart the HP_PMDB_Platform_IM service.

Part III: Migrating to Windows 2012 Environment

The Sybase IQ database bundled with the SHR media is not supported on Windows 2012 environment. You can install Sybase IQ on Windows 2008 or on Linux operating system.

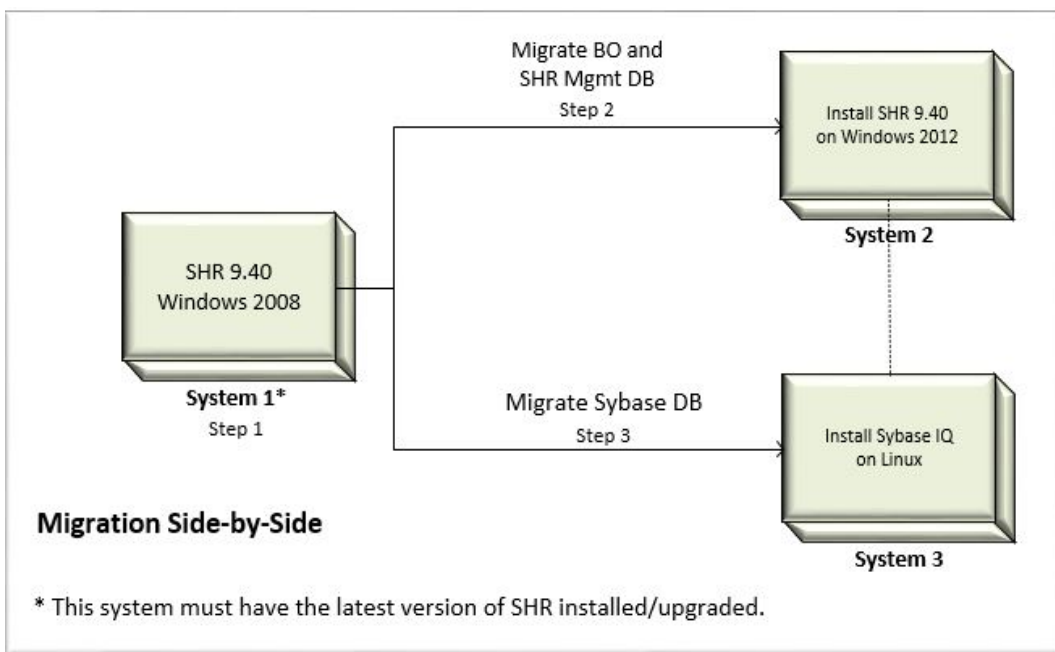
This section provides the steps to migrate SHR 9.40 installed/upgraded on Windows 2008 to Windows 2012 environment with Sybase IQ database separately on a Linux system.

Note: Ensure that you have upgraded to the latest version of SHR before migrating to windows 2012 environment.

Chapter 8: Migration Scenarios

Method 1: Side-by-Side

This section guides you to migrate from a typical Windows 2008 setup to a new custom setup. The new setup consists of SHR on Windows 2012 operating system and Sybase IQ on Linux system.



Note: Ensure that you have upgraded to the latest version of SHR before migrating to windows 2012 environment.

To proceed with the migration of SHR, complete the following tasks:

Step 1:

1. Take the backup of complete SHR setup. For more information, see [Database Backup and Recovery](#) for steps.
2. Ensure that the PostgreSQL service is running. Run the following command and take the back up of the Management database:

On Windows: %PMDB_HOME%/../JRE64/bin/java -cp %PMDB_HOME%/lib/utills.jar com.hp.bto.bsmr.common.util.PostgresUpgrade PRE_DB_UPGRADE postgres 21425 <Backup location> dwabc %PMDB_HOME%

Caution: You can perform any one of the following for the License:

- Take a complete backup of System 1. Remove it from the network and use the same IP address and hostname in System 2 and restore the data. OR
- Use **Rehost** option to obtain the license for the IP address of System 2 from the License Management Portal. Contact HP Support for more information.

Step 2:

1. On System 2, install the latest version of SHR and SAP BusinessObjects (bundled with the SHR9.40 media). Ensure that you have the same directory structure similar to the System 1.

For more information, see *HP Service Health Reporter Interactive Installation Guide*.

Caution: The SHR components in all of the systems must have a static IP address.

2. Perform all the post-installation configuration steps on System 2. See *Primary Configuration* chapter in this guide for the steps. Do not perform the tasks “Selecting the Data Source” and “Configuring the Topology Source” at this moment.

Install the content packs on System 2. Ensure that you install the same content packs as in System 1.

Validate the installation on the system. Ensure that the services are running. For more information, see *HP Service Health Reporter Interactive Installation Guide*.

3. Restore the backup of Management database on System 2 as follows:
 - a. Stop all SHR services. Wait for all SHR processes to finish.
 - b. Run the following command to verify if all of the required services and processes are stopped:
`%PMDB_HOME%\DR\SHRServiceCheck.bat`
 - c. Start PostgreSQL service.
 - d. Run the below command to restore Management database:
 - **On Windows:** `%PMDB_HOME%\..\JRE64\bin/java -cp %PMDB_HOME%\lib\log4j-1.2.15.jar;%PMDB_HOME%\lib\utils.jar com.hp.bto.bsmr.common.util.PostgresUpgrade POST_DB_UPGRADE postgres 21425 <Backup location> dwabc %PMDB_HOME%`
 - e. Restore the following configuration files:
 - `%PMDB_HOME%\config\collection.properties`
 - `%PMDB_HOME%\data\downtime\downtime.xml` if it exists
 - `%PMDB_HOME%\config\<name>customgroup.xml`, if it exists
4. Restore the backup of the SAP BusinessObjects server on System 2. See [Database Backup and Recovery](#).

Note: Use Hostname (short name) of the SHR system 1 as BO repository User ID.

- Restore the following configuration files:
 - `%PMDB_HOME%\BOWebServer\conf\server.xml`
 - `%PMDB_HOME%\BOWebServer\webapps\InfoViewApp\WEB-INF\web.xml`
 - `%PMDB_HOME%\BOWebServer\webapps\CmcApp\WEB-INF\web.xml`

Note: Update the host name of system 1 to system 2 in the following files after restore and restart the BusinessObjects service: Business Objects Webserver.

%PMDB_HOME%/BOWebServer/webapps/InfoViewApp/WEB-INF/web.xml

%PMDB_HOME%/BOWebServer/webapps/CmcApp/WEB-INF/web.xml

Step 3:

1. On System 3, which runs on Linux operating system, install Sybase IQ (bundled with the SHR9.40 media). For more information, see *HP Service Health Reporter Interactive Installation Guide*.
Validate the installation on the system. Ensure that the services are running. For more information, see *HP Service Health Reporter Interactive Installation Guide*.
2. Restore the backup of Sybase IQ to the System 3 as follows:
 - a. Copy the backup of Sybase IQ files to the System 3.
 - b. Copy the pmdbConfig file from System 1 to System 3:
copy %PMDB_HOME%\config\pmdbConfig.cfg file from System 1 to \$PMDB_HOME/config folder on System 3.
 - c. Run the following command:
dos2unix \$PMDB_HOME/config/pmdbConfig.cfg
 - d. Change the server name in \$PMDB_HOME/config/pmdbConfig.cfg with the remote IQ system short name.
 - e. Stop the Sybase IQ service in System 3. Perform the following steps:
 - cd /etc/init.d
 - service HP_PMDB_Platform_Sybase stop
 - f. Verify if the Sybase IQ service is stopped. Perform the following steps:
 - Run the following command:
ps -ef|grep -i iqsrv
 - If the iq service is still running, note the process ID displayed by the command output.
 - Run the command by entering the process ID in <pid>: kill -9 <pid>
 - g. Move all the files in the Sybase database folder to a new location in the system. These files will be recreated by the restore process.
 - h. Start Sybase IQ server in System 3 by running the following command:
start_iq @/opt/HP/BSM/PMDB/config/pmdbConfig.cfg
 - i. Connect from System 1 to remote Sybase IQ server on System 3 with the default utility_db password as follows:
 - i. On the SHR system, click **Start > Run**. The Run dialog box appears.
 - ii. Type dbisql and press ENTER. The Connect dialog box on Interactive SQL program appears.
 - iii. Type the following:
 - A. In the User ID field, type **dba**.
 - B. In the Password field, type **sql**.

- C. In Action select **Connect to a running database on another computer** from the drop down.
- D. In Host, type the hostname of the System 3.
- E. In Port, type 21424.
- F. In the Server Name field, type the name of the server where the SHR Sybase IQ database is installed.

Tip: The server name can be found in `pmdbConfig.cfg` file. Open the file. The server name is the text succeeding `-n`.

- G. In the Database name field, type **utility_db**.

iv. Click Connect. The Interactive SQL window opens.

- j. Restore the database as follows:

On the SQL Statements box type the following sql statement without gap between the statements:

Note: The following statements are single query. Execute all of them at once.

```
restore DATABASE '<Location of Sybase DB files on System 3/pmdb.db
>' from '<Filename with absolute path of Sybase IQ backup folder on System
3/Full.<day of the backup taken> >'
RENAME IQ_SYSTEM_MAIN TO '<Location of Sybase DB folder on System 3>\pmdb.iq'
RENAME IQ_SYSTEM_TEMP TO '<Location of Sybase DB folder on System
3>\pmdb.iqtmp'
RENAME IQ_SYSTEM_MSG TO '<Location of Sybase DB folder on System
3>\pmdb.iqmsg'
RENAME pmdb_user_main TO '<Location of Sybase DB folder on System 3>\pmdb_
user_main.iq'
```

For example:

```
restore DATABASE '/sybase_db/pmdb.db' from '/sybase_bkp/Full.monday'
RENAME IQ_SYSTEM_MAIN TO '/sybase_db/pmdb.iq'
RENAME IQ_SYSTEM_TEMP TO '/sybase_db/pmdb.iqtmp'
RENAME IQ_SYSTEM_MSG TO '/sybase_db/pmdb.iqmsg'
RENAME pmdb_user_main TO '/sybase_db/pmdb_user_main.iq'
```

- k. Stop and start the Sybase service:

```
service HP_PMDB_Platform_Sybase stop
service HP_PMDB_Platform_Sybase start
```

- l. Run the following commands using `dbisql` as `pmdb_admin` user:

```
DELETE FROM IM_PM_OS_INFO_FILLDETAIL WHERE OS_INFO_ID IN (SELECT IM_PM_OS_
INFO_ID FROM IM_PM_OS_INFO WHERE upper (HOSTNAME) = UPPER('<short host name
of System 1>'))
DELETE FROM IM_PM_OS_INFO WHERE upper (HOSTNAME) = UPPER('<short host name of
System 1>')
```

```
DELETE FROM IM_PM_APPS_INFO WHERE upper(HOSTNAME) = UPPER('<short host name  
of System 1>')
```

Post-Migration Configurations

Ensure that all the services are up and running in all systems.

Perform the following in System 2 after migration:

1. To cover the data gaps, edit the config.prp file with the collection initial history values.

```
dbcollector.initHistory = <system downtime for migration in hours>
```

```
collector.initHistory = <system downtime for migration in hours>
```

Note: To ensure that you cover the data gap include additional hours while you enter the value *system downtime for migration in hours*.

For Example:

```
dbcollector.initHistory = 48
```

```
collector.initHistory = 48
```

2. Execute the following query using pgAdmin:

```
Truncate dwabc.PA_LAST_POLL;
```

```
Truncate dwabc.DB_LAST_POLL;
```

3. Perform the following steps to synchronize the collection data sources:

- a. Execute the following query using pgAdmin:

```
UPDATE dwabc.remote_poller SET datasource_status=0
```

- b. Sync collection data sources using **Administrator Console** (Under **Administrator > Collector Configuration** page).

4. Restart the HP_PMDB_Platform_Collection service in System 2.

Verify that SHR is Running Successfully

Launch the following URL and verify that you are able to log on to the Administration Console as administrator:

```
http://<SHR_Server_FQDN>:21411
```

Launch the following URL and verify that you are able to log on to the InfoView Console as administrator:

```
http://<SHR_Server_FQDN>:8080
```

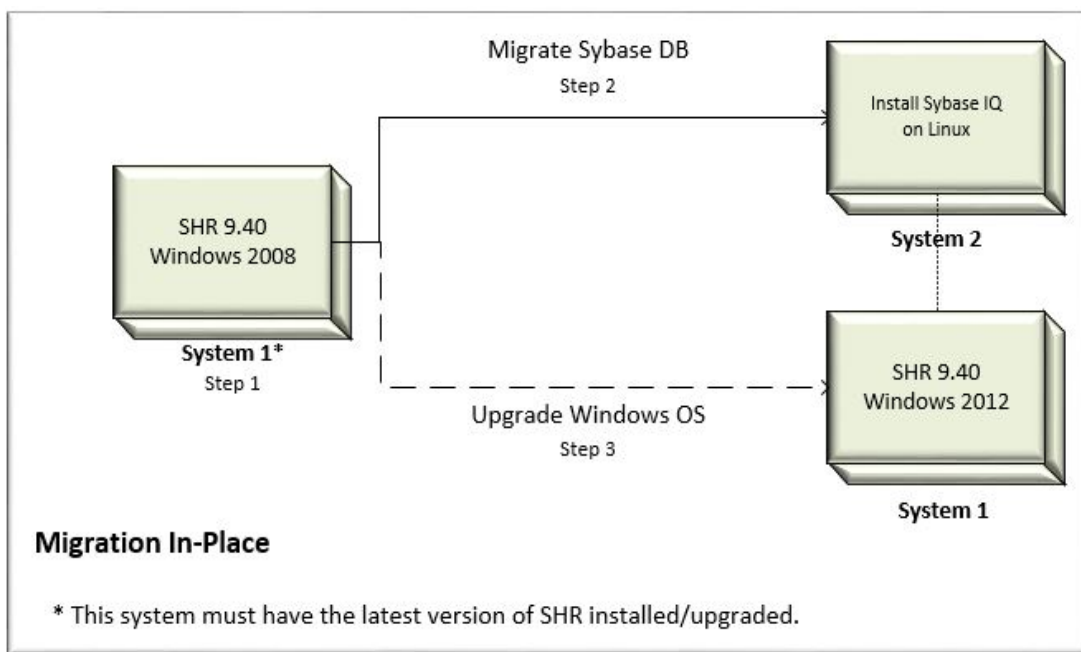
Note: You have to recreate administrator and collection services

If you have installed SHR in a domain, reconfigure the following services. For more information, see "*Configuring SHR Services when SHR is Installed on a Domain*" section of the *HP Service Health Reporter Configuration Guide*.

- HP PMDB Platform Administrator Service
- HP PMDB Platform Collection Service

Method 2: In-Place

This section guides you to migrate from a typical Windows 2008 setup to a custom setup. The custom setup consists of Sybase IQ on Linux system and SHR on Windows 2012 operating system (the existing system with the operating system upgraded).



Note: Ensure that you have upgraded to the latest version of SHR before migrating to windows 2012 environment.

To proceed with the migration of SHR, complete the following tasks:

Step 1:

1. Take the Sybase IQ back up from the SHR server. For more information, see [Database Backup and Recovery](#).

Step 2:

1. On System 2, which runs on Linux operating system, install Sybase IQ (bundled with the SHR 9.40 media). For more information, see *HP Service Health Reporter Interactive Installation Guide*.
Validate the installation on the system. Ensure that the services are running. For more information, see *HP Service Health Reporter Interactive Installation Guide*.
2. Restore the backup of Sybase IQ to the System 2 as follows:
 - a. Copy the backup of Sybase IQ files to the System 2.
 - b. Copy the `pmdbConfig` file from System 1 to System 2:
`copy %PMDB_HOME%\config\pmdbConfig.cfg` file from System 1 to `$PMDB_HOME/config` folder in System 2.
 - c. Run the following command:

```
dos2unix $PMDB_HOME/config/pmdbConfig.cfg
```

- d. Change the server name in `$PMDB_HOME/config/pmdbConfig.cfg` with the remote IQ system (System 2) short name.
- e. Stop the Sybase IQ server in System 2. Perform the following steps:
 - `cd /etc/init.d`
 - `service HP_PMDB_Platform_Sybase stop`
- f. Verify if the Sybase IQ service is stopped. Perform the following steps:
 - Run the following command:

```
ps -ef|grep -i iqsrv
```
 - If the iq service is still running, note the process ID displayed by the command output.
 - Run the command by entering the process ID in `<pid>`: `kill -9 <pid>`
- g. Move all the files in the Sybase database folder to a new location in the system. These files will be recreated by the restore process.
- h. Start Sybase IQ server in System 2 by running the following command:

```
start_iq @/opt/HP/BSM/PMDB/config/pmdbConfig.cfg
```
- i. Connect from System 1 to remote Sybase IQ server on System 2 with the default `utility_db` password as follows:
 - i. On the SHR system, click **Start > Run**. The Run dialog box appears.
 - ii. Type `dbisql` and press ENTER. The Connect dialog box on Interactive SQL program appears.
 - iii. Type the following:
 - A. In the User ID field, type **dba**.
 - B. In the Password field, type **sql**.
 - C. In Action select **Connect to a running database on another computer** from the drop down.
 - D. In Host, type the hostname of the System 2.
 - E. In Port, type 21424.
 - F. In the Server Name field, type the name of the server where the SHR Sybase IQ database is installed.

Tip: The server name can be found in `pmdbConfig.cfg` file. Open the file. The server name is the text succeeding `-n`.

- G. In the Database name field, type **utility_db**.
 - iv. Click Connect. The Interactive SQL window opens.
- j. Restore the database as follows:

On the SQL Statements box type the following sql statement without gap between the statements:

Note: The following statements are single query. Execute all of them at once.

```
restore DATABASE '<Location of Sybase DB files on System 2/pmdb.db
>'from'<Filename with absolute path of Sybase IQ backup folder on System
2/Full.<day of the backup taken> >'
RENAME IQ_SYSTEM_MAIN TO'<Location of Sybase DB folder on System 2>\pmdb.iq'
RENAME IQ_SYSTEM_TEMP TO'<Location of Sybase DB folder on System
2>\pmdb.iqtmp'
RENAME IQ_SYSTEM_MSG TO'<Location of Sybase DB folder on System
2>\pmdb.iqmsg'
RENAME pmdb_user_main TO'<Location of Sybase DB folder on System 2>\pmdb_
user_main.iq'
```

For example:

```
restore DATABASE '/sybase_db/pmdb.db'from' /sybase_bkp/Full.monday'
RENAME IQ_SYSTEM_MAIN TO' /sybase_db/pmdb.iq'
RENAME IQ_SYSTEM_TEMP TO' /sybase_db/pmdb.iqtmp'
RENAME IQ_SYSTEM_MSG TO' /sybase_db/pmdb.iqmsg'
RENAME pmdb_user_main TO' /sybase_db/pmdb_user_main.iq'
```

3. To update the config.prp, stop all the SHR service in System 1.

From the %PMDB_HOME%\bin\scripts folder, run the following script to recreate DSN:

```
perl updateSHRConfig.pl -h <hostname> -s <IQServerName> -d <databasepassword> -f
<Databasefolderpath>
```

4. Copy the config.prp from System 1 to data folder in System 2.
5. Start Sybase IQ service in System 2.
6. Start SHR services in System 1.
7. Ensure end to end data is getting collected, Sybase IQ database is loaded with appropriate data and the report displays the required details.

Step 3:

1. On System 1, stop all SHR services using the following steps:
 - a. Log on to the SHR system.
 - b. Open the Services window.
 - c. Stop the following services:
 - HP_PMDB_Platform_Administrator
 - HP_PMDB_Platform_Collection
 - HP_PMDB_Platform_DB_Logger
 - HP_PMDB_Platform_Timer
 - HP_PMDB_Platform_IM
 - HP_PMDB_Platform_Message_Broker
 - HP_PMDB_Platform_PostgreSQL
 - HP_PMDB_Platform_Sybase

- Sybase IQ Agent 15.4 Service
 - Business Objects Webserver Service
2. Open Windows Task Manager, go to the Processes tab:
 - If the abcloadNrun processes are running, wait until they complete.
 3. Upgrade Windows 2008 OS in System 1 to Windows 2012.
 4. Start the SHR services in System 1.

Post-Migration Configurations

Perform the following task after migration:

Task: Verify that SHR is Running Successfully

Launch the following URL and verify that you are able to log on to the Administration Console as administrator:

http://<SHR_Server_FQDN>:21411

Launch the following URL and verify that you are able to log on to the InfoView Console as administrator:

http://<SHR_Server_FQDN>:8080

Note: You have to recreate administrator and collection services

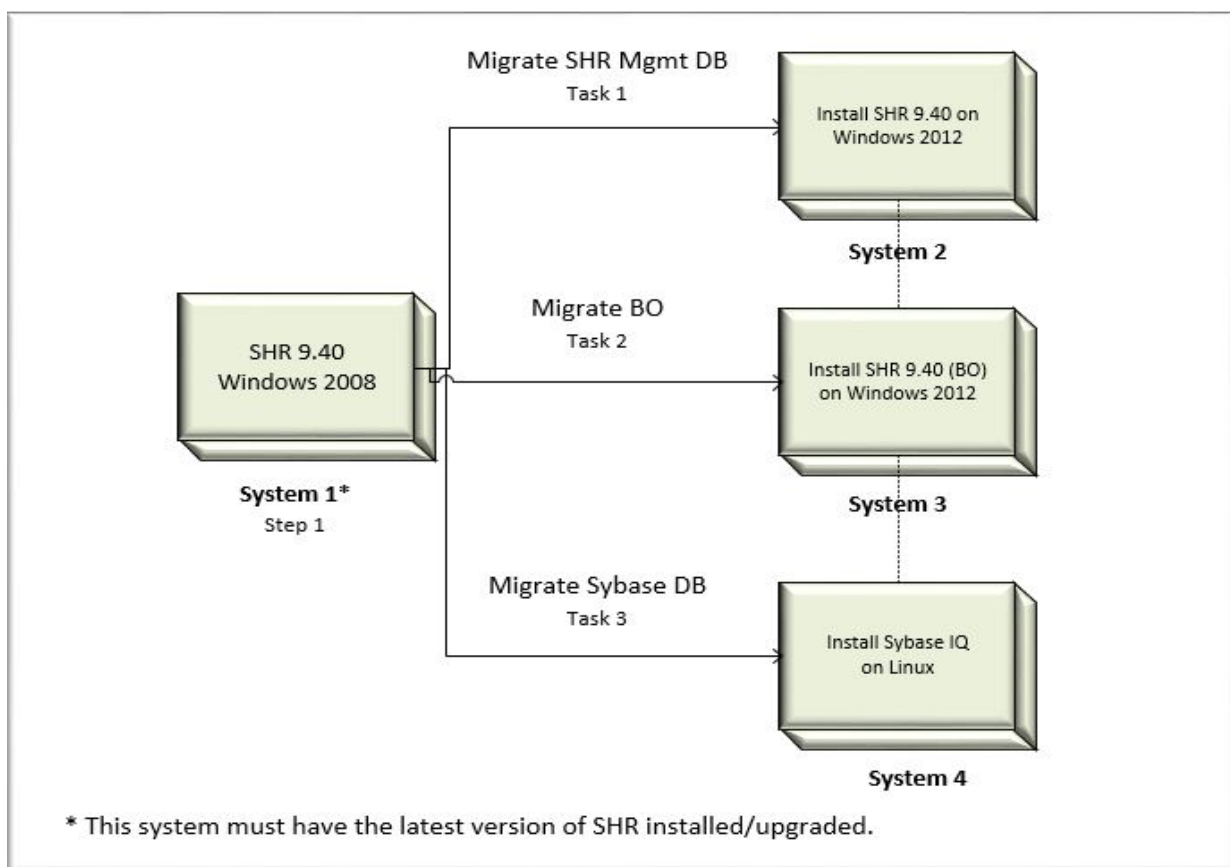
If you have installed SHR in a domain, reconfigure the following services. For more information, see [Configuring SHR Services when SHR is Installed on a Domain](#) section.

- HP PMDB Platform Administrator Service
- HP PMDB Platform Collection Service

If the aggregation of data failed after migration, see [Troubleshooting for Aggregation of Data Failed After Migration](#).

Chapter 9: Migrating a Typical Installation to Custom Installation

This section will guide you on migrating from a Typical (Single-System) Installation to a Custom (Multi-System) Installation where SAP BusinessObjects and SHR Management database is on Windows 2012 operating system and Sybase IQ is on Linux operating system.



Note: Ensure that you have upgraded to the latest version of SHR before migrating to windows 2012 environment.

Prerequisites

Before you proceed with the migration of SHR, complete the following steps:

For Windows:

Step 1:

1. In the System 1, take a backup of the complete SHR setup. For more information, see [Database Backup and Recovery](#).

2. Ensure that the PostgreSQL service is running.
3. Run the following command and take the complete back up of the Management database:

```
Windows: %PMDB_HOME%/../JRE64/bin/java -cp %PMDB_HOME%/lib/Utils.jar  
com.hp.bto.bsmr.common.util.PostgresUpgrade PRE_DB_UPGRADE postgres 21425  
<Backup location> dwabc %PMDB_HOME%
```

Caution: You can perform any one of the following for the License:

- Take a complete backup of System 1. Remove it from the network and use the same IP address and hostname in System 2 and restore the data. OR
- Use **Rehost** option to obtain the license for the IP address of System 2 from the License Management Portal. Contact HP Support for more information.

Step 2:

1. Install SHR on System 2 which runs on Windows 2012 operating system. Ensure that you have the same directory structure similar to the System 1.

For more information, see *HP Service Health Reporter Interactive Installation Guide*.

Caution: The SHR components in all of the systems must have a static IP address.

2. Install SAP BusinessObjects on System 3 which runs on Windows 2012 operating system (bundled with SHR 9.40 media). For more information, see *HP Service Health Reporter Interactive Installation Guide*.
3. On System 4, which runs on Linux operating system, install Sybase IQ (bundled with the SHR 9.40 media). For more information, see *HP Service Health Reporter Interactive Installation Guide*.

Step 3:

1. Perform all the post-installation configuration steps on System 2. See *Primary Configuration* chapter in this guide for the steps. Do not perform the tasks “Selecting the Data Source” and “Configuring the Topology Source” at this moment.
2. Install the content packs on System 2. Ensure that you install the same content packs as in System 1.
3. Validate the installation on all the three systems. Ensure that the services are running. For more information, see *HP Service Health Reporter Interactive Installation Guide*.

Migration

Perform the following tasks for Migration:

Task 1: System 2

Restore the backup of Management database on System 2 as follows:

1. Stop all SHR services. Wait for all processes to finish.
2. Run the following command to verify whether all the required services and processes are stopped:
`%PMDB_HOME%\DR\SHRServiceCheck.bat`
3. Start PostgreSQL service.
4. Run the below command to restore Management database:

Windows: %PMDB_HOME%/../JRE64/bin/java -cp %PMDB_HOME%/lib/log4j-1.2.15.jar;%PMDB_HOME%/lib/utils.jar;com.hp.bto.bsmr.common.util.PostgresUpgrade POST_DB_UPGRADE postgres 21425 <Backup location> dwabc %PMDB_HOME%

5. Restore the following configuration files:

- %PMDB_HOME%\config\collection.properties
- %PMDB_HOME%\data\downtime\downtime.xml if it exists
- %PMDB_HOME%\config\<name>customgroup.xml if it exists

Task 2: System 3

Restore the backup of the SAP BusinessObjects server on System 3. For more information, see [Database Backup and Recovery](#).

Note: Ensure that you use Hostname (short name) of the SHR system 1 as BO repository User ID.

Restore the following configuration files:

- %PMDB_HOME%\BOWebServer\conf\server.xml
- %PMDB_HOME%\BOWebServer\webapps\InfoViewApp\WEB-INF\web.xml
- %PMDB_HOME%\BOWebServer\webapps\CmcApp\WEB-INF\web.xml

Update the host name of System 1 to System 3 in the following files after restore and restart the BusinessObjects service: Business Objects Webserver.

- %PMDB_HOME%/BOWebServer/webapps/InfoViewApp/WEB-INF/web.xml
- %PMDB_HOME%/BOWebServer/webapps/CmcApp/WEB-INF/web.xml

Task 3: System 4

Restore the backup of Sybase IQ to the System 4 as follows:

1. Copy the backup of Sybase IQ files to the System 4.
2. Copy the pmdbConfig file from System 1 to System 4:
copy %PMDB_HOME%\config\pmdbConfig.cfg file from System 1 to \$PMDB_HOME/config folder in System 4.
3. Run the following command:
dos2unix \$PMDB_HOME/config/pmdbConfig.cfg
4. Change the server name in \$PMDB_HOME/config/pmdbConfig.cfg with the remote Sybase IQ system (System 4) short name.
5. Stop the Sybase IQ service in System 4. Perform the following steps:
 - cd /etc/init.d
 - service HP_PMDB_Platform_Sybase stop
6. Verify if the Sybase IQ service is stopped. Perform the following steps:

- Run the following command:

```
ps -ef|grep -i iqsrv
```
 - If the iq service is still running, note the process ID displayed by the command output.
 - Run the command by entering the process ID in <pid>: `kill -9 <pid>`
7. Move all the files in the Sybase database folder to a new location in the system. These files will be recreated by the restore process.
 8. Start Sybase IQ server in System 4 by running the following command:

```
start_iq @/opt/HP/BSM/PMDB/config/pmdbConfig.cfg
```
 9. Connect from System 1 to remote Sybase IQ server on System 4 with the default utility_db password as follows:
 - a. On the SHR system, click **Start > Run**. The Run dialog box appears.
 - b. Type `dbisql` and press ENTER. The Connect dialog box on Interactive SQL program appears.
 - c. Type the following:
 - i. In the User ID field, type **dba**.
 - ii. In the Password field, type **sql**.
 - iii. In Action select **Connect to a running database on another computer** from the drop down.
 - iv. In Host, type the hostname of the System 4.
 - v. In Port, type 21424.
 - vi. In the Server Name field, type the name of the server where the SHR Sybase IQ database is installed.
 - d. Click Connect. The Interactive SQL window opens.
 10. Restore the database as follows:

Tip: The server name can be found in `pmdbConfig.cfg` file. Open the file. The server name is the text succeeding `-n`.

On the SQL Statements box type the following sql statement without gap between the statements:

Note: The following statements are single query. Execute all of them at once.

```
restore DATABASE'<Location of Sybase DB files on System 4>/pmdb.db  
>'from'<Filename with absolute path of Sybase IQ backup folder on System  
4/Full.<day of the backup taken> >  
RENAME IQ_SYSTEM_MAIN TO'<Location of Sybase DB folder on System 4>\pmdb.iq'  
RENAME IQ_SYSTEM_TEMP TO'<Location of Sybase DB folder on System 4>\pmdb.iqtmp'  
RENAME IQ_SYSTEM_MSG TO'<Location of Sybase DB folder on System 4>\pmdb.iqmsg'  
RENAME pmdb_user_main TO'<Location of Sybase DB folder on System 4>\pmdb_user_  
main.iq'
```

For example:


```
restore DATABASE'/sybase_db/pmdb.db'from'/sybase_bkp/Full.monday'  
RENAME IQ_SYSTEM_MAIN TO'/sybase_db/pmdb.iq'  
RENAME IQ_SYSTEM_TEMP TO'/sybase_db/pmdb.iqtmp'  
RENAME IQ_SYSTEM_MSG TO'/sybase_db/pmdb.iqmsg'  
RENAME pmdb_user_main TO'/sybase_db/pmdb_user_main.iq'
```

11. Stop and start the Sybase service:

```
service HP_PMDB_Platform_Sybase stop  
service HP_PMDB_Platform_Sybase start
```

12. Run the following commands using dbisql as pmdb_admin user:

```
DELETE FROM IM_PM_OS_INFO_FILLDETAIL WHERE OS_INFO_ID IN (SELECT IM_PM_OS_INFO_  
ID FROM IM_PM_OS_INFO WHERE upper (HOSTNAME) = UPPER('<short host name of  
System 1>'))  
DELETE FROM IM_PM_OS_INFO WHERE upper (HOSTNAME) = UPPER('<short host name of  
System 1>')  
DELETE FROM IM_PM_APPS_INFO WHERE upper(HOSTNAME) = UPPER('<short host name of  
System 1>')
```

Post-Migration Configurations

Ensure that all the services are up and running in all three systems.

Perform the following in System 2 after migration:

1. To cover the data gaps, edit the config.prp file with the collection initial history values.

```
dbcollector.initHistory = <system downtime for migration in hours>  
collector.initHistory = <system downtime for migration in hours>
```

Note: To ensure that you cover the data gap include additional hours while you enter the value *system downtime for migration in hours*.

For Example:

```
dbcollector.initHistory = 48  
collector.initHistory = 48
```

2. Execute the following query using pgAdmin:

```
Truncate dwabc.PA_LAST_POLL;  
Truncate dwabc.DB_LAST_POLL;
```

3. Perform the following steps to synchronize the collection data sources:

- a. Execute the following query using pgAdmin:

```
UPDATE dwabc.remote_poller SET datasource_status=0
```

- b. Sync collection data sources using **Administrator Console** (Under **Administrator > Collector Configuration** page).

4. Restart the HP_PMDB_Platform_Collection service in System 2.

Verify that SHR is Running Successfully

Launch the following URL and verify that you are able to log on to the Administration Console as administrator:

http://<SHR_Server_FQDN>:21411

Launch the following URL and verify that you are able to log on to the InfoView Console as administrator:

http://<SHR_Server_FQDN>:8080

Note: Recreate Administrator and Collection Services

If you have installed SHR in a domain, reconfigure the following services. For more information, see *"Configuring SHR Services when SHR is Installed in a Domain"* section of the *HP Service Health Reporter Configuration Guide*.

- HP PMDB Platform Administrator Service
- HP PMDB Platform Collection Service

If the aggregation of data failed after migration, see [Troubleshooting for Aggregation of Data Failed After Migration](#).

Part IV: Additional Configurations

This section provides information and procedures to configure secure connection for SHR. This section also provides information to create keystore file using keytool, schedule database backup, and restore the database backup.

Chapter 10: Configuring the HP Operations Agent for Data Collection in Secure Mode

The HP Operations Agent supports HTTP 1.1-based communications interface for data access between client and server applications. However, you can also configure data collection from HP Operations Agent-managed nodes via the secure (HTTPS) mode. Because HTTPS communication is certificate-based, certificates must be installed on the SHR system and on the managed nodes. The SHR system acts as a certificate client and the certificate server (certificate authority) is provided by the HPOM.

If the `SSL_SECURITY` is enabled in agents, then the collection from the agent to SHR fails with **No trusted certificate found** error. The collection happens only with HTTPS protocol and proper certificates installed. To get data, the certificates from certificate server corresponding to the agent(s) should be installed on SHR system or on the remote collector.

To check if the `SSL_SECURITY` is enabled, run the following command:

```
ovconfigchg
```

If `SSL_SECURITY` is set to `ALL` or `REMOTE` then it is enabled.

To install certificates from the server to SHR or remote collector, follow these steps:

Task 1: Configuration on SHR system

1. Log on to SHR machine.
2. To list the installed certificate on SHR machine, run the following command:

```
ovcert -list
```
3. To delete the certificate on SHR machine, run the following command:

```
ovcert -remove <certificate no>
```

where, *certificate no* is the certificate alias number.
4. Enter `Y` in the following prompt to remove the certificate. A status message is displayed.
5. To change the certificate server to OM server, run the following command:

```
ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <OM_SERVER>
```

where, *<OM_SERVER>* is the name of the OM system

or

Run the following command and change the certificate server values manually:

```
ovconfchg -edit
```
6. To request for certificate, run the following command:

```
ovcert -certreq
```
7. Log on to OM system and run the following command to list the certificate:

```
ovcm -listpending -l
```
8. Run the following command to get the certificate ID corresponding to SHR machine:

```
ovcm -grant <certificate ID> -host <shr_hostname>
```

where, <certificate ID> is the certificate ID corresponding to SHR system

<shr_hostname> is the name of the SHR system

9. Run the following commands to verify that the certificates are installed properly:

```
ovcert -list
```

```
ovcert -check
```

10. Run the following command on the SHR system:

```
ovcert -exporttrusted -file <filename> -ovrg server
```

11. Run the following command on the SHR system:

```
ovcert -importtrusted -file <filename>
```

where, <filename> is the name of the file mentioned in the above step.

12. Run the following command to trust the OM server keystore and import the certificate to the SHR local keystore:

```
ovcert -trust <OM_SERVER> -ovrg server
```

where, <OM_SERVER> is the name of the OM server

13. Run the following command to restart the ovc:

```
ovc - restart
```

The collection happens from the agents that are enabled, that is, where SSL_SECURITY is set to ALL or REMOTE.

Note: If you are configuring HTTPS for new remote collector, perform the following "[Task 2a: Configuring HTTPS on new remote collector](#)" below. If you are configuring HTTPS for already existing remote collector, perform the following "[Task 2b: Configuring HTTPS on an existing remote collector](#)" on the next page.

Task 2a: Configuring HTTPS on new remote collector

Perform the following steps once the new remote collector is installed.

1. Go to %PMDB_HOME%\bin\script (on Windows) and \$PMDB_HOME/bin/script (on Linux) and run the following command to configure the poller with OM server:

```
perl configurePoller.pl <OM_Server>
```

2. Ensure that you have added the new remote collector in OM server and the certificate request is accepted.
3. Run the following commands on the remote collector to verify that the certificates are installed properly:

```
ovcert -list
```

```
ovcert -check
```

4. Log on to SHR system and run the following command:

```
C:\>ovcert -exporttrusted -file C:\trusted_cert -ovrg server
```

5. Copy the certificate file generated in the above step to the new remote collector.

6. Run the following command on the remote collector to import the trusted certificate file:

```
ovcert -importtrusted -file C:\trusted_cert
```

7. To get the coreID from SHR system, follow these steps:
 - a. Log on to SHR system and run the following command:

```
ovcoreid
```

You have to note the core ID displayed by the above command.
8. Run the following command on the remote collector and edit the MANAGER and MANAGER_ID parameters:

```
ovconfchg -edit
```

Set the MANAGER parameter to *<SHR server name>* and MANAGER_ID to the core ID you noted in the above step.
9. Restart the ovc.
10. Log on to the SHR Administration Console. Go to **Administrator > Collector Configuration** and configure the new remote collector.
For information on configuring the new remote collector, see ["Task 5: Configuring the Collectors Installed on Remote Systems" on page 50](#).

Task 2b: Configuring HTTPS on an existing remote collector

1. Run the following commands on the remote collector to check the existing certificate and remove it:

```
ovcert -list
```

```
ovcert -remove
```
2. Run the following command to change the certificate server from SHR Server to OM Server:

```
ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <OM_SERVER>
```

where, *<OM_SERVER>* is the name of the OM system
or
Run the following command and change the certificate server values manually:

```
ovconfchg -edit
```
3. To request for certificate, run the following command:

```
ovcert -certreq
```
4. Log on to OM system and run the following command to list the certificate:

```
ovcm -listpending -l
```
5. Run the following command to get the certificate ID corresponding to remote collector :

```
ovcm -grant <certificate ID> -host <Remotecollector_hostname>
```

where, *<certificate ID>* is the certificate ID corresponding to SHR system
<Remotecollector_hostname> is the host name of remote collector
6. Run the following commands on remote collector to verify that the certificates are installed properly:

```
ovcert -list
```

```
ovcert -check
```
7. Log on to SHR system and run the following command:

```
ovcert -exporttrusted -file <file_name> -ovrg server
```

where, *<file_name>* is the trusted certificate file name

8. Copy the certificate file generated in the above step to the remote collector.

9. Run the following command on the remote collector to import the trusted certificate file:

```
ovcert -importtrusted -file <file_name>
```

where, *<file_name>* is the trusted certificate file name exported in the [Step 7](#).

10. Log on to the SHR Administration Console.

11. To verify that proper collection is happening, go to **Administrator > Collector Configuration** and click **Test** and then click **Save**.

Chapter 11: Configuring the Report Drill Feature Settings

SHR includes the SAP BusinessObjects InfoView portal that enables you to view the generated reports. SAP BusinessObjects InfoView provides a Drill feature that you can use to view information at a daily, monthly, and yearly level. However, when drilling up or down within a report, sections of the report might not display the relevant data for the specified level. This is because the report blocks lose the synchronization between the Drill options in the report. To ensure that the reports display the correct data, you need to re-establish the synchronization by configuring the SAP BusinessObjects InfoView Preference settings.

1. Launch the Administration Console in a web browser:
 - a. Launch the following URL:
`http://<SHR_Server_FQDN>:21411`
The Home page opens.
 - b. Type **administrator** in the **Login Name** field and click **Log In** to continue.
The **Home** page is displayed.
2. In the Administrator Console, click **Administration > SAP BOBJ**.
The SAP BOBJ page is displayed.
3. Click **Launch InfoView** to open SAP BusinessObjects InfoView.
The BusinessObjects InfoView Login page opens.
4. Type the SAP BusinessObject InfoView user name and password in the **User Name** and **Password** field, respectively.
5. Click **Log On**.
The SAP BusinessObjects InfoView portal opens.
6. Under **Personalize**, click **Preferences**.
The Preferences page opens.
7. Click **Web Intelligence**.
8. Under **Drill options**, select the **Synchronize drill on report blocks** option, and Click **OK**.
9. Close the web browser.

Chapter 12: Create Password for the Administrator Account

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

1. Launch the Administration Console in a web browser:
 - a. Launch the following URL:
`http://<SHR_Server_FQDN>:21411`
The Home page opens.
 - b. Type **administrator** in the **Login Name** field and click **Log In** to continue.
The **Home** page is displayed.
2. In the Administrator Console, click **Administration > SAP BOBJ**.
The SAP BOBJ page is displayed.
3. Click **Launch CMC**.
The Log On to the Central Management Console page is displayed.
4. On the **Log On to the Central Management Console** login screen, in the **User Name** field, type **Administrator**.
5. Click **Log On**. The **CMC Home** page appears.
6. Click **Users and Groups**. The **Users and Groups** page appears.
7. On the right pane, double-click **Administrators**.
8. Right-click **Administrator** and then click **Properties**. The **Properties:Administrator** dialog box appears.
9. Under **Enterprise Password Settings**, in the **Password** field, type a new password.
10. In the **Confirm** field, retype the password to confirm it.
11. Click **Save & Close** to accept the changes.
12. Click **Log Out** to exit the Central Management Console.

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

Chapter 13: Configuring the Internal Alerting Service

The Home page of Administration Console displays the connectivity status, runtime file distribution, content health summary, collection status and alerts. SHR can be configured to send traps or emails when there is a failure in SHR system. You can also view the alerts in administration console of SHR. Alerts are sent when a service stops or when there is a failure in data processing.

The **HPE_PMDB_Platform_IA** service is responsible for internal alerting. Internal Alerting (IA) is a supportability tool used to alert when some parts of SHR are non operative. IA also sends alerts for current status of the services mentioned below. You can receive the following types of alerts from IA:

- Email
- SNMP trap
- Health alerts on Administration Console

The following services are monitored by IA:

1. Collection Configuration
2. Duplicate Dimensions
3. IQ Insufficient System Configuration
4. IQ Index Corruption
5. Server Runtime Data on Disk
6. Collector Runtime Data on Disk
7. Data Latency
8. Service Down
9. Connectivity
10. Collector Certificate
11. System Resource

Scheduled Execution

The Service Down and System Resource are monitored every hour. However, all the other features are monitored at 8:00 AM local time every day.

Configure Internal Alerting Service

1. Open the `IA_Config.prp` file in a text editor from `%PMDB_HOME%\data` (on Windows) or `$PMDB_HOME/data` (on Linux).

To configure e-mail, follow these steps:

- a. Enter the e-mail ID where you want to receive the alerts in `email.to` parameter.
- b. Enter the domain name of the system where SHR is installed in `email.from` parameter.
- c. Enter the domain name of the mail server in `email.host` parameter.

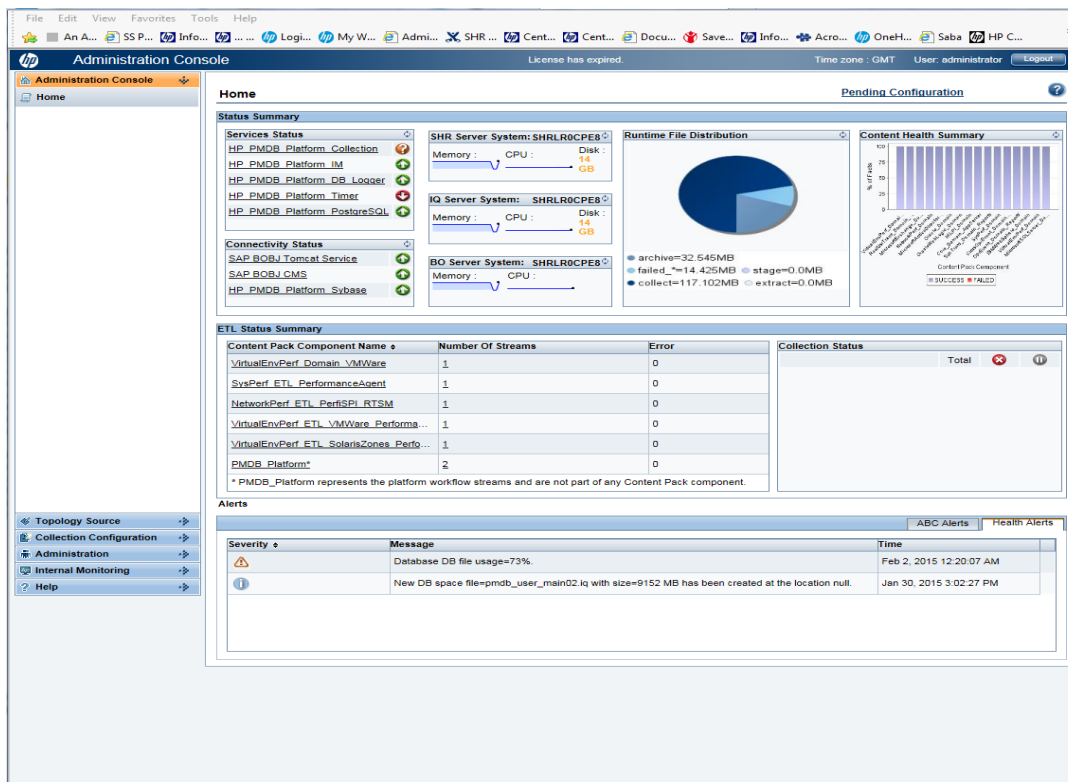
To configure SHR to send SNMP traps to the third party SNMP Trap receiver, follow these steps:

Note: Copy the hp-shr.mib and hp-nnmi.mib files from %PMDB_HOME%\config (on Windows) and \$PMDB_HOME/config (on Linux) to the system where SNMP Trap Receiver is installed. Load these .mib files to the SNMP Trap Receiver.

- a. Enter the IP address of the system where SNMP Trap Receiver is installed in snmp.TargetHost parameter.
 - b. Enter the port number of the system where SNMP Trap Receiver is installed in snmp.TargetPort parameter.
2. Save and close the IA_Config.prp file.
 3. Restart the HP_PMDB_Platform_IA service.
 4. Run the following command to enable the internal alerting service:
 enableIA

You can also view the SHR Health alerts in the Administration Console.

1. Log on to Administration Console. The Home page is displayed.
2. Click **Health Alerts** tab to view the internal alerts.



Change threshold value for free space of the disk

You will get an alert if the free space falls below 15% of the disk space. If you receive an alert when the free space falls below 15% of the disk space, reset the threshold value by editing the im.disk.space.warnLimit (Free Space Threshold) parameter in config.prp located at {PMDB_HOME}/data/.

Chapter 14: Configuring Manual Restart of Tomcat Services

Note: This section is applicable only for SHR on Red Hat Enterprise Linux 6.6.

SHR supports Red Hat Enterprise Linux 6.6. After you install SHR, complete the post installation configuration and install the Content Pack, log on to InfoView or Central Management Console (CMC). If you are not able to access Infoview or CMC, you have to restart the Tomcat services manually.

To restart the Tomcat services manually, follow these steps:

1. Open the Linux command line console and log on to SHR system as root user.
2. Run the following command to shutdown the Tomcat services and wait for some time:

```
sh /opt/HP/BSM/BO/bobje/tomcatshutdown.sh
```

Wait till the shutdown is complete.

3. Run the following command to check if the Tomcat is gracefully shutdown.

```
ps -eaf |grep -i BOWebServer
```

If the Tomcat is still running, note the PID listed.

- a. Run the following command to kill the Tomcat process:

```
kill -9 <PID>
```

where, <PID> is the process ID noted in the step above.

4. Run the following command to restart the Tomcat services:

```
sh /opt/HP/BSM/BO/bobje/tomcatstartup.sh
```

You can now log on to Administrator Console and access the Infoview or CMC.

Chapter 15: 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, following these steps:

1. Take a backup of `util_db.ini` in `$PMDB_HOME/./Sybase/IQ-15_4/bin64` folder (**Linux**) or `%PMDB_HOME%\..\Sybase\IQ-15_4\Bin64` folder (**Windows**).
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:

On Windows:

```
%PMDB_HOME%\..\Sybase\IQ-15_4\Bin64\dbfhide new.ini util_db.ini
```

On 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.

Chapter 16: Configuring Secure Connection for SHR (HTTPS)

SHR has two console interfaces, the Administration console and the SAP BusinessObjects InfoView. It is possible to run both the consoles in a secured environment with HTTPS network protocol or in a non-secured environment with HTTP network protocol. The default protocol for both the consoles is HTTP. To set up a secured environment for Administration console and SAP BusinessObjects InfoView console, you must configure HTTPS network protocol.

Creating a Keystore File

Before you configure secure connection, you must create a keystore file containing the SHR server certificate and private key.

The keystore file is password-protected. SHR enables you to configure keystore location and password using keystore and keystorepasswd properties. Keystore path should be specified using forward slash in windows system. Keystore type property enables you to specify the type of the keystore, supported values are JKS and PKCS12.

Note: It is possible to create a keystore file using other tools.

To create a keystore file using keytool, run the following command:

General Syntax:

```
keytool -genkey -keystore <keystorefile_name> -alias <alias_name> -keyalg <alg_name>
```

For example,

On Windows:

```
keytool -genkey -keystore C:\SHRTest.jks -alias changeit -keyalg RSA
```

On Linux:

```
keytool -genkey -keystore opt/SHRTest.jks -alias changeit -keyalg RSA
```

The parameters that need to be passed to create a keystore certificate are as follows:

Parameter name	Example
<i>keystorefile_name</i>	On Windows: C:\SHRTest.jks On Linux: opt/SHRTest.jks

Parameter name	Example
<i>alias_name</i>	changeit
<i>keyalg_name</i>	RSA

Configuring Secure Connection (HTTPS)

You can configure secure connection for the Administration console and the InfoView console.

For the Administration console of SHR

To configure a secure connection for the Administrations console of SHR, follow these steps:

Task 1: Stop the HP_PMDB_Platform_Administrator service

- **On Windows:**

To stop HP_PMDB_Platform_Administrator service:

- Click **Start > Run**. The Run dialog box opens.
- Type `services.msc` in the Open field, and then press ENTER. The Services window opens.
- On the right pane, right-click **HP_PMDB_Platform_Administrator**, and then click **Stop**.

- **On Linux:**

Run the command

```
service HP_PMDB_Platform_Administrator stop
```

Task 2: Edit the server.xml file

Tip: Take a backup of the `server.xml` file before editing.

- Uncomment the SSL Connector tag that has the port value set to 21412.
- Set the following fields in the `server.xml` file, located at:

- **On Windows:**

```
%PMDB_HOME%\adminserver\conf/
```

- **On Linux:**

```
$PMDB_HOME/adminserver/conf/
```

Note: If you have not already created the keystore file, see ["Creating a Keystore File"](#) on the previous page.

Field	Description
keystoreFile	Full path of the keystore file where you have stored the server certificate to be loaded. The <code><keystorefile_name></code> you gave while creating the keystore

Field	Description
	file.
keystorePass	The password used to access the server certificate from the specified keystore file.
keystoreType	The type of keystore file to be used for the server certificate. The supported value is JKS.
keyAlias	The alias used for the server certificate in the keystore. The <code><alias_name></code> you gave while creating the keystore file.

Note: You do not have to set the `keyalg` in `server.xml` file.

Task 3: Edit the config.prp file

Tip: Take a backup of the `config.prp` file before editing.

Note: You have to perform this task only if HTTPS is turned on for BO web server.

1. Set the following fields in the `config.prp` file, located at:

- **On Windows:**

`%PMDB_HOME%\data`

- **On Linux:**

`$PMDB_HOME/data`

Field	Value
<code>bo.protocol</code>	<code>https</code>
<code>ucmdb.protocol</code>	<code>https</code>
<code>bo.ssl.enabled.port</code>	<code>8443</code>

Note: `bo.ssl.enabled.port` is set to the port number specified in the `port` attribute of `connector` tag in the `server.xml` file, the default value is 8443.

Task 4: Uncomment the security constraint in web.xml

1. Browse to the following folder:

- **On Windows:**

`%PMDB_HOME%\adminServer\webapps\BSMRApp\WEB-INF`

- **On Linux:**

`$PMDB_HOME\adminServer\webapps\BSMRApp\WEB-INF`

2. Open `web.xml` with a text editor.

3. Uncomment the following lines:


```
<!-- Uncomment the below tag for Enabling SSL connection-->
<!-- <security-constraint>
<web-resource-collection>
<web-resource-name>Entire Application</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint> -->
```

Task 5: Start the HP_PMDB_Platform_Administrator service

- **On Windows:**

To start HP_PMDB_Platform_Administrator service:

1. Click **Start > Run**. The Run dialog box opens.
2. Type `services.msc` in the Open field, and then press **ENTER**. The Services window opens.
3. On the right pane, right-click **HP_PMDB_Platform_Administrator**, and then click **Start**.

- **On Linux:**

Run the command

```
service HP_PMDB_Platform_Administrator start
```

Task 6: Verify the configuration.

To verify the configuration, log on to the Administration console using the following URL:

1. `https://<hostname>: 21412`
where, *<hostname>* is the name of the SHR system.
2. `http://<hostname>: 21411`
where, *<hostname>* is the name of the SHR system.

For the InfoView Console and CMC of SHR

To enable HTTPS communication for InfoView Console and CMC of SHR, follow these steps:

Note: In a custom installation of SHR, perform the following tasks on the system where SHR BusinessObjects is installed.

Task 1: Stop the SAP BusinessObjects Webserver service

- **On Windows:**

To stop the SAP BusinessObject WebServer service:

1. Click **Start > Run**. The Run dialog box opens.
2. Type `services.msc` in the Open field, and then press **ENTER**. The Services window opens.
3. On the right pane, right-click **BusinessObject WebServer**, and then click **Stop**.

- **On Linux:**

1. Go to `/opt/HP/BSM/PMDB/BOWebServer/bin`
2. Run the following command:
`./shutdown.sh`

Task 2: Edit the server.xml file

Tip: Take a backup of the `server.xml` file before editing.

Open the `server.xml` file located at `%PMDB_HOME%\BOWebServer\conf` (for Windows) or `$PMDB_HOME/BOWebServer/conf` (for Linux):

To edit the file, follow these steps:

1. Uncomment the SSL Connector tag that has the port value set to 8443.
2. To create a keystore file using `keytool`, see ["Creating a Keystore File " on page 118](#).
3. Set the following fields in the `server.xml` file to the values as given in the description.

Field	Description
<code>keystoreFile</code>	Full path of the keystore file where you have stored the server certificate to be loaded. The <code><keystorefile_name></code> you gave while creating the keystore file.
<code>keystorePass</code>	The password used to access the server certificate from the specified keystore file.
<code>keystoreType</code>	The type of keystore file to be used for the server certificate. The supported value is JKS.
<code>keyAlias</code>	The alias used for the server certificate in the keystore. The <code><alias_name></code> you gave while creating the keystore file.

Note: You do not have to set the `keyalg` in `server.xml` file.

Task 3: Update the web.xml of BO Infoview, CMC, and OpenDocument web applications

1. Browse to the following folders:
 - **For InfoView**
`%PMDB_HOME%\BOWebServer\webapps\InfoViewApp\WEB-INF`
 - **For CMC**
`%PMDB_HOME%\BOWebServer\webapps\CmcApp\WEB-INF`
 - **For OpenDocument**
`%PMDB_HOME%\BOWebServer\webapps\OpenDocument\WEB-INF`
2. Open `web.xml` with a text editor.
3. Add the following in the `web.xml`.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Entire Application</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

Task 4: Start the SAP BusinessObjects WebServer

- **On Windows:**

To stop SAP BusinessObject WebServer service:

1. Click **Start** > **Run**. The Run dialog box opens.
2. Type `services.msc` in the Open field, and then press **ENTER**. The Services window opens.
3. On the right pane, right-click **BusinessObject WebServer**, and then click **Stop**.

- **On Linux:**

1. Go to `/opt/HP/BSM/PMDB/BOWebServer/bin`,
2. Run the following command:
`./startup.sh`

Task 5: Verify configuration

To verify whether the configuration is successful, follow these steps:

1. Log on to `https://<hostname>:8443/InfoViewApp`
where, `<hostname>` is the name of the SHR system.
2. Log on to `https://<hostname>:8443/CmcApp`
where, `<hostname>` is the name of the SHR system.

Deleting a Certificate from the Keystore

To delete a certificate from the keystore file using `keytool`, run the following command:

General Syntax:

```
keytool -delete -keystore <keystorefile_name> -alias <alias_name>
```

For example,

On Windows:

```
keytool -delete -keystore C:\SHRTest.jks -alias changeit
```

On Linux:

```
keytool -delete -keystore opt/SHRTest.jks -alias changeit
```

The parameters that need to be passed to delete a certificate are as follows:

Parameter name	Example
<i>keystorefile_name</i>	On Windows: C:\SHRTest.jks On Linux: opt/SHRTest.jks
<i>alias_name</i>	changeit A unique alias name associated with the certificate that needs to be deleted.

Chapter 17: Client Authentication Certificate for SHR

SHR provides certificate based client authentication. SHR verifies the identity by validating the certificate and authorizes the user using SAP BusinessObjects.

Authentication and Authorization

SHR uses SAP BusinessObjects for authentication and authorization. SAP BusinessObjects user accounts are managed by SAP BusinessObjects Central Management console. You must be a SAP BusinessObjects administrator to access SHR Administration console. By default, SHR uses username/password based authentication mechanism. You can also configure SHR to use client certificate based authentication by following the steps in "[Task 4: Configuring for Certificate-based Authentication](#)" for Administration console and for SAP BusinessObjects view, "[Configuring SAP BusinessObjects InfoView](#)". SHR verifies the identity of the user by validating the certificate and authorizes the user using SAP BusinessObjects.

Prerequisites of Certificate Based Authentication

Before you configure certificate based authentication ensure that the following prerequisites are met.

Task 1: Create a keystore file containing SHR server certificate and private key

The keystore file is password protected. SHR enables you to configure keystore location and password using keystorepath and keystorepasswd properties. Keystorepath should be specified in the properties files in "[Task 4: Configuring for Certificate-based Authentication](#)" of [Configuring SHR Administration Console](#) and "[Task 4: Set up the certificate-based configuration](#)" of [Configuring SAP BusinessObjects InfoView](#). Keystoretype property enables you to specify the type of the keystore, supported values are **JKS** and **PKCS12**. The certificate alias in the keystore is specified using the keyalias property as shown in the following table:

Property name	Example
Keystorepath	\\certs\serverkeystore.jks (Linux) C:\\certs\\serverkeystore.jks (Windows)
Keystorepasswd	changeit
Keyalias	shserver
Keystoretype	JKS

Task 2: Create a keystore file containing the Certifying Authority (CA) certificates

You must create a keystore file containing the CA certificates trusted by the SHR server. This file is password protected. SHR enables you to configure truststore by setting the truststorepath,

truststorepasswd, and truststoretype properties to values as shown in the following table. The *truststorepath* should be specified in the properties files in "[Task 4: Configuring for Certificate-based Authentication](#)" and "[Task 4: Set up the certificate-based configuration](#)".

Property name	Example of values
truststorepath	\certrelated\Trustkeystore (Linux) C:\\certrelated\\Trustkeystore (Windows)
truststorepasswd	changeit
truststoretype	JKS

Task 3: Determine if certificate revocation check should be enabled

You should set com.sun.net.ssl.checkRevocation to true, to enable certificate revocation check. SHR supports two methods of checking for revoked certificates.

- Certificate Revocation List (CRL) - A CRL contains information about revoked certificates and is downloaded from the CA. SHR extracts the CRL distribution point URL from the certificate. You should set com.sun.security.enableCRLDP to true to enable this check.
- Online Certificate Status Protocol (OCSP) - OCSP is a protocol for checking revocation of a single certificate using an online service called an OCSP responder. You should set ocsp.enable to true to enable revocation check using OCSP protocol. SHR extracts the OCSP URL from the certificate for validating the certificate. If you want to configure a local OCSP responder service, SHR enables you to configure it using ocsp.responderURL property.

For details on how to enable certificate revocation, CRL and OCSP on SHR Administration Console, see "[Task 4: Configuring for Certificate-based Authentication](#)" in "[Configuring SHR Administration Console](#)"

For details on how to enable certificate revocation, CRL and OCSP on SHR BusinessObjects InfoView, see "[Task 4: Set up the certificate-based configuration](#)" in "[Configuring SAP BusinessObjects InfoView](#)".

Task 4: Determine the proxy server address if there is a proxy between the SHR server and internet

In case of a proxy server, you must set it to enable SHR server to download the CRL. You can configure the proxy server as:

http.proxyHost	set the http proxy Hostname
http.proxyPort	set the http proxy Port number
https.proxyHost	set the https proxy Hostname
https.proxyPort	set the https proxy Port number

For more details, see "[Task 4: Configuring for Certificate-based Authentication](#)" in "[Configuring SHR Administration Console](#)"

Task 5: Determine the username extraction mechanism

The username extraction mechanism depends on the format of your certificate. The user name extracted from the certificate should match the user names configured in SAP BusinessObjects. SHR enables you to extract username using SubjectDN and Subject Alternative Name (SAN) mechanisms.

To configure the username extraction mechanism you have to make the changes in properties field, entry, type, pattern and OID in the server.xml file.

```
<Realm className="com.hp.bto.bsmr.SHRSecureAuth.auth.SHRRealm" field="SubjectDN"
entry="CN" Type="" oid="" pattern="" useSubjectDNonMatchFail="true"/>
```

- To extract username from SubjectDN, set the following values to the properties

Property name	Value
field	SubjectDN
entry	set to CN to indicate CN as the username set to OU to indicate OU as the username

The entry property enables you to specify the entry that should be considered as username in SubjectDN. You can also use a pattern to extract username from SubjectDN instead of using entry parameter. To configure a pattern to extract user name from SubjectDN, use pattern parameter. For example, if the pattern is configured as EMAILADDRESS=(.+@) and if abc@hp.com is the value of emailaddress field, then abc is extracted as the user name.

- To extract username from Subject Alternative Name (SAN)

Set the property field to the value SAN. You can configure rcf822Name or otherName part of the SAN username using the property Type. To configure rcf822Name, set the value of the property Type to rcf822Name. To configure otherName set the value of the property type to otherName and set the value of object identifier (OID) to OID.

By default, SHR extracts username from CN.

You can configure SHR to allow a user to log on using smart card only. To enable smart card logon, you must set the property smartcard.enable to true.

The location of the file server.xml is shown in the table below:

For configuring	Path
Administrator console	\$PMDB_HOME/adminserver/conf (for Linux) %PMDB_HOME%\adminserver\conf (for Windows)
SAPInfoview BusinessObjects	\$PMDB_HOME/BOWebServer/conf (for Linux) %PMDB_HOME%\BOWebServer\conf (for Windows)

Task 6: Import Certificate and Configure Browser

- Import the certificate that has been issued by the root CA to the SHR server. Import it to your web browser using the **Trusted Root Certificate** tab available in the Internet Explorer. For details, see the Internet Explorer help.
- Configure your web browser to accept the protocol TLSv1, here v1 indicates the version.

Note: For High Availability, configure both servers.

SHR enables you to configure certificate based authentication for Administration console interface and SAP BusinessObjects InfoViewApp interface.

Configuring Username Extraction Method

Username extraction can be configured by editing the `server.xml` file, for details, see [Task 5: Determine the username extraction mechanism](#).

Configuring SHR Administration Console

Before you proceed, ensure that the post-install configuration of SHR is successful. To configure SHR Administration console for Certificate Based Authentication:

Task 1: Configuring shared secret

Shared secret is used to establish trusted authentication. You must enter the shared secret in character format only.

1. Type `http://<HostName>:21411` on the browser to log on to the Administration Console of SHR.
2. Navigate to **Administration > Security > BO Trusted Authentication**

Security

LW-SSO BO Trusted Authentication

BO Trusted Authentication Configuration

Enabled

Shared Secret

Save

3. Select the **Enabled** check box.
4. Type the **Shared Secret**.
5. Click **Save**.

After successful configuration, the message given below is displayed:

Security

i BO Trusted Authentication Configuration saved successfully!

BO Trusted Authentication Configuration

Enabled

Shared Secret

Save

Task 2: Stop the HP_PMDB_Platform_Administrator service

- **On Windows**

To stop the HP_PMDB_Platform_Administrator service, follow these steps:

1. Click **Start > Run**. The Run dialog box opens.
2. Type `services.msc` in the Open field, and then press **ENTER**. The Services window opens.
3. On the right pane, right-click `HP_PMDB_Platform_Administrator`, and then click **Stop**.

- **On Linux**

Run the following command:

```
service HP_PMDB_Platform_Administrator stop
```

Task 3: Configuring the config.prp file

In the file `config.prp`, located at `%PMDB_HOME%\datafolder` (for Windows) and `$PMDB_HOME/data` (for Linux) set the given value to the following fields.

Field	Value
<code>shr.loginMethod</code>	<code>certbased</code>
<code>shr.auth.classes</code>	<code>com.hp.bto.bsmr.security.auth.BOTrustedExceptionAuthenticator</code>

Task 4: Configuring for Certificate-based Authentication

Specify following parameters in `adminserverclientauth.prp` file located at `$PMDB_HOME/data` (for Linux) and `%PMDB_HOME%\data` folder (for Windows). Edit the following fields and set the values according to the given description:

Field	Description
<code>truststorepath</code>	Full path of the truststore file, which is to use to validate client certificates.
<code>truststorepasswd</code>	The password to access the trust store.
<code>truststoretype</code>	The type of keystore used for the trust store.
<code>keystorepath</code>	Full path of the keystore file where you have stored the server certificate to be loaded.
<code>keystorepasswd</code>	The password used to access the server certificate from the specified keystore file.
<code>keystoretype</code>	The type of keystore file to be used for the server certificate.
<code>keyAlias</code>	The alias used to for the server certificate in the keystore
<code>smartcard.enable</code>	Set to true to enable smart card logon and to false to disable smart card logon.
<code>http.proxyHost</code>	HTTP proxy Host name.

Field	Description
http.proxyPort	HTTP proxy Port number.
com.sun.net.ssl.checkRevocation	Set it as true for enabling revocation and to false to disable revocation.
com.sun.security.enableCRLDP	Set it to true to enable CRL revocation, otherwise set it to false.
crlFile	Enter the CRL file path.
ocsp.enable	Set it to true to enable OSCP based revocation, otherwise set it to false.
ocsp.responderURL	Set the OCSP responder URL.

Note: You must set the OSCP based revocation to false, when the CRL based revocation is set to true and vice versa.

After setting the properties value, do the following:

- **On Windows**

- a. Go to the %PMDB_HOME%\bin folder.
- b. Run the command

```
perl adminserverclientauth.pl -authType clientcert -configFile <config file location>
```

where *<config file location>* indicates the full path of adminserver.prp file
For example, %PMDB_HOME%\data\adminserverclientauth.prp

- **On Linux**

- a. Go to \$PMDB_HOME/bin folder.
- b. Run the command

```
perl adminserverclientauth.pl -authType clientcert -configFile <config file location>
```

where *<config file location>* indicates the full path of adminserver.prp file.
For example, \$PMDB_HOME/data/adminserverclientauth.prp

Task 5: Configure Username Extraction

Ensure that CN entry in the SubjectDN field is extracted as username by SHR. Modify the file server.xml as described in [Task 5: Determine the username extraction mechanism](#).

Task 6: Start the HP_PMDB_Platform_Administrator service

- **On Windows**

To start the HP_PMDB_Platform_Administrator service, follow these steps:

1. Click **Start > Run**. The Run dialog box opens.
2. Type `services.msc` in the Open field, and then press **ENTER**. The Services window opens.
3. On the right pane, right-click HP_PMDB_Platform_Administrator, and then click **Start**.

- **On Linux**

`service HP_PMDB_Platform_Administrator start`

Task 7: Verify certificate based authentication

1. Type `http://<HostName>:21411` on the Web browser to log on to the Administration Console of SHR.
2. Click **Log on with a digital certificate**.

Configuring SAP BusinessObjects InfoView

If you have not configured the shared secret, perform it using "[Configuring SHR Administration Console](#)" on page 128.

Note: In a custom installation of SHR with a remote SAP BusinessObjects system, copy the `SHRTrustedPrinciple.conf` file from `<Install_Dir>/PMDB/adminServer/conf` to `<Install_Dir>/PMDB/BOWebServer/conf` on the system where SAP BusinessObjects is installed.

Task 1: To configure the InfoView console and Open Document for certificate based authentication

Note: In a custom installation of SHR, perform this tasks on the system where SHR BusinessObjects is installed.

- **On Windows**

To Stop the SAP BusinessObject WebServer Service:

- a. Log on to the host system as administrator.
- b. Click **Start > Run**. The Run dialog box opens.
- c. Type `services.msc` in the **Open** field, and then press **ENTER**. The Services window opens.
- d. Right-click the **Business Object WebServer service** and select **Stop** to stop the service.

- **On Linux**

- a. Go to `/opt/HP/BSM/PMDB/BOWebServer/bin`
- b. Run the command
`./shutdown.sh`

Task 2: Stop the HP_PMDB_Platform_Administrator service

- **On Windows**

To stop the HP_PMDB_Platform_Administrator service, follow these steps:

1. Click **Start > Run**. The Run dialog box opens.
2. Type `services.msc` in the Open field, and then press **ENTER**. The Services window opens.
3. On the right pane, right-click `HP_PMDB_Platform_Administrator`, and then click **Stop**.

- **On Linux**

1. `service HP_PMDB_Platform_Administrator stop`

Task 3: Edit the config.prp file

In the file `config.prp`, located at `%PMDB_HOME%\data` folder (for Windows) and `$PMDB_HOME/data` (for Linux) set the given value to the field.

Field	Value
<code>bo.protocol</code>	<code>https</code>

Task 4: Set up the certificate-based configuration

Note: In a custom installation of SHR, perform this tasks on the system where SHR BusinessObjects is installed.

Set the following fields in the file `BOclientauth.prp`, located at `$PMDB_HOME/data` (for Linux) and `%PMDB_HOME%\data` folder (for Windows) to the values as given in the description.

Field	Description
<code>truststorepath</code>	Full path to the truststore file
<code>truststorepasswd</code>	The password to access the trust store
<code>truststoretype</code>	The type of key store used for the trust store
<code>keystorepath</code>	Full path of the keystore file where you have stored the server certificate to be loaded.
<code>keystorepasswd</code>	The password used to access the server certificate from the specified keystore file.
<code>keystoretype</code>	The type of keystore file to be used for the server certificate.
<code>keyAlias</code>	The alias used to for the server certificate in the keystore.
<code>smartcard.enable</code>	Set it to true for enabling smart card logon or else set it to false.
<code>http.proxyHost</code>	HTTP proxy Host name
<code>http.proxyPort</code>	HTTP proxy Port number
<code>https.proxyHost</code>	HTTPS proxy Host name
<code>https.proxyPort</code>	HTTPS proxy Port number
<code>com.sun.net.ssl.checkRevocation</code>	Set it to true to enable revocation or else set it to false.
<code>com.sun.security.enable-CRLDP</code>	Set it to true to enable CRL revocation or else set it to false.
<code>crlFile</code>	Enter the CRL file path.
<code>ocsp.enable</code>	Set it to true for OSCP based revocation or else set it to false.
<code>ocsp.responderURL</code>	Set the OSCP responder URL.

Note: You must set the OSCP-based revocation to false, when the CRL based revocation is set to true and vice versa.

After setting the properties, do the following:

- **On Windows**

1. Go to the %PMDB_HOME%\bin folder.
2. Run the command

```
perl BOclientauth.pl -authType clientcert -configFile <config file location>
```

where *<config file location>* indicates the full path of BOclientauth.prp file. For example, %PMDB_HOME%\data\BOclientauth.prp.

- **On Linux**

1. Go to the \$PMDB_HOME/bin folder.
2. Run the command

```
perl BOclientauth.pl -authType clientcert -configFile <config file location>
```

where *<config file location>* indicates the full path of BOclientauth.prp file.
For example, \$PMDB_HOME/data/BOclientauth.prp.

Task 5: Start the SAP BusinessObjects WebServer Service

Note: In a custom installation of SHR, perform this tasks on the system where SHR BusinessObjects is installed.

- **On Windows**

1. Log on to the host system as administrator.
2. Click **Start > Run**.
3. Type `services.msc` in the Open field, and then press **ENTER**. The Services window opens.
4. Right-click the **SAP BusinessObject WebServer service** and select **Start** to start the service.

- **On Linux**

- a. Go to the /opt/HP/BSM/PMDB/BOWebServer/bin folder.
- b. Run the command `./startup.sh`

Task 6: Start the HP_PMDB_Platform_Administrator service

- **On Windows**

To start the HP_PMDB_Platform_Administrator service, follow these steps:

1. Click **Start > Run**. The Run dialog box opens.
2. Type `services.msc` in the Open field, and then press **ENTER**. The Services window opens.
3. On the right pane, right-click HP_PMDB_Platform_Administrator, and then click **Start**.

- **On Linux**

1. `service HP_PMDB_Platform_Administrator start`

Task 7: Verify certificate based authentication

1. Type `http://<HostName>:8080/InfoViewApp` on the Web browser to log on to the InfoView Console of SHR.

2. Log on to InfoView console.
3. If you see the screen given below, then the configuration is complete.



4. You can now login to the InfoView console with a digital certificate.

Task 8: Enabling InfoView to authenticate users through LDAP or Active Directory

1. From the SHR system, open the `web.xml` file located at `%PMDB_HOME%/BOWebServer/webapps/InfoViewApp/WEB-INF/web.xml`.
2. Set the value of the `<authentication.visible>` parameter to `<true>`.
3. Save and close the file.
4. Restart the web application server.

Chapter 18: Database Backup and Recovery

SHR enables you to back up and recover the database to prevent data loss in the event of a database failure. It is recommended that you take regular backup of the database before you begin using SHR in production.

Database backup and recovery of SHR includes planning for taking regular back up of SHR databases, and creating a backup of key configuration and license files. SHR enables you to back up and recover the Sybase IQ database, the SAP BusinessObjects database, and the SAP BusinessObjects file store to prevent data loss in the event of a disaster.

Note: While planning for database backup, for the backup storage space, you must have twice the storage space of the database size that you calculated using the *Licensing and Sizing Calculator*.

For sizing calculation, refer *Licensing and Sizing Calculator* from <https://hpln.hp.com/group/service-health-reporter>.

SHR provides the following database backup options:

- **Full Backup:** A full backup enables you to take a complete back up of the following SHR databases (including the database files and transaction logs):
 - Sybase IQ
 - SAP BusinessObjects (SQL Anywhere)
 - Management database tables (PostgreSQL)

In addition, you can take a complete back up of the SAP BusinessObjects file store.

- **Incremental Backup:** An incremental backup enables you to take a backup of the transaction logs. It takes a backup of the files that have been modified or added since the last full backup.

Tip: It is recommended to take a full backup every week and an incremental backup daily.

Important Considerations

- You must schedule the full backup and the incremental backup tasks to run at regular intervals.
- In the event of a database failure, you can recover the SHR database from the backup location. The backup system and the primary system must be identical with same hardware specifications, operating systems, SHR version, file path, topology, post installation configurations and deployed content packs.
- If you have changed any of the configuration files (Example: CAC), performance tuning in the primary setup then perform all those changes for the disaster recovery setup.

Caution: SHR must have a static IP address. You must set up the SHR Disaster Recovery environment (remote or local) with the same IP address and host name similar to the primary SHR server to restore the permanent license. No additional license is required for restoring SHR.

Creating a Backup of SHR Databases on Windows

Note: In a Custom Installation scenario, perform the following steps on the systems where you have installed the SHR components.

For Sybase IQ Database

Tip: To backup the Sybase IQ database in a custom installation scenario, you must provide the path or location of the remote Sybase IQ database server.

Task 1: Edit the Backup Scripts

SHR provides two backup scripts for full and incremental backup, respectively. Before you begin the backup, edit these scripts to fit the requirements. These scripts are available in the %PMDB_HOME%\scripts\Sybase folder. The scripts are:

- For Full Backup: %PMDB_HOME%\scripts\Sybase\IQ_backup_full.sql
- For Incremental Backup: %PMDB_HOME%\scripts\Sybase\IQ_backup_incr_since_full.sql

To edit the scripts, follow these steps:

1. Browse to the %PMDB_HOME%\scripts\Sybase folder.
2. Open IQ_backup_full.sql with the Notepad application.

In the last parameter within the .sql script, create a folder (for example, E:\HP-SHR\Backup) where you want to save the backup files.

Note: Do not use an escape sequence (/n, /r) in the path where you want to save the backup files. Example: C:/new, C:/readonly.

```
dsi_pmdb_backup 'FULL',NULL,'READWRITE_FILES_
ONLY',NULL,NULL,NULL,NULL,NULL,'D','BACKUP'
```

Similarly, for the incremental backup, enter the location for backup as follows:

```
dsi_pmdb_backup 'INCREMENTAL_SINCE_FULL',NULL,'READWRITE_FILES_
ONLY',NULL,NULL,NULL,NULL,NULL,'D','BACKUP'
```

Note: For an SHR installation with a remote database, BACKUP denotes a valid path on the Sybase IQ database server.

3. Run the following from the %PMDB_HOME%\DR\ folder:
 - Execute_FullBackup_Script.bat for full backup.
 - Execute_IncrSncFullBackup_Script.bat for incremental backup.

After the scripts are run, a database backup is created with file name suffixed with day of the week at the specified location.

The scripts generate the following log files:

- Full backup - %PMDB_HOME%\tmp\Execute_IQ_backup_full.out
- Incremental backup - %PMDB_HOME%\tmp\Execute_backup_incr_since_full.out

Task 2: Edit the Copy Backup Script

SHR provides a Copy Backup script that takes a backup of the previous full backup file in the specified location.

To edit the copy backup script, open the %PMDB_HOME%\DR\Copy_Backup.bat script with a text editor, and then enter the location of the existing full backup file and the location where you want to save the copied files before starting the full backup procedure.

```
COPY "location of existing full backup file" "copy to location"> %PMDB_
HOME%\tmp\Copy_Backup.txt 2>&1 /Y /V
```

For an SHR installation with a remote database, you must run this script on the system where the Sybase IQ database is installed.

An example of the script is as follows:

```
COPY "E:\HP-SHR\Backup\Full*" "E:\HP-SHR\Backup\Old\" > %PMDB_HOME%\tmp\Copy_
Backup.txt 2>&1 /Y /V
```

Task 3: Schedule the Backup

Use the Windows Task Scheduler to schedule and run backup scripts. It is recommended to take a full backup once a week and an incremental backup once a day.

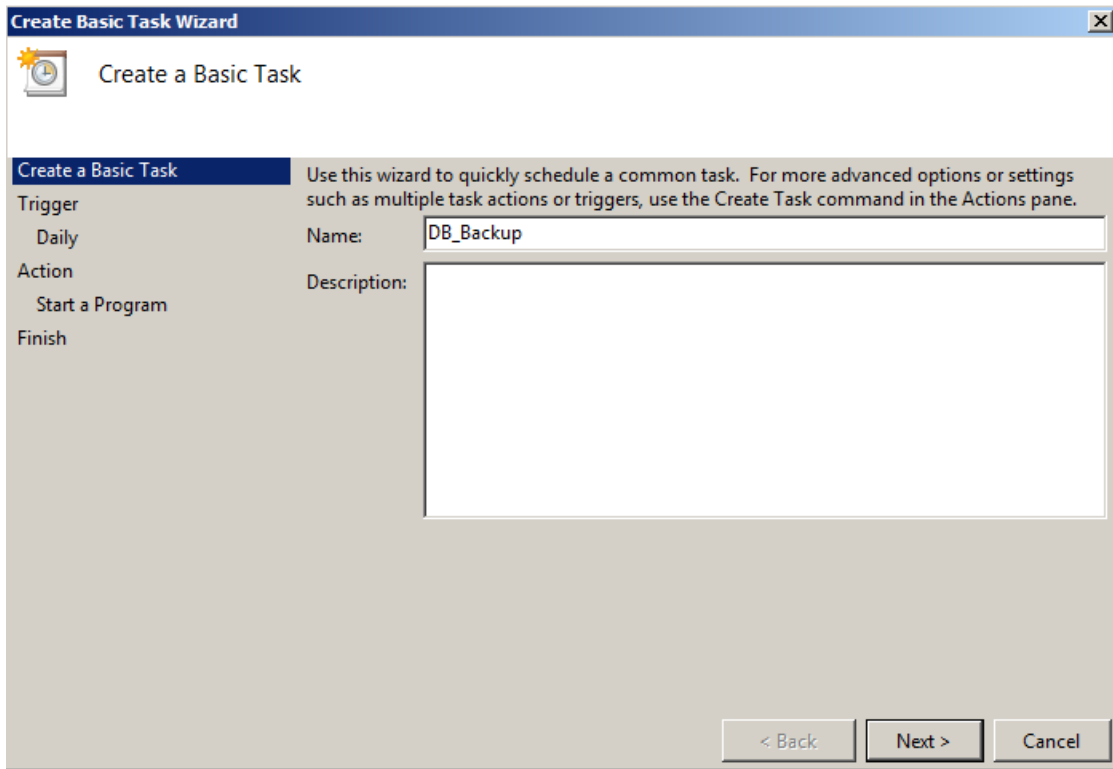
Note: If Sybase IQ is installed on a remote system, then ensure to schedule the backup activity on the system where the Sybase IQ database is installed. Do not schedule this task on the SHR system.

Schedule to Run the Copy Backup Script

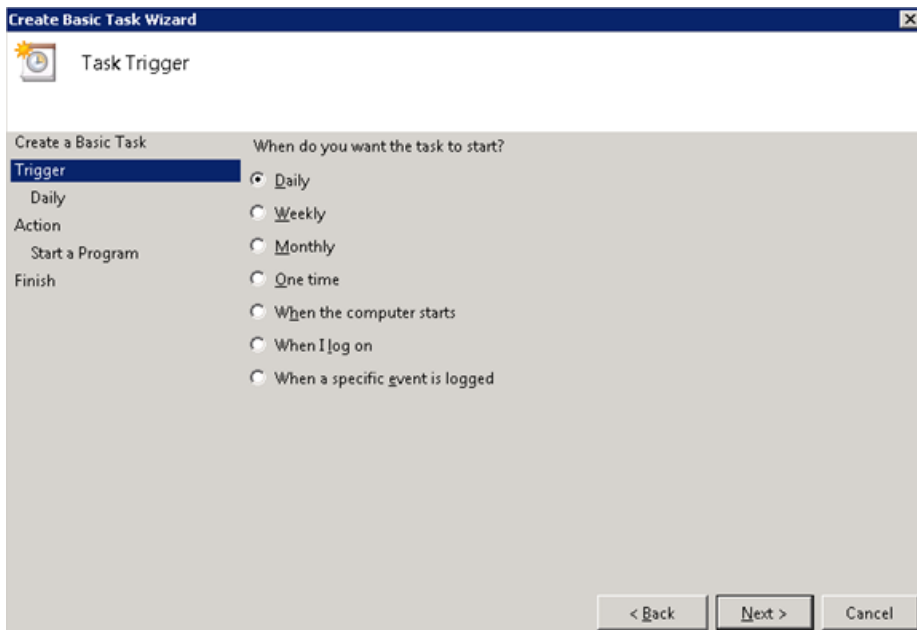
The Copy Backup script creates a copy of the full backup database files in the specified location to avoid overwriting an existing full backup. You must schedule to run the Copy Backup script every time before you run the full backup script.

On Windows 2008

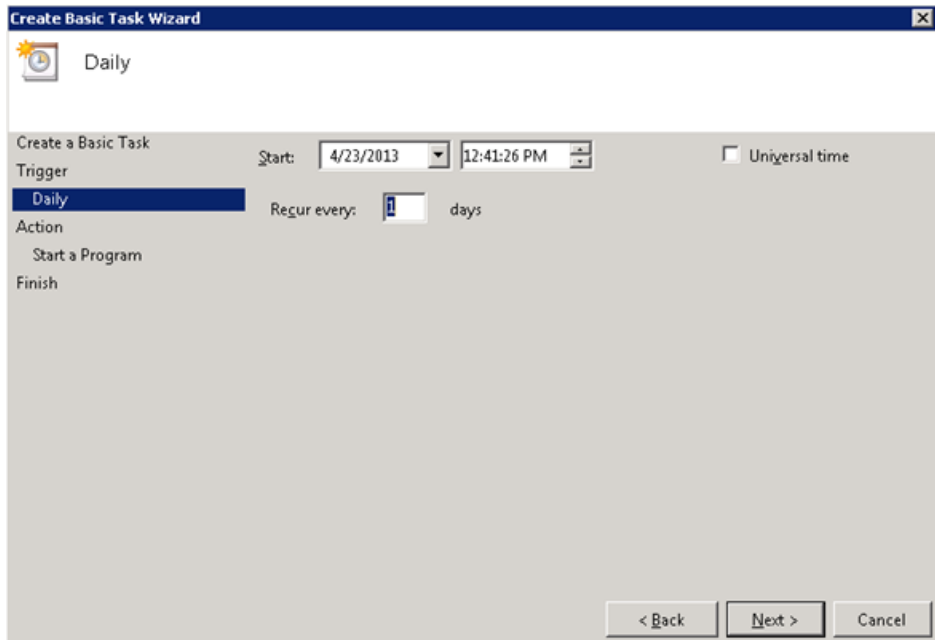
1. Go to **Start > Program > Administrative Tools > Task Scheduler**. The Task Scheduler window opens.
2. In the Task Scheduler window, right-click **Create Basic Task**. The Create Basic Task wizard opens. Type a name for the task, and then click **Next**.



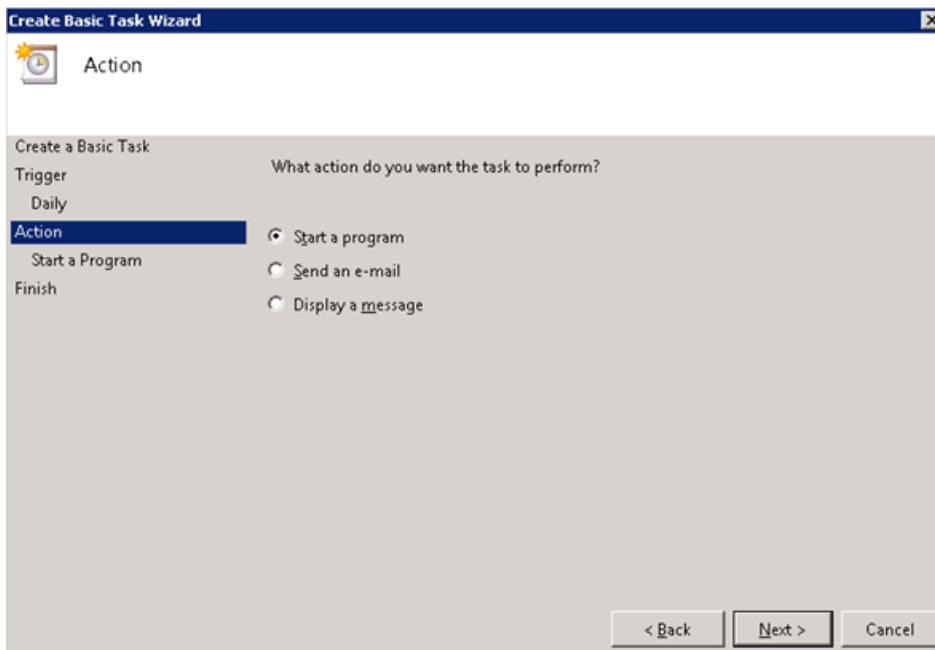
3. Select **Daily**, and then click **Next**.



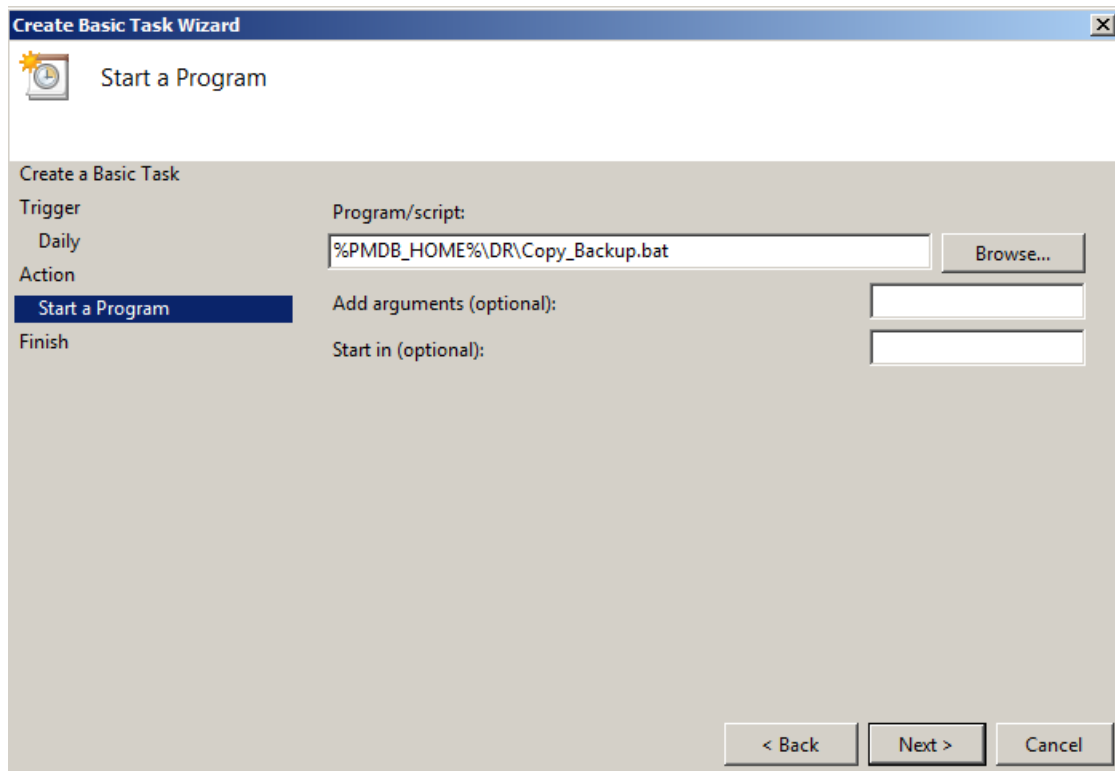
4. Select the start time, type 1 in the **Recur every** text box, and then click **Next**.



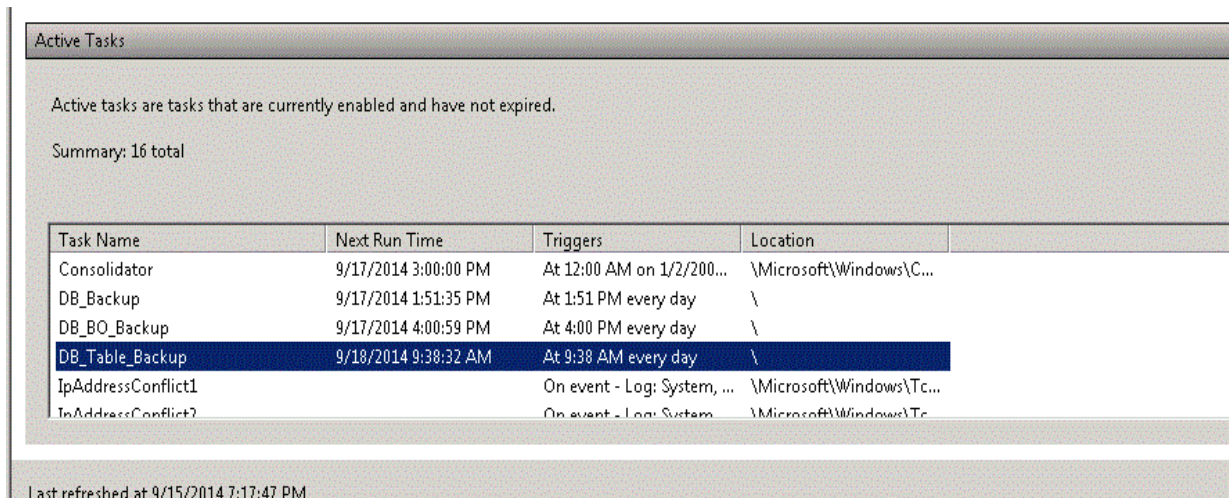
5. Select **Start a program**, and then click **Next**.



6. Browse to %PMDB_HOME%\DR, select **Copy_Backup.bat**, and then click **Next**.



7. Click **Finish**. You can check the task created in the **Active Tasks** of the Task Scheduler window.



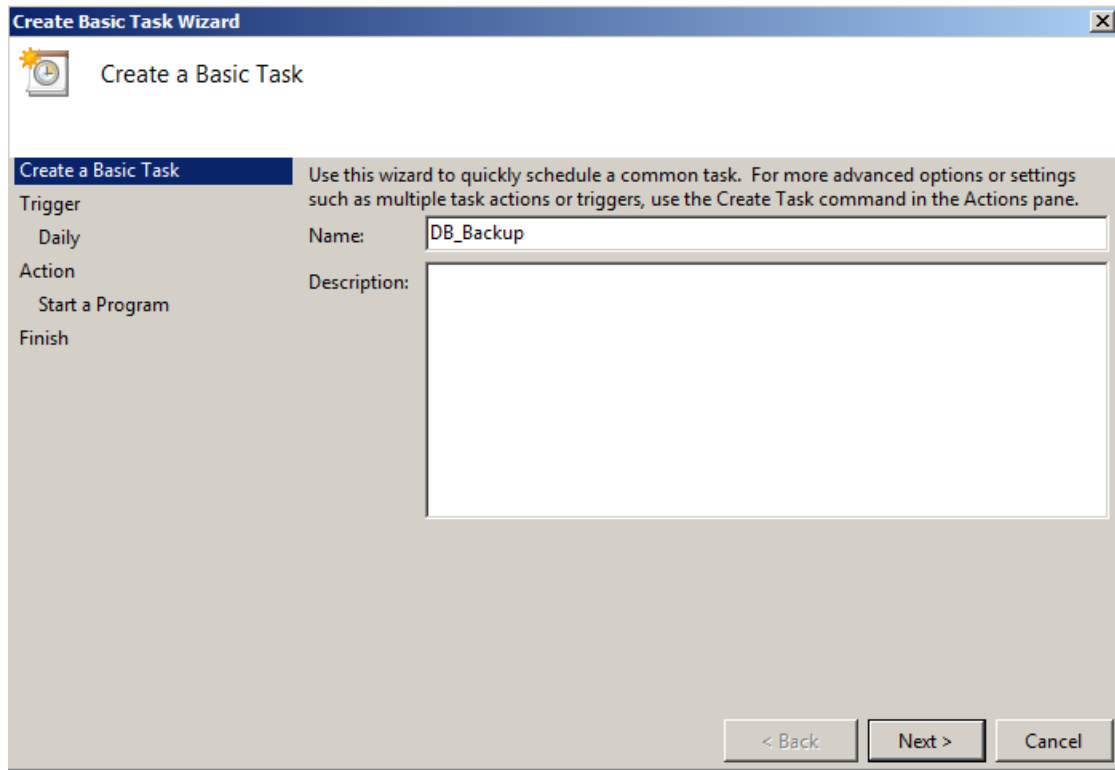
Schedule to Run the Full Backup Script

You must schedule to run the Full Backup script *after* the Copy Backup script.

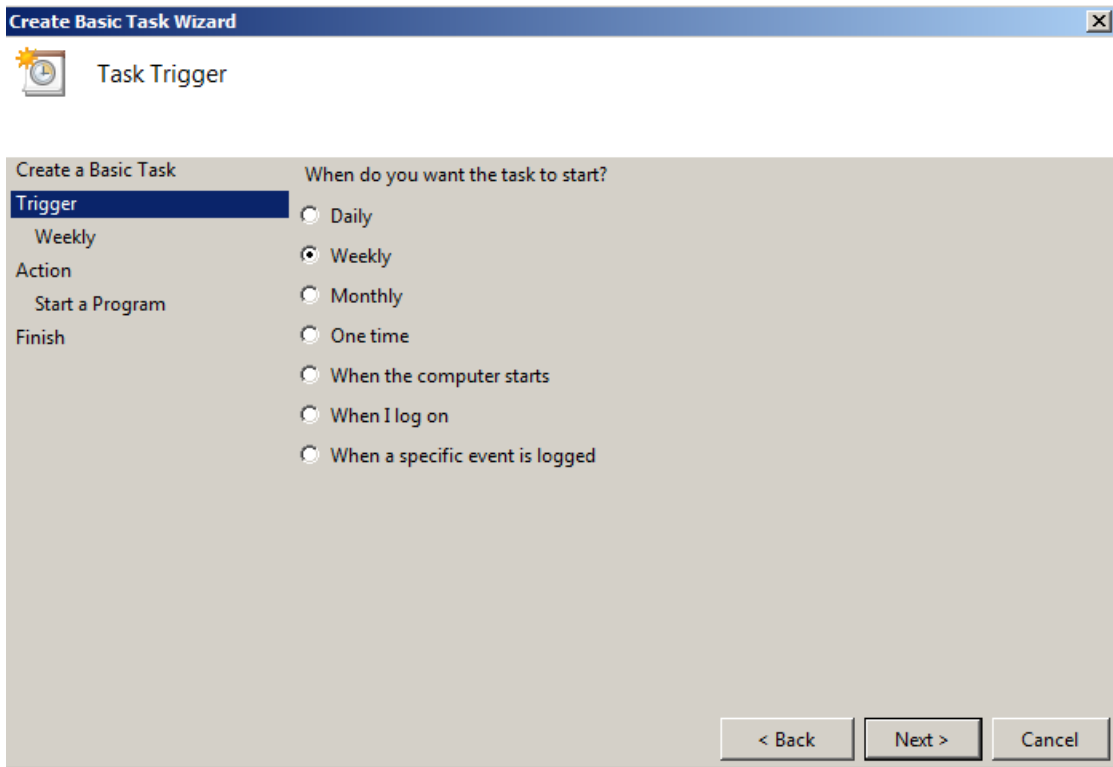
On Windows 2008

1. Go to **Start > Program > Administrative Tools > Task Scheduler**. The Task Scheduler window opens.

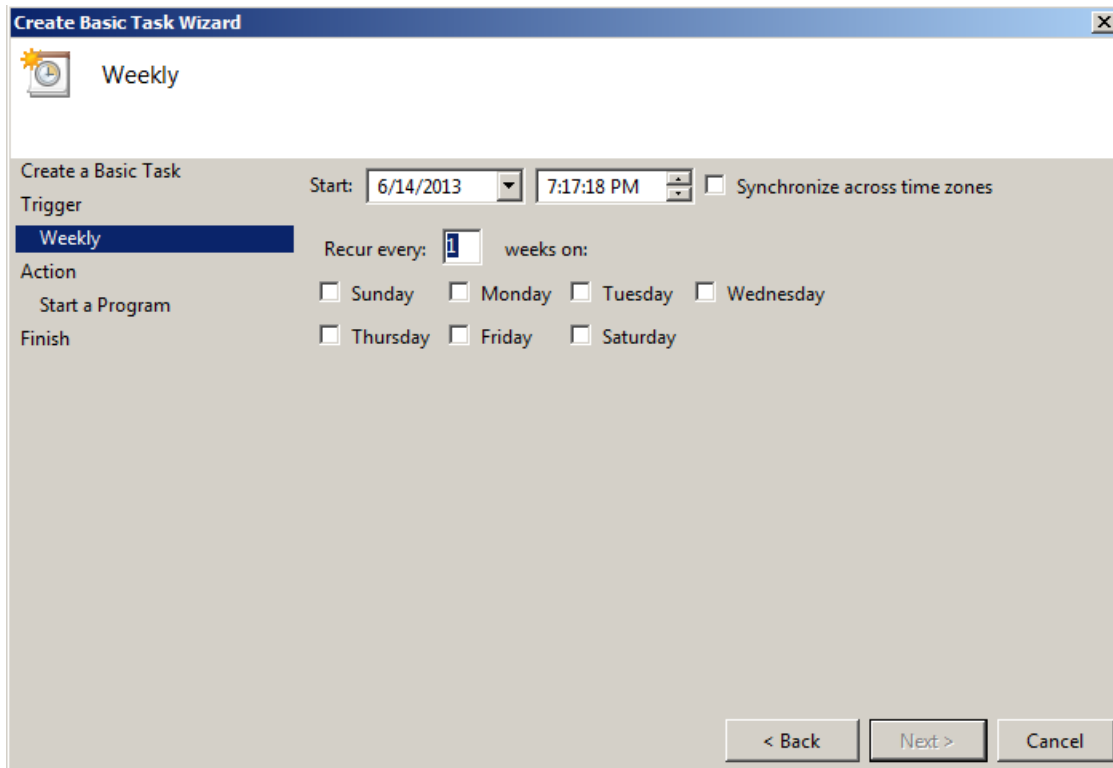
2. In the Task Scheduler window, right-click **Create Basic Task**. The Create Basic Task wizard opens. Type a name for the task, and then click **Next**.



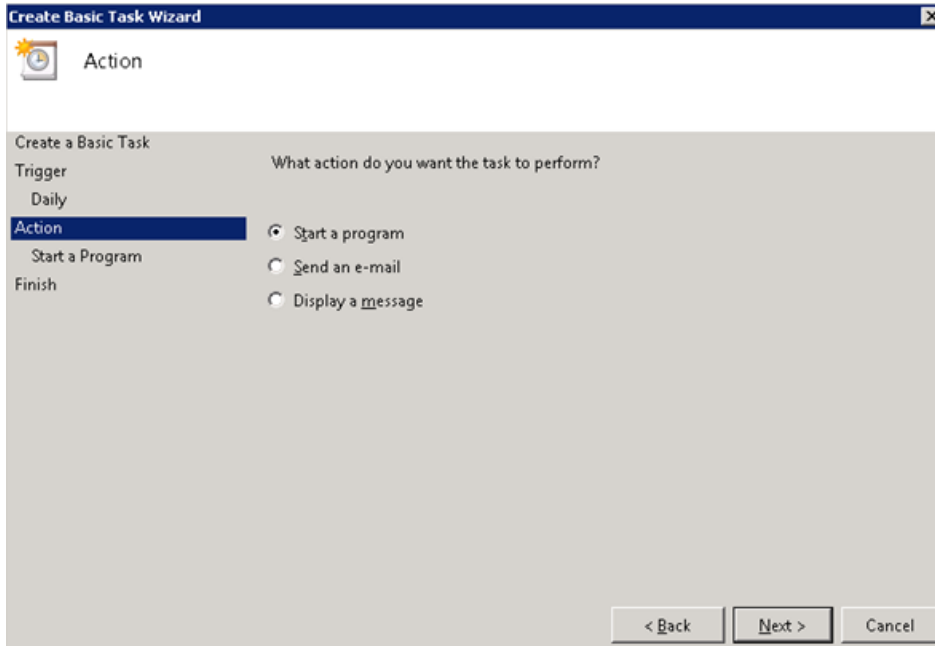
3. Select **Weekly**, and then click **Next**.



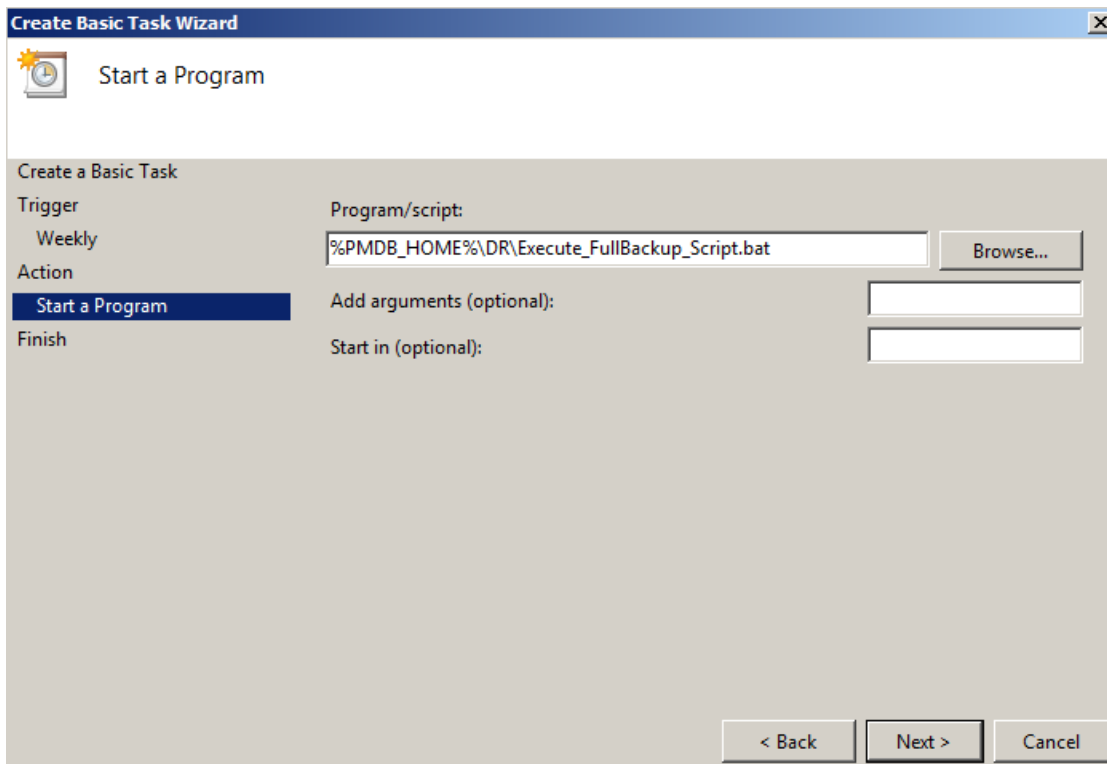
4. Select the start time, day of the week, type one in the **Recur every** text box, and then click **Next**.



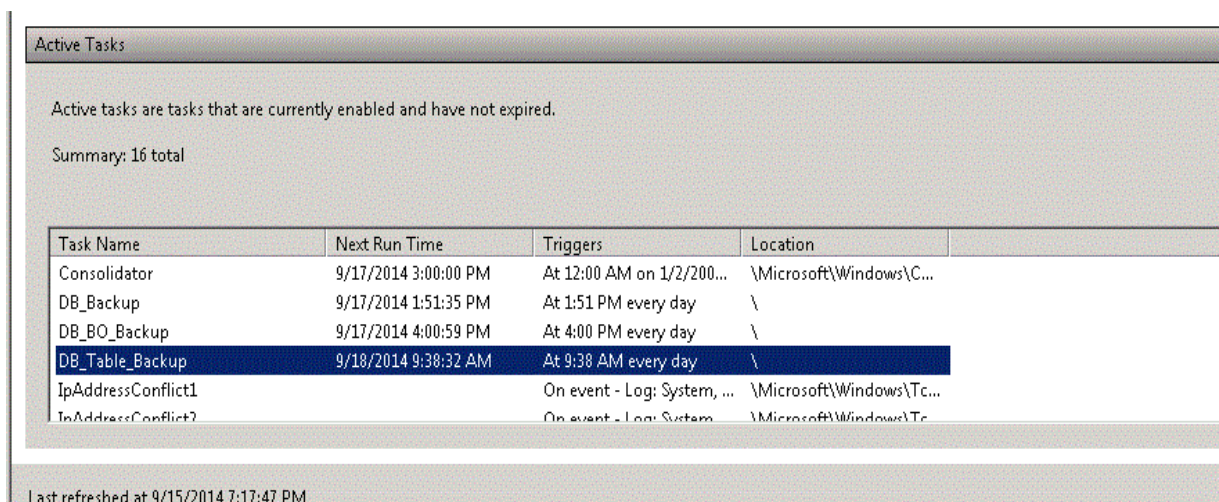
5. Select **Start a program**, and then click **Next**.



6. Browse to %PMDB_HOME%\DR, select **Execute_FullBackup_Script.bat**, and then click **Next**.



7. Click **Finish**. You can check the task created in the **Active Tasks** of the Task Scheduler window.



Active Tasks

Active tasks are tasks that are currently enabled and have not expired.

Summary: 16 total

Task Name	Next Run Time	Triggers	Location
Consolidator	9/17/2014 3:00:00 PM	At 12:00 AM on 1/2/200...	\Microsoft\Windows\C...
DB_Backup	9/17/2014 1:51:35 PM	At 1:51 PM every day	\
DB_BO_Backup	9/17/2014 4:00:59 PM	At 4:00 PM every day	\
DB_Table_Backup	9/18/2014 9:38:32 AM	At 9:38 AM every day	\
IpAddressConflict1		On event - Log: System, ...	\Microsoft\Windows\Tc...
InAddressConflict2		On event - Log: System	\Microsoft\Windows\Tc...

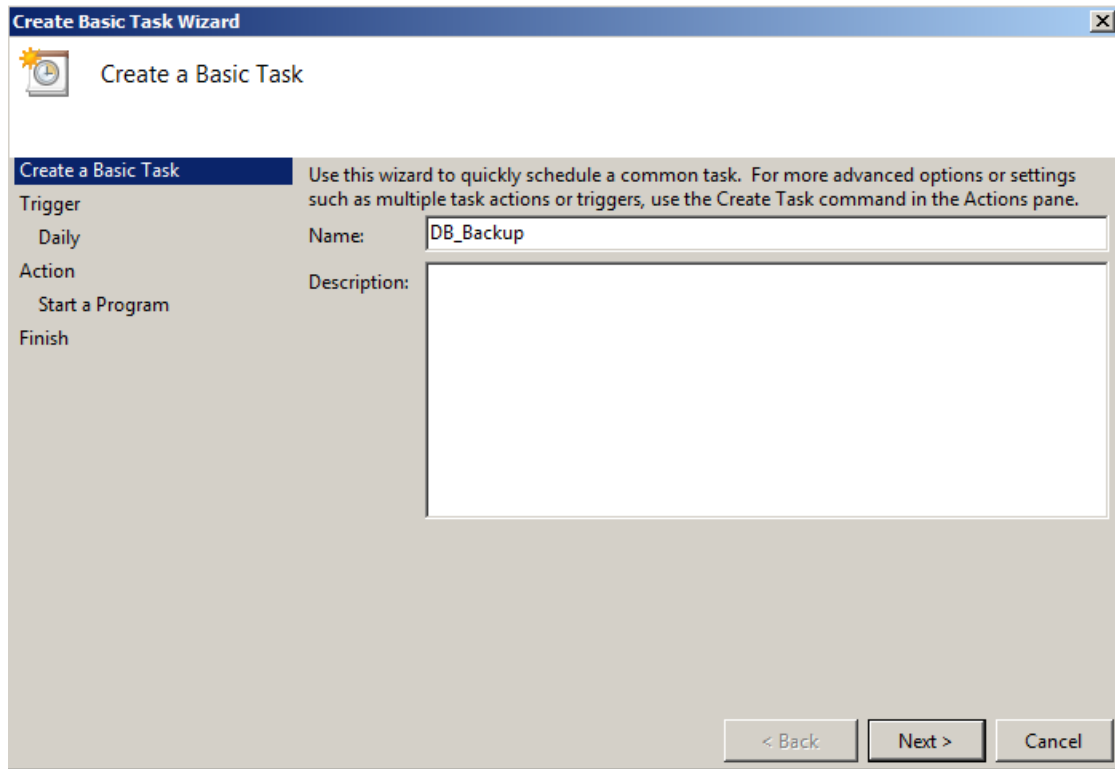
Last refreshed at 9/15/2014 7:17:47 PM

Schedule to Run the Incremental Backup Script

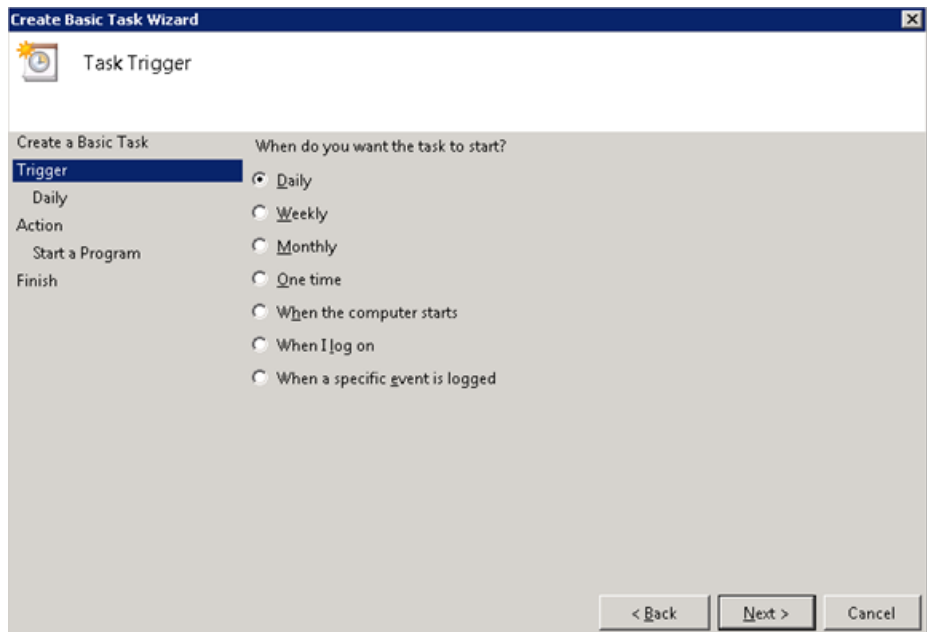
You must schedule to run the Incremental Backup script once a day.

On Windows 2008

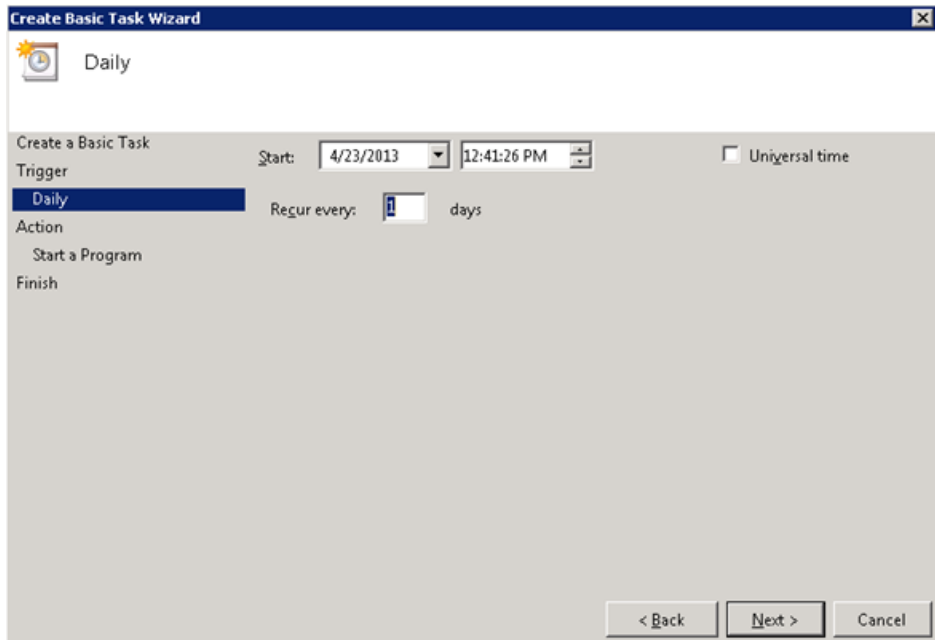
1. Go to **Start > Program > Administrative Tools > Task Scheduler**. The Task Scheduler window opens.
2. In the Task Scheduler window, right-click **Create Basic Task**. The Create Basic Task wizard opens. Type a name for the task, and then click **Next**.



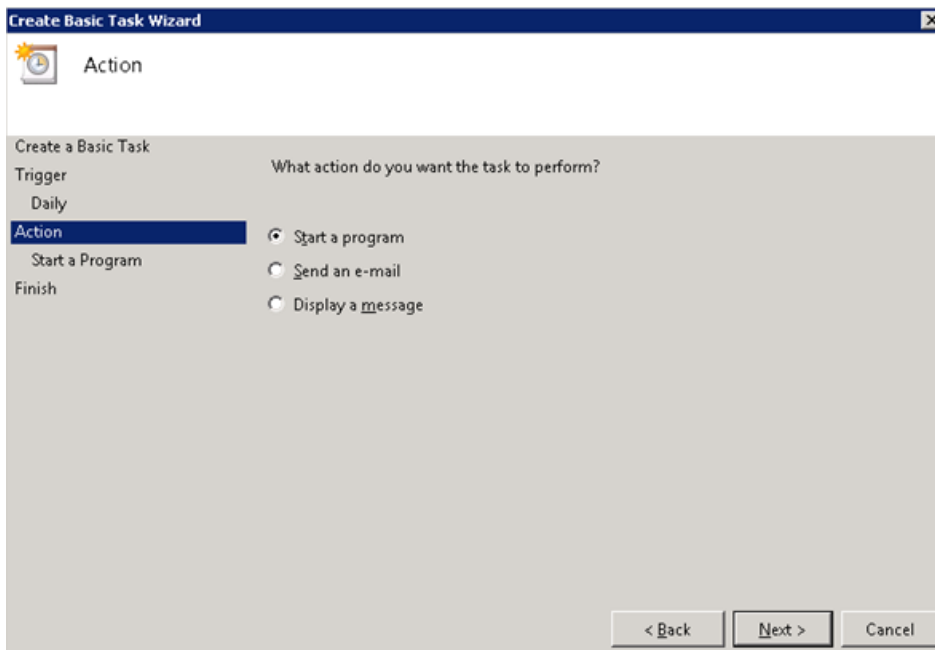
3. Select **Daily**, and then click **Next**.



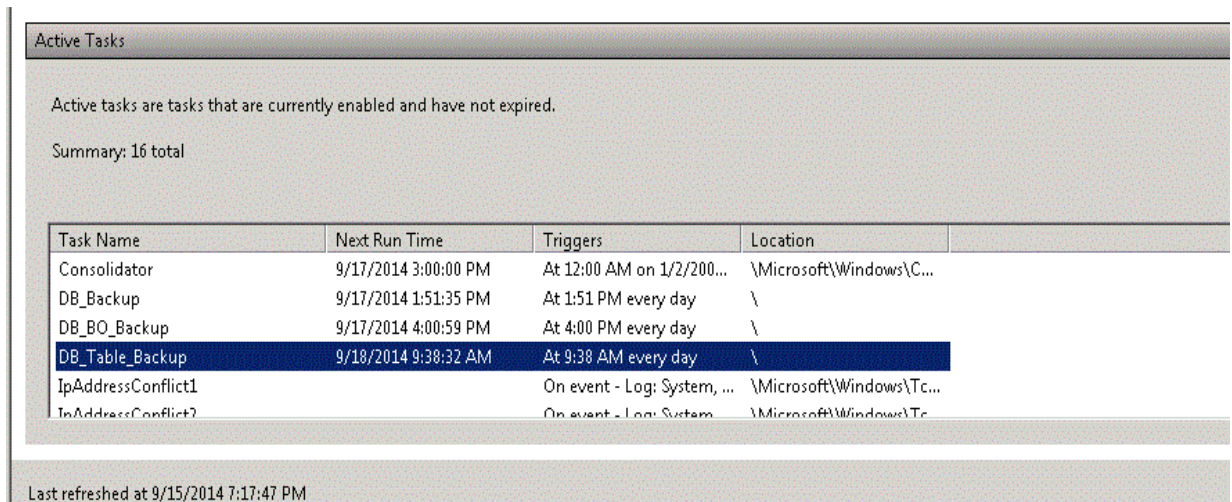
4. Select the start time, type 1 in the **Recur every** text box, and then click **Next**.



5. Select **Start a program**, and then click **Next**.



6. Browse to %PMDB_HOME%\DR, select **Execute_IncSncFullBackup_Script.bat**, and then click **Next**.
7. Click **Finish**. You can check the task created in the **Active Tasks** of the Task Scheduler window.



Task Name	Next Run Time	Triggers	Location
Consolidator	9/17/2014 3:00:00 PM	At 12:00 AM on 1/2/200...	\Microsoft\Windows\C...
DB_Backup	9/17/2014 1:51:35 PM	At 1:51 PM every day	\
DB_BO_Backup	9/17/2014 4:00:59 PM	At 4:00 PM every day	\
DB_Table_Backup	9/18/2014 9:38:32 AM	At 9:38 AM every day	\
IpAddressConflict1		On event - Log: System, ...	\Microsoft\Windows\Tc...
InAddressConflict2		On event - Log: System	\Microsoft\Windows\Tc...

Last refreshed at 9/15/2014 7:17:47 PM

For SAP BusinessObjects Database and File Store

The %PMDB_HOME%\DR\Execute_BO_FullBackup.bat script helps you take a backup of the SAP BusinessObjects database and file store. The same script will take the back up of the License, Configuration, CAC, and Custom files.

1. Create a folder where you want to store the backup files and date.
2. Browse to the %PMDB_HOME%\DR folder.

Note: If you have changed the SAP BusinessObjects database password, edit/replace pmdb_admin default password with the new password in the Execute_BO_FullBackup.bat file.

3. Run the following command:

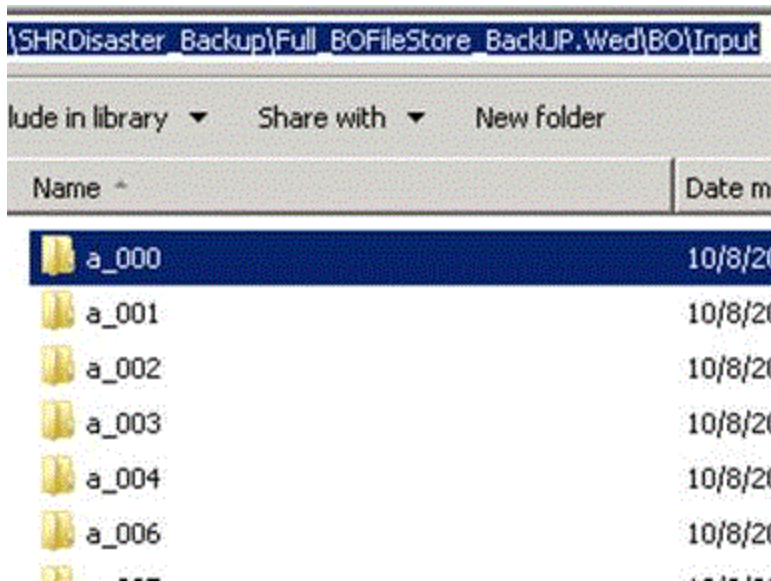
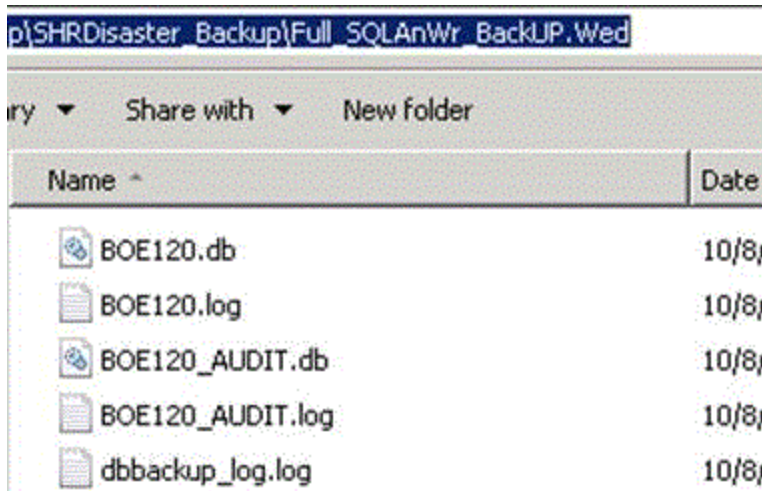
```
Execute_BO_FullBackup.bat <backup_path> <SAP_BusinessObjects_InstalledDrive>.
```

<backup_path> is the location where you want to store the backup files and data.

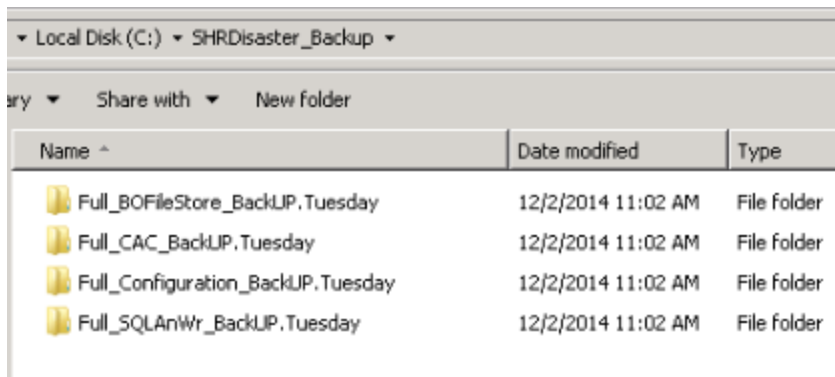
<SAP_BusinessObjects_InstalledDrive> is the drive where SAP BusinessObjects is installed.

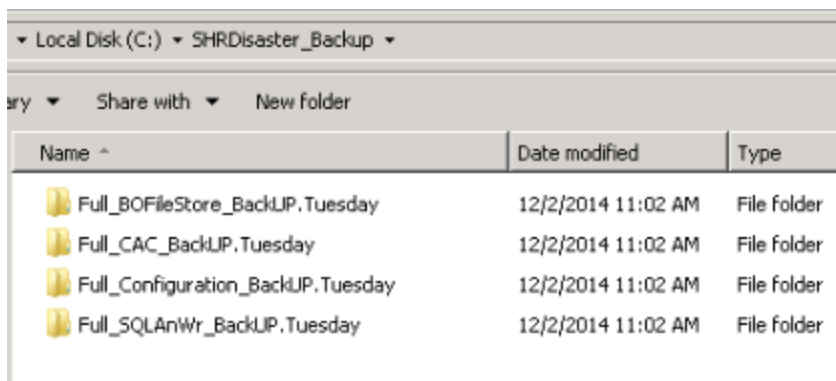
For Example: %PMDB_HOME%\DR> Execute_BO_FullBackup.bat C:\BO_backup C:\.

Following are the examples of the back up files of BusinessObjects database and File Store:



Following is the example of the backup files for License, Configuration, CAC, and Custom files:



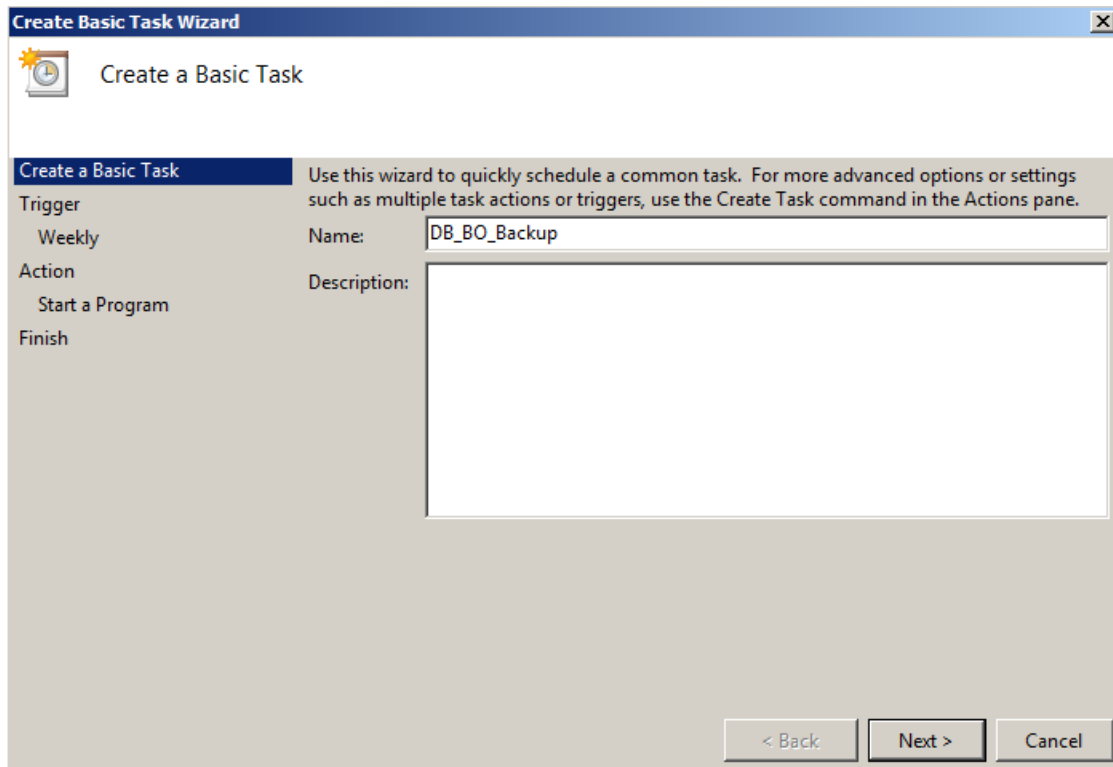


The script generates the following log files:

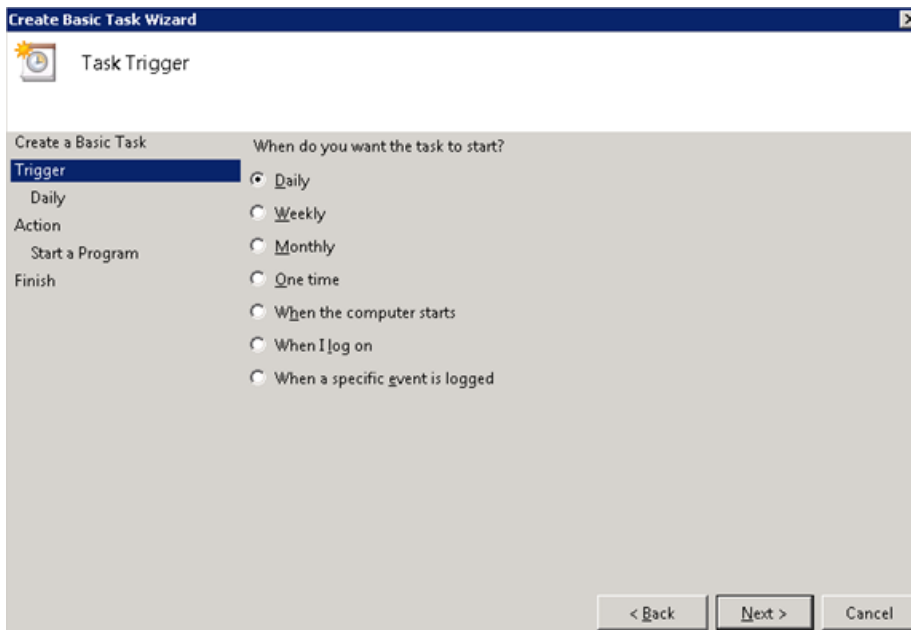
- **BO_Backup_log.log** - located at <bo_backup_path>\SHRDisaster_Backup\Full_BOFileStore_BackUP.<day of back up taken>
Example: <bo_backup_path>\SHRDisaster_Backup\Full_BOFileStore_BackUP.Wednesday
- **dbbackup_log.log** - located at <bo_backup_path>\SHRDisaster_Backup\Full_SQLAnWr_BackUP.<day of back up taken>
Example: <bo_backup_path>\SHRDisaster_Backup\Full_SQLAnWr_BackUP.Wednesday
- **Config_backup_log.log** - **Log files for License and Configuration files** located at <bo_backup_path>\SHRDisaster_Backup\Full_Configuration_BackUP.<day of back up taken>
Example: <bo_backup_path>\SHRDisaster_Backup\Full_Configuration_BackUP.Tuesday
- **customgroup_backup_log.log** - **Log files for all Custom group XML files** located at <bo_backup_path>\SHRDisaster_Backup\Full_Configuration_BackUP.<day of back up taken>
Example: <bo_backup_path>\SHRDisaster_Backup\Full_Configuration_BackUP.Tuesday
- **CAC_backup_log.log** - **Log files for CAC files** located at <bo_backup_path>\SHRDisaster_Backup\Full_CAC_BackUP.<day of back up taken>
Example: <bo_backup_path>\SHRDisaster_Backup\Full_CAC_BackUP.Tuesday

To schedule the backup, follow these steps:

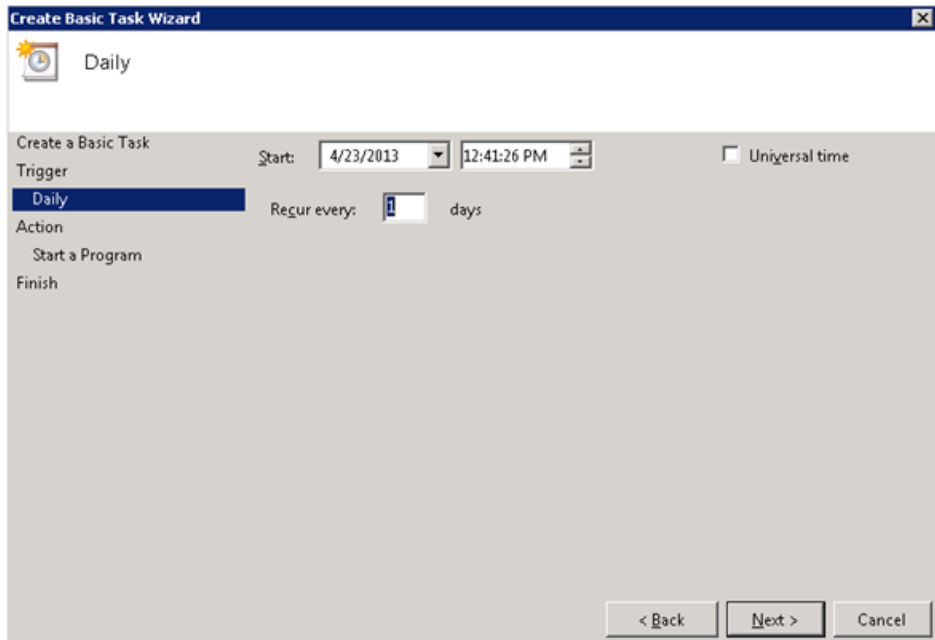
1. **On Windows 2008:** Go to **Start > Program > Administrative Tools > Task Scheduler**. The Task Scheduler window appears.
On Windows 2012: Go to **Start** and type **Task Scheduler** in **Search**. Double-click on the **Task Scheduler** to open it.
2. **On Windows 2008:** In the Task Scheduler window, right-click **Create Basic Task**. The Create Basic Task wizard opens. Type a name for the task, and then click **Next**.
On Windows 2012: In the **Task Scheduler** window, click **Create Basic Task**. The **Create Basic Task** wizard appears. Type a name for the task, and then click **Next**.



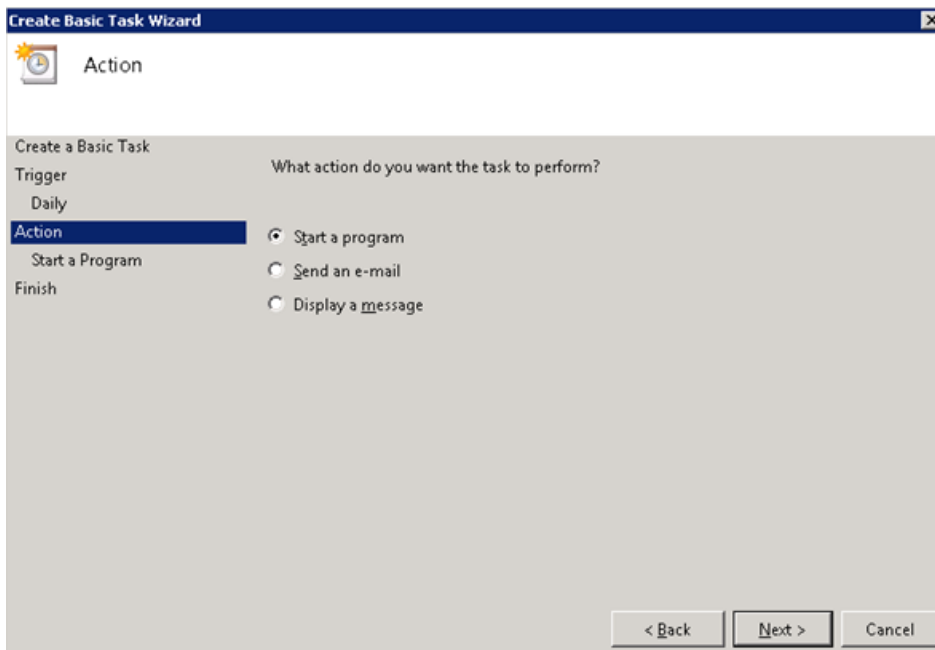
3. Select **Daily**, and then click **Next**.



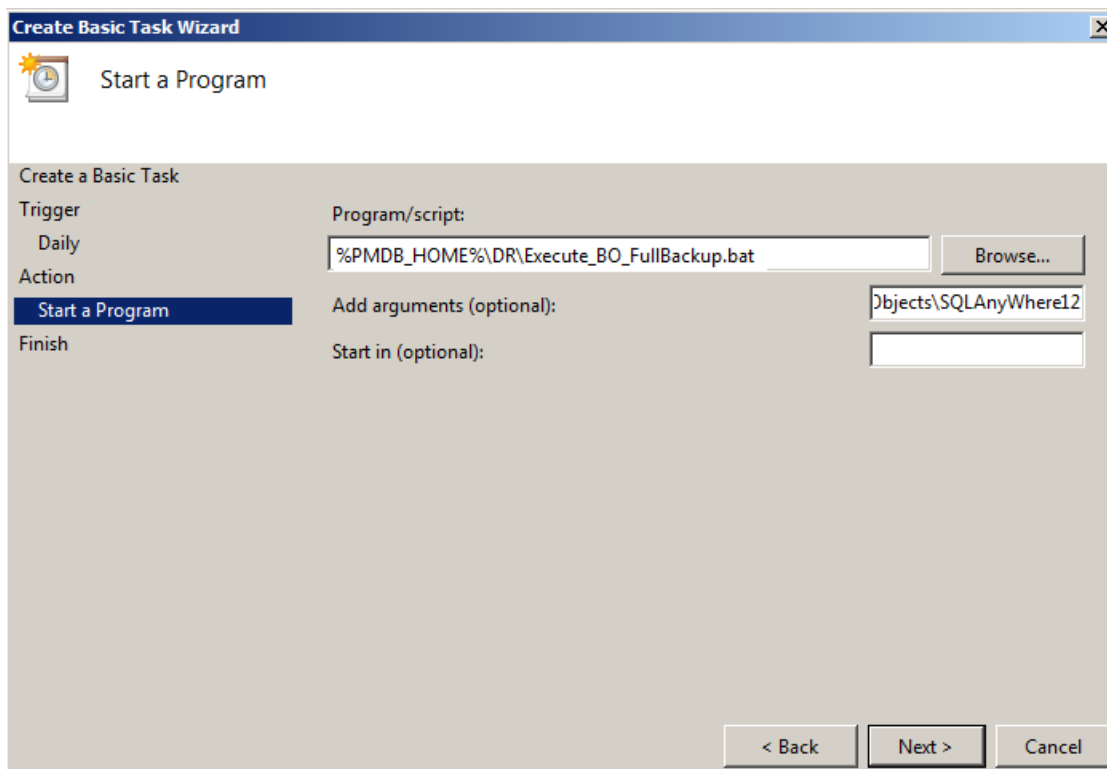
4. Select the start time, type 1 in the **Recur every** text box, and then click **Next**.



5. Select **Start a program**, and then click **Next**.



6. Browse to %PMDB_HOME%\DR, select **Execute_BO_FullBackup.bat**, and then click **Next**.



7. In the Add arguments field, type the following details:
<backup_path> <SAP_BusinessObjects_InstalledDrive>

Note: Include a space between two items.

In this instance:

- <backup_path> is the location where you want to store the backup files and data.
- <SAP_BusinessObjects_InstalledDrive> is the drive where SAP BusinessObjects is installed. By default, this is the C:\ drive. If a different drive was selected for SAP BusinessObjects during SHR installation, enter that drive.

Example: C:\BO_backup C:\

Note: If you want to backup the files to a custom folder, you must create it before starting the backup activity.

8. Click **Finish**. You can check the task created in the **Active Tasks** of the Task Scheduler window.

Task Name	Next Run Time	Triggers	Location
Consolidator	9/17/2014 3:00:00 PM	At 12:00 AM on 1/2/200...	\Microsoft\Windows\C...
DB_Backup	9/17/2014 1:51:35 PM	At 1:51 PM every day	\
DB_BO_Backup	9/17/2014 4:00:59 PM	At 4:00 PM every day	\
DB_Table_Backup	9/18/2014 9:38:32 AM	At 9:38 AM every day	\
IpAddressConflict1		On event - Log: System, ...	\Microsoft\Windows\Tc...
IpAddressConflict2		On event - Log: System, ...	\Microsoft\Windows\Tc...

Last refreshed at 9/15/2014 7:17:47 PM

For Management Database Table

Task 1: Edit the Backup Scripts

SHR provides the %PMDB_HOME%\scripts\MgmtDB\Postgres\backup_aggregate_control.sql and %PMDB_HOME%\DR\DB_tables_backup.bat scripts to back up the management database table. You must manually edit the backup_aggregate_control.sql script to specify the backup location. To edit the script, follow these steps:

1. Browse to the %PMDB_HOME%\scripts\MgmtDB\Postgres folder.
2. Open backup_aggregate_control.sql with a text editor.
3. Go to the following line:
`\copy dwabc.AGGREGATE_CONTROL TO 'E:\\bo_backup\\backup_AGGREGATE_CONTROL.dat'`
4. Replace E:\\bo_backup with the directory where you want to back up the data.

Tip: Type \\ instead of \, while specifying the directory path.

5. Save the file.
6. Run DB_tables_backup.bat from the location %PMDB_HOME%\DR.

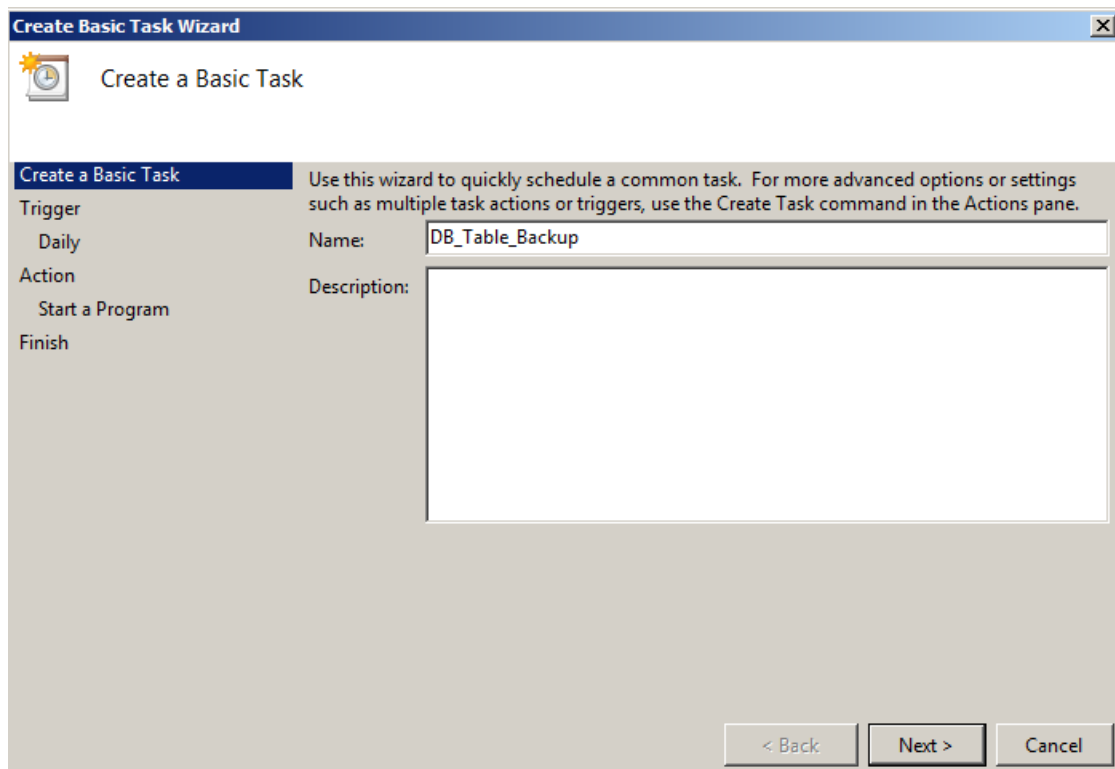
You can verify the database backup in backup.AGGREGATE_CONTROL.dat.

Task 2: Schedule to Run the Backup Script

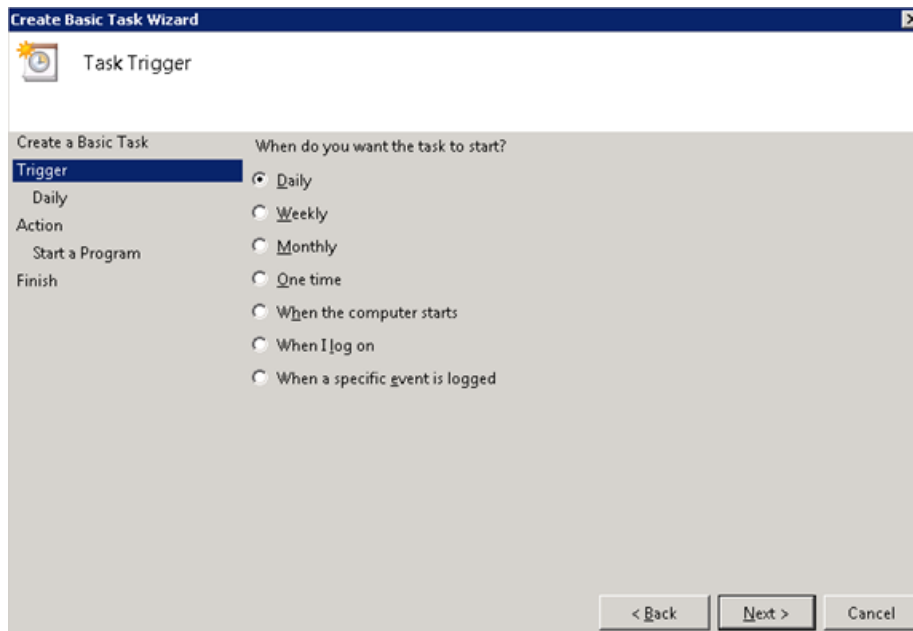
You must schedule to run the backup script once a day.

1. **On Windows 2008:** Go to **Start > Program > Administrative Tools > Task Scheduler**. The Task Scheduler window appears.
On Windows 2012: Go to **Start** and type **Task Scheduler** in **Search**. Double-click on the **Task Scheduler** to open it.
2. **On Windows 2008:** In the Task Scheduler window, right-click **Create Basic Task**. The Create Basic Task wizard opens. Type a name for the task, and then click **Next**.

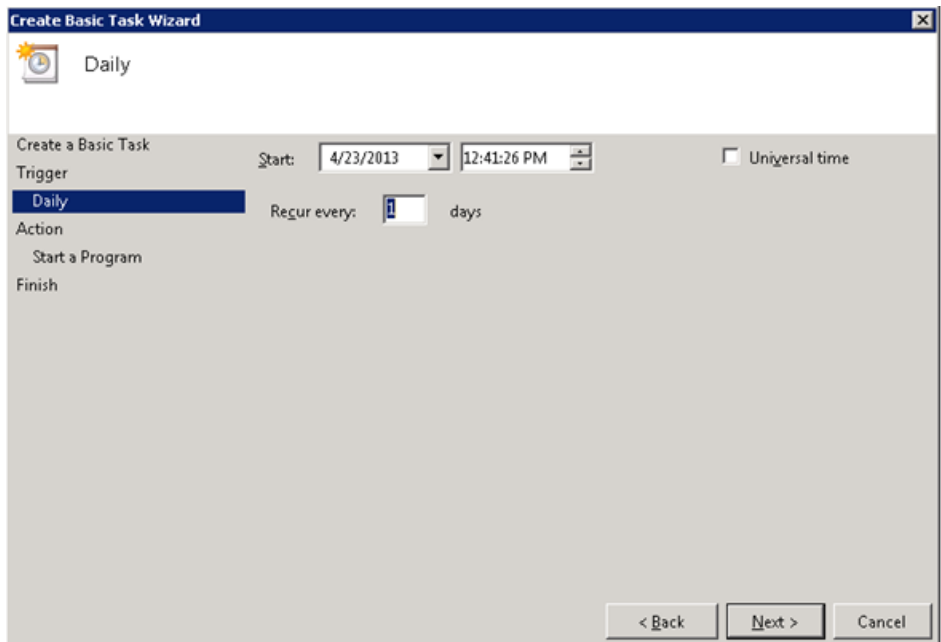
On Windows 2012: In the **Task Scheduler** window, click **Create Basic Task**. The **Create Basic Task** wizard appears. Type a name for the task, and then click **Next**.



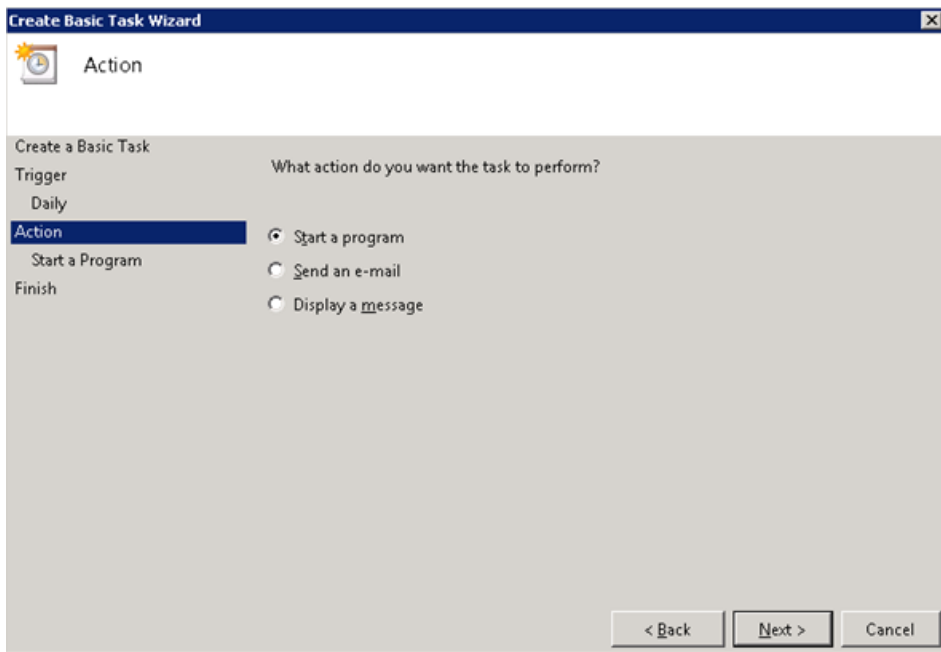
3. Select **Daily**, and then click **Next**.



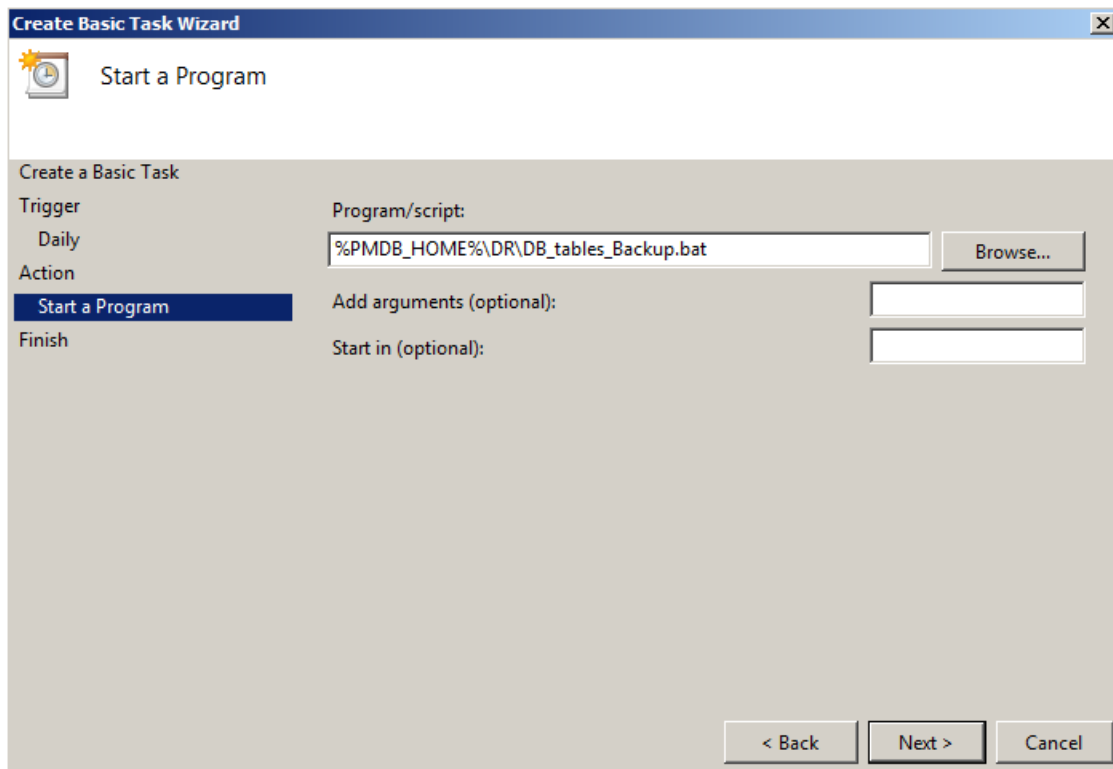
4. Select the start time, type 1 in the Recur every field, and then click **Next**.



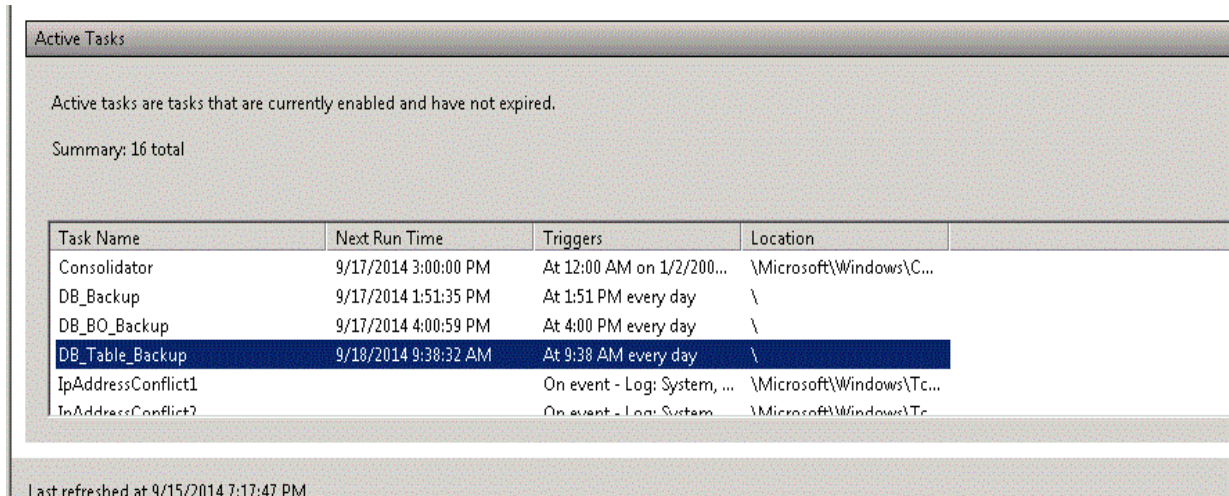
5. Select **Start a program**, and then click **Next**.



6. Browse to %PMDB_HOME%\DR, select **DB_tables_Backup.bat**, and then click **Next**.



7. Click **Finish**. You can check the task created in the **Active Tasks** of the Task Scheduler window.



Creating a Backup of SHR Databases on Linux

Note: In a Custom Installation scenario, perform the following steps on the systems where you have installed the SHR components.

For Sybase IQ Database

Tip: You must provide the path or location of the remote Sybase IQ database.

Task 1: Edit the Backup Scripts

SHR provides two backup scripts for full and incremental backup, respectively. Before you begin the backup, edit these scripts to fit the requirements.

These scripts are available in the \$PMDB_HOME/scripts/Sybase directory.

These scripts are:

- For Full Backup: IQ_backup_full.sql
- For Incremental Backup: IQ_backup_incr_since_full.sql

To edit the scripts, follow these steps:

1. Browse to the \$PMDB_HOME/scripts/Sybase directory.
2. Open IQ_backup_full.sql with a text editor application.
3. In the last parameter within the .sql script, create a directory where you want to save the backup files. That is, replace BACKUP with the actual location.

For example:

Default String	After Modifying
dsi_pmdb_backup 'FULL',NULL,'READWRITE_FILES_ ONLY',NULL,NULL,NULL,NULL,NULL,'D','BACKUP'	dsi_pmdb_backup 'FULL',NULL,'READWRITE_FILES_ ONLY',NULL,NULL,NULL,NULL,NULL,'D','/backup'

4. Similarly, in the incremental backup script (IQ_backup_incr_since_full.sql), replace the BACKUP string with the actual backup location.

For example:

Default String	After Modifying
dsi_pmdb_backup 'INCREMENTAL_SINCE_FULL',NULL,'READWRITE_FILES_ ONLY',NULL,NULL,NULL,NULL,NULL,'D','BACKUP'	dsi_pmdb_backup 'INCREMENTAL_SINCE_FULL',NULL,'READWRITE_FILES_ ONLY',NULL,NULL,NULL,NULL,NULL,'D','/backup'

Tip: For a remote Sybase IQ setup, the value of BACKUP parameter must be the path of the remote database server.

Run the .sql scripts using the following Shell scripts:

- Execute_FullBackup_Script.sh (Full Back up)
- Execute_IncSncFullBackup_Script.sh (Incremental Back up)

These Shell scripts are available in the `$PMDB_HOME/DR` directory.

After running these scripts, a database backup is created with file name suffixed with day of the Week at the specified location.

For Example:

Full backup

Full.tuesday.1 Full.tuesday.2

Incr backup

Incr_sncfull.tuesday.1

The scripts generate the following log files:

- Full Backup - `$PMDB_HOME/tmp/Execute_IQ_backup_full.out`
- Incremental Backup - `$PMDB_HOME/tmp/Execute_backup_incr_since_full.out`

Task 2: Edit the Copy Scripts

SHR provides a script for copying database files backup into a specific directory.

To edit the copy script, type the location where the backup of the database file exists and the location where you want to copy the copied files before starting the full backup procedure. You must run this script on the system where the Sybase IQ database is installed.

```
cp "location of existing full backup file" "copy to location"> $PMDB_HOME/tmp/Copy_Backup.txt 2>&1
```

Replace location of existing full backup file and copy to location with actual location details.

An example of the script:

```
cp /disk1/HP-SHR/Backup/Full* "/disk1/HP-SHR/Backup/Old/" > $PMDB_HOME/tmp/Copy_Backup.txt 2>&1
```

Task 3: Schedule the Backup

To take regular back up of the database, you must schedule to run the backup scripts by using the Linux CronJobs scheduler. It is recommended that you take a full back up once a week and an incremental back up once a day.

The Copy Backup script creates a copy of the full backup database files in the specified location to avoid overwriting an existing backup. You must schedule to run the Copy Backup script every time before you run the full backup script.

Follow these steps to set up a cronjob scheduler on Linux:

1. To edit your crontab file, type the following command at the Linux Terminal:
`crontab -e`
2. Schedule to run the copy backup script every day:
Type the following line in the crontab file.
`0 15 * * * /opt/HP/BSM/PMDB/DR/Copy_Backup.sh`
In the above example, the copy backup script is run every day at 15:00 Hours.
3. Schedule to run the full backup script once a week:

Type the following line in the crontab file.

```
0 15 * * 1 /opt/HP/BSM/PMDB/DR/Execute_FullBackup_Script.sh
```

In the above example, the full backup script is run on the first day of the week at 15:00 Hours.

4. Schedule to run the incremental backup script every day:

Type the following line in the crontab file.

```
0 15 * * * /opt/HP/BSM/PMDB/DR/Execute_IncSncFullBackup_Script.sh
```

In the above example, the incremental backup script is run every day at 15:00 Hours.

5. After adding the entries, save the crontab file.

All the log files for crontab are in the location /var/mail.

For SAP BusinessObjects Database and File Store

The \$PMDB_HOME/DR/Execute_BO_FullBackup.sh script helps you take a backup of the SAP BusinessObjects database and file store. The same script will take the back up of the License, Configuration, CAC, and Custom files.

1. Create a folder where you want to store the backup files and data.
2. Browse to the \$PMDB_HOME/DR folder.

Note: If you have changed the SAP BusinessObjects database password, edit/replace pmdb_admin default password with the new password in the Execute_BO_FullBackup.sh file.

3. Run Execute_BO_FullBackup.sh <backup_path>.

For Example: \$PMDB_HOME/DR> Execute_BO_FullBackup.sh/bo_backup.

Following are the examples for backup of BusinessObjects database and File Store:

```
[root@I111111111 bo_backup]# cd SHRDisaster_Backup/
[root@I111111111 SHRDisaster_Backup]# ls
Full_BOFileStore_BackUP.Wed Full_SQLAnWr_BackUP.Wed
[root@I111111111 SHRDisaster_Backup]# cd Full_BOFileStore_BackUP.Wed/
[root@I111111111 Full_BOFileStore_BackUP.Wed]# ls
BO_Backup_log.log frsinput frsoutput
[root@I111111111 Full_BOFileStore_BackUP.Wed]# cd frsinput/
[root@I111111111 frsinput]# ls
a_000 a_011 a_021 a_030 a_040 a_049 a_057 a_066 a_075 a_086 a_093 a_100 a_107 a_114 a_127 a_136 a_143 a_159 a_230 a_239 a_248
a_002 a_013 a_022 a_032 a_041 a_050 a_058 a_067 a_077 a_087 a_094 a_101 a_108 a_115 a_130 a_137 a_144 a_160 a_231 a_240 a_249
a_003 a_014 a_023 a_033 a_043 a_051 a_059 a_068 a_079 a_088 a_095 a_102 a_109 a_116 a_131 a_138 a_145 a_219 a_232 a_242 a_251
a_004 a_015 a_025 a_034 a_044 a_052 a_061 a_070 a_081 a_089 a_096 a_103 a_110 a_117 a_132 a_139 a_146 a_225 a_233 a_243 a_252
a_006 a_017 a_026 a_036 a_045 a_054 a_062 a_071 a_082 a_090 a_097 a_104 a_111 a_118 a_133 a_140 a_147 a_226 a_234 a_244 a_253
a_007 a_018 a_028 a_038 a_047 a_055 a_063 a_073 a_083 a_091 a_098 a_105 a_112 a_119 a_134 a_141 a_155 a_227 a_236 a_245 a_254
a_009 a_019 a_029 a_039 a_048 a_056 a_064 a_074 a_084 a_092 a_099 a_106 a_113 a_121 a_135 a_142 a_156 a_228 a_237 a_247 temp
```

```
[root@I111111111 SHRDisaster_Backup]# cd Full_SQLAnWr_BackUP.Wed/
[root@I111111111 Full_SQLAnWr_BackUP.Wed]# ls
dbbackup_log.log IWFVM01234BOE120_AUDIT.db IWFVM01234BOE120_AUDIT.log IWFVM01234BOE120.db IWFVM01234BOE120.log
```

Following is the example of the backup files for License, Configuration, CAC, and Custom files:

```
[root@iwfvm05326 SHRDisaster_Backup]# ls
Full_BOFileStore_BackUP.Tuesday Full_CAC_BackUP.Tuesday Full_Configuration_BackUP.Tuesday Full_SQLAnWr_BackUP.Tuesday
[root@iwfvm05326 SHRDisaster_Backup]#
```

The script generates the following log files:

- `BO_Backup_log.log` - located at `<bo_backup_path>/SHRDisaster_Backup/Full_BOFileStore_BackUP.<day of back up taken>`
Example: `<bo_backup_path>/SHRDisaster_Backup/Full_BOFileStore_BackUP.Wednesday`
- `dbbackup_log.log` - located at `<bo_backup_path>/SHRDisaster_Backup/Full_SQLAnWr_BackUP.<day of back up taken>`
Example: `<bo_backup_path>/SHRDisaster_Backup/Full_SQLAnWr_BackUP.Wednesday`
- `Config_backup_log.log` - Log files for License and Configuration files located at `<bo_backup_path>/SHRDisaster_Backup/Full_Configuration_BackUP.<day of back up taken>`
Example: `<bo_backup_path>/SHRDisaster_Backup/Full_Configuration_BackUP.Tuesday`
- `customgroup_backup_log.log` - Log files for all Custom group XML files located at `<bo_backup_path>/SHRDisaster_Backup/Full_Configuration_BackUP.<day of back up taken>`
Example: `<bo_backup_path>/SHRDisaster_Backup/Full_Configuration_BackUP.Tuesday`
- `CAC_Backup_log.log` - Log files for CAC files located at `<bo_backup_path>/SHRDisaster_Backup/Full_CAC_BackUP.<day of back up taken>`
Example: `<bo_backup_path>/SHRDisaster_Backup/Full_CAC_BackUP.Tuesday`

To schedule the back up, follow these steps:

1. Log on to the SHR system as root.
2. To edit your crontab file, type the following command at the command prompt:
`crontab -e`
3. Add a line to the crontab file to invoke the `/opt/HP/BSM/PMDB/DR/Execute_BO_FullBackup.sh` script once every week.

Example:

```
0 15 * * 1 /opt/HP/BSM/PMDB/DR/Execute_BO_FullBackup.sh /root/SHR_Backup
```

In the above example, the `/opt/HP/BSM/PMDB/DR/Execute_BO_FullBackup.sh` script is invoked on the first day of the week at 15:00 hours and the data file backup is stored at `/root/SHR_Backup`.

4. Save the crontab file.

All the log files for crontab are in the location `/var/mail`.

For Management Database Tables

The `DB_Tables_Backup.sh` script enables you to backup the management database tables. Before you schedule to run the script, you must modify the `backup_aggregate_control.sql` script, which is used by `DB_Tables_Backup.sh`.

Task 1: Edit the `backup_aggregate_control.sql` Script

1. Open the `backup_aggregate_control.sql` script from the `$PMDB_HOME/scripts/MgmtDB/Postgres` directory with a text editor.
2. Locate the following line:


```
\copy dwabc.AGGREGATE_CONTROL TO '/opt//bo_backup//backup_AGGREGATE_
CONTROL.dat'
```

3. Replace `/opt//bo_backup` with the directory where you want to back up the data.

Tip: Type `//` instead of `/`, while specifying the directory path.

4. Save the file.
5. Run `DB_tables_backup.sh` from the location `$PMDB_HOME/DR`

You can verify the database backup in `backup.AGGREGATE_CONTROL.dat`.

Task 2: Schedule to Run DB_Tables_Backup.sh the Script

1. Log on to the SHR system as root.
2. To edit your crontab file, type the following command at the command prompt:
`crontab -e`
3. Add a line to the crontab file to invoke the `/opt/HP/BSM/PMDB/DR/DB_tables_backup.sh` script once every day.

Example:

```
0 15 * * * /opt/HP/BSM/PMDB/DR/DB_tables_backup.sh
```

In the above example, the `/opt/HP/BSM/PMDB/DR/DB_tables_backup.sh` script is invoked on the at 15:00 hours everyday.

4. Save the crontab file.

All the log files for crontab are in the location `/var/mail`.

Restoring SHR Databases

Before restoring the backup of data, you must install SHR on the system using the media. After the installation is complete, you must transfer all backup data into a local directory of the system.

Note: In a Custom Installation scenario, perform the following steps on the systems where you have installed the SHR components.

Restoring SHR on Windows

For Sybase IQ Database

1. Stop the `HP_PMDB_Platform_Sybase` service by following these steps:
 - a. Click **Start > Run**. The Run dialog box opens.
 - b. Type `services.msc` in the **Open** field, and then press **ENTER**. The Services window opens.
 - c. On the right pane, right-click the `HP_PMDB_Platform_Sybase` service, and then click **Stop**.
 - d. From the Windows Task Manager, select the **Processes** tab, look for `iqsrsv15.exe`, right-click it and select **End Process**.

2. Search for all files with extensions `.db`, `.log`, and `.iq` from the database file location and move these files to any other location on the system. These files are recreated by the restore process.
3. Start Sybase IQ server. At the command prompt run the following command:

```
start_iq @%PMDB_HOME%\config\pmdbConfig.cfg
```

Type the command in a single line.
4. To connect to Sybase IQ server, follow these steps:
 - a. On the SHR system, click **Start > Run**. The Run dialog box opens.
 - b. Type `dbisql` in the Open field and press **ENTER**. The **Connect** dialog box on Interactive SQL program opens.
 - c. Type the following:
 - In the User ID field, type `dba`
 - In the Password field, type `sql`
 - In **Action** select **Connect to a running database on this computer** from the drop down.
 - In the Server Name field, type the name of the server where the SHR Sybase IQ database is installed.

Tip: The server name can be found in `pmdbConfig.cfg` file. Open the file. The server name is the text succeeding `-n`.

- In the Database name field, type `utility_db`.
 - d. Click **Connect**. The Interactive SQL window opens.
5. Restore the Full Backup.
 - On the SQL Statements box type the following sql statement:

```
RESTORE DATABASE <location where database files were present>FROM <location where the backup file is saved>
```


For example: `RESTORE DATABASE 'E:\SybaseDB\pmdb.db' FROM 'E:\HP-SHR\backup\Full.Sunday'`


- Press **F9** or **Execute all SQL Statement(s)** to execute the sql statement.
- Check if the database files are restored to the previous database file location.

For Example: `pmdb_user_main01.iq`, `pmdb.db`, `pmdb.iq`, `pmdb.iqtmp`.

Tip: If you get the following error while restoring the Sybase database, ignore and continue with the restore process.

"Unable to start specified database: Illegal character in database alias."

- To stop the Sybase IQ server, follow these steps:
 - Go to Notifications in the Task bar and search for the Sybase IQ icon .
 - Right-click on the icon and select **Shut down <server name>**.
 - Click **Yes**.

- From the Services window, select **HP_PMDB_Platform_Sybase** service and click **Start**.
6. Restore the Incremental Backup, if any, after restoring a Full Backup.
- If several incremental backup files are available, select and restore the latest incremental backup. For example, if the database fails on a Thursday and a Full Backup had been taken on the previous Sunday, you must restore the Full Backup files of Sunday followed by the Incremental Backup taken on the previous Wednesday.
- To restore the Incremental Backup on the SQL Statements box type the following sql statement:
- ```
RESTORE DATABASE <location where database files were present>FROM <location where the incremental backup file is saved>
```
- For example: RESTORE DATABASE 'E:\SybaseDB\pmdb.db' FROM 'E:\HP-SHR\backup\Incr\_sncfull.Wednesday'
- Press F9 or **Execute all SQL Statement(s)** to execute the sql statement.
  - Check if the database files are restored to the previous database file location.
- For Example: pmdb\_user\_main01.iq, pmdb.db, pmdb.iq, pmdb.iqtmp.
- To stop the Sybase IQ server, follow these steps:
    - Go to Notifications in the Task bar and search for the Sybase IQ icon .
    - Right-click on the icon and select **Shut down <server name>**.
    - Click **Yes**.
  - From the Services window, select **HP\_PMDB\_Platform\_Sybase** service and click **Start**.

## For SAP BusinessObjects Database and File Store

To restore the SAP BusinessObjects database and file store, follow these steps:

1. Log on to the SHR system and open SAP BusinessObjects Central Configuration Manager.
  2. Stop the Server Intelligence Agent and BusinessObjects web server.
  3. From the **Services** window, click the **BOE120SQLAW** service and click **Stop**.
  4. Rename the existing file store folder. The default location of the file store is C:\Program Files (x86)\Business Objects\BusinessObjects Enterprise 12.0\FileStore.  
You can rename it to FileStore\_old.
  5. Run the restore script from the location %pmdb\_home%\DR:  
Execute\_BO\_FullRestore.bat <BO Full Backup FileStore Path> <BO Full Backup SQL AnWr Backup file path> <BO Drive>
- In this instance:
- *Execute\_BO\_FullRestore.bat* is located in %pmdb\_home%\DR.

**For Example:** E:\HP-SHR\PMDB\DR>Execute\_BO\_FullRestore.bat "E:\BO\_backup\SHRDisaster\_Backup\Full\_BOFileStore\_BackUP.Friday" "E:\BO\_backup\SHRDisaster\_Backup\Full\_SQLAnWr\_BackUP.Friday" E:

The same script will restore the backup of the License, Configuration, CAC, and Custom files.

Following are the log files located at %pmdb\_home%\log:

- SQLAnWr\_Restore.log
- BO\_Restore.log
- Config\_Restore.log - Log files for License, Configuration files and Custom XML files.
- CAC\_Restore.log - Log for CAC files.

6. Delete the original SAP BusinessObjects server:

- Go to the SQL Anywhere home directory. The default location is <SAP\_BusinessObjects\_Install\_Drive>\Program Files (x86)\Business Objects\SQLAnywhere12\bin.
- Double-click the dbisqlc file. The Connect to SQL Anywhere window appears.
- In the Connect to SQL Anywhere window, type the following details:
  - User ID: Type the hostname of the SHR system (not FQDN).

**Note:** If you are performing this step for SHR Migration to a Windows 2012 operating system, type the short name of System 1.

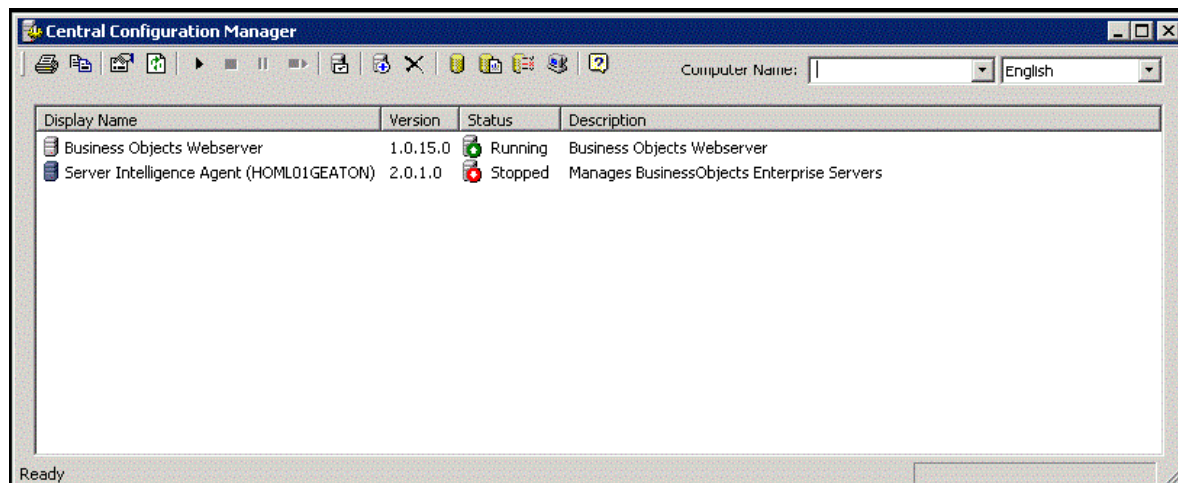
- Password: Type <password> (pmdb\_admin is the default password if the SAP BusinessObjects database password is not changed).
  - Select **Start and connect to the running database on this computer** from the drop down.
  - Select the **Database file** location by clicking **Browse** button.  
The default database file location is C:\Program Files (x86)\Business Objects\SQLAnywhere12\bin\BOE120.db.
  - Leave the Database Name field blank.
  - Server name: BOE120SQLAW\_<SHR\_hostname>
  - Select **Stop database after last disconnect**.  
Do not change any other settings.
  - Click **OK**. The SQL Anywhere console opens.
- In the command pane, type the following query:  
delete from cms\_infoobjects6 where parentid=16 or parentid=59;
  - Click **Execute**. You will get a message that displays the number of records deleted.
  - Close the Connect to SQL Anywhere window.

7. Create a new Server Intelligent Agent:

- On Windows 2008:** From the **Start** menu, click **Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Configuration Manager**. The Central Configuration Manager window opens.

**On Windows 2012:** Go to Start and type Central Configuration Manager in Search. Double-click on the Central Configuration Manager to open it.

- b. In the **Central Configuration Manager** window, note down the name of the Server Intelligence Agent (displayed within parenthesis).



- c. Go to `<SAP_BusinessObjects_Install_Directory>\BusinessObjects Enterprise 12.0\win32_x86`.

The default SAP BusinessObjects installation directory is `C:\Program Files (x86)\Business Objects\BusinessObjects Enterprise 12.0`.


- d. Delete all files that start with **\_boe**.  
e. Delete the Server Intelligence Agent by running the following command:

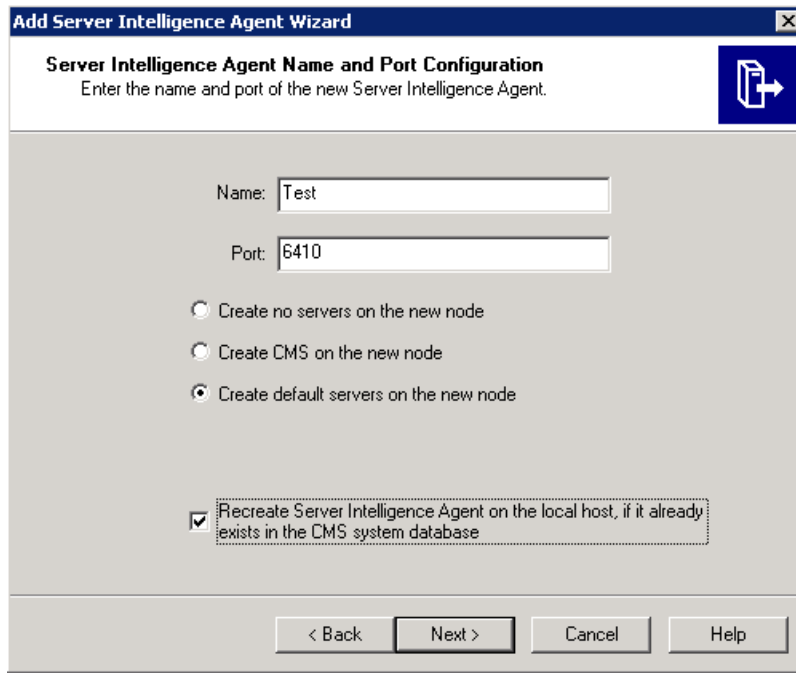
```
sc delete BOE120SIA<name>
```

In this instance, `<name>` is the name of the Sever Intelligence Agent that you noted down earlier.

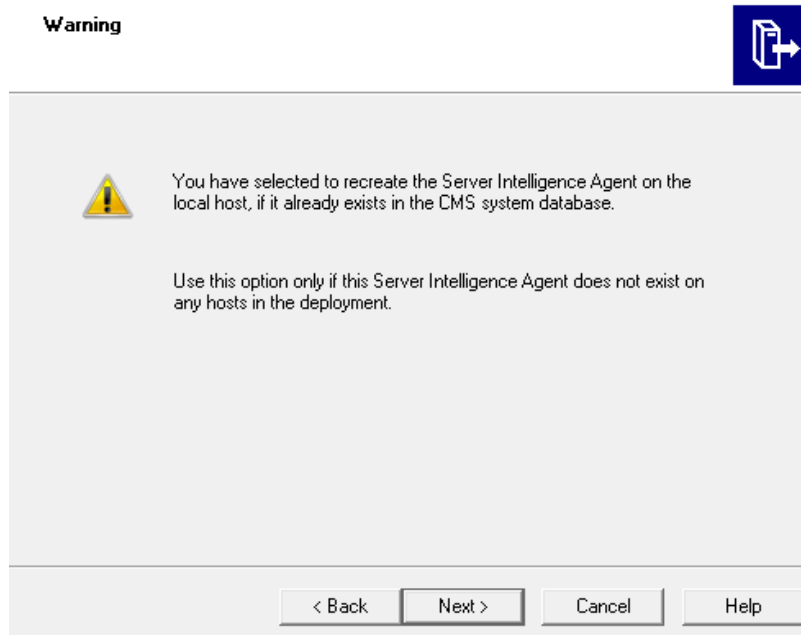
The following message appears in the command line console:

```
[SC] DeleteService SUCCESS
```

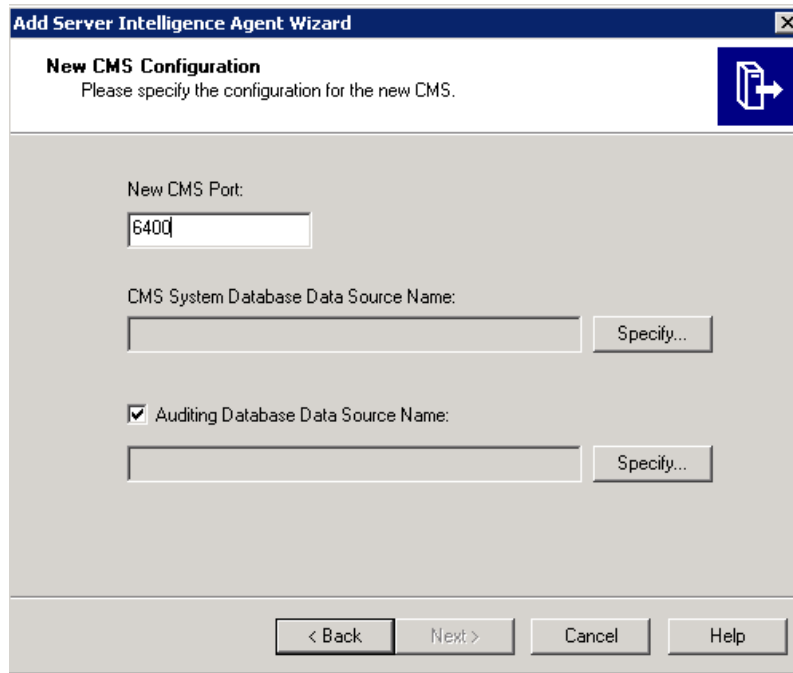
- f. Click **Refresh** in the **Central Configuration Manager** window and verify if the Server Intelligence Agent is deleted.  
g. From the **Services** window, click the **BOE120SQLAW** service and click **Start**.  
h. In the Central Configuration Manager window, right-click and stop BusinessObjects Webserver if it is in running state.  
i. Click **Add Server Intelligent Agent** (  ). The Add Server Intelligence Agent wizard opens.  
j. In the Add Server Intelligence Agent wizard, type a name for the Server Intelligence Agent and **6410** for port, select the **Create default servers on the new node** option, select the **Recreate Server Intelligence Agent ...** check box, and then click **Next**.



A warning may appear, you can click **Next** and the New CMS Configuration page is displayed.



- k. In the New CMS Configuration page, type **6400** in **New CMS Port** text box.



- l. In the **CMS System Database Data Source Name**, click **Specify**. The Select Database Driver dialog box opens.
- m. In the Select Database Driver dialog box, select **SQL Anywhere (ODBC)**, and then click **OK**. The Select Data Source window opens.
- n. In the Select Data Source window, go to Machine Data Source, select **BOE120**, and then click **OK**.
- o. In the Connect to SQL Anywhere window, type the host name of the SHR system as the user ID, type the SQL Anywhere database password (`pmdb_admin` is the default password if the SAP BusinessObjects database password is not changed), and then click **OK**. Do not change any other settings. Do not select **Encrypt Password**.

**Note:** If you are performing this step for SHR Migration to a Windows 2012 operating system, type the short name of System 1 as the user ID.

- p. Enable auditing:
  - o Under the Auditing Database Data Source Name check box, click **Specify**. The Create Database Driver dialog box opens.
  - o In the Create Database Driver dialog box, select **SQL Anywhere (ODBC)**, and then click **OK**. The Select Data Source window opens.
  - o In the Select Data Source window, go to Machine Data Source, select **BOE120\_AUDIT**, and then click **OK**.
  - o In the Connect to SQL Anywhere window, type the host name of the SHR system as the user ID, type the SQL Anywhere database password (`pmdb_admin` is the default password if the SAP BusinessObjects database password is not changed), and then click **OK**. Do not change any other settings. Do not select **Encrypt Password**.

**Note:** If you are performing this step for SHR Migration to a Windows 2012 operating system, type the short name of System 1 as the user ID.

- q. Click **Next**.

**Note:** Ensure that for the Administrator (default user) the password must be same as the primary setup.

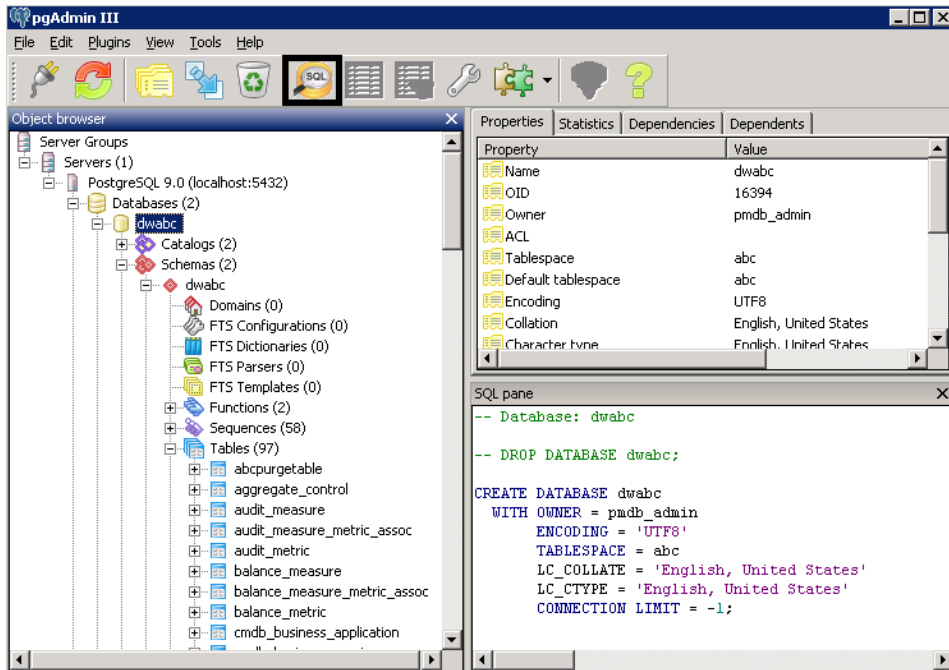
- r. Click **Next**.
- s. Click **Finish**. A new Server Intelligence Agent is created.  
Example: If the Server Intelligence Agent is created with the name *test* the display name will be *Server Intelligence Agent (test)*.
- t. Double-click Server Intelligence Agent, in the **Server Intelligence Agent (test) Properties** window select **Dependency**.
- u. Click **Add**. The **Add Dependency window** appears.
- v. Select **BOE120SQLAW** from the list and click **Add**, then click **OK**.
- w. Start the Server Intelligence Agent and the BusinessObjects Webserver.
8. After starting the services, follow these steps:
- Launch Central Management Console (CMC).
  - Log in to CMC with administrator account.
  - Click on Servers.
  - Double-click on **InputFileRepository** server.
  - In Context menu click on **Properties**.
  - Type the path in **Temporary Directory**. (For Example: <installation directory of BOE>:\Program Files (x86)\Business Objects\BusinessObjects Enterprise 12.0\FileStore\Input\temp)
  - Type the path in **File Store Directory**. (For Example: <installation directory of BOE>:\Program Files (x86)\Business Objects\BusinessObjects Enterprise12.0\FileStore\BO\Input).
  - Click on **Save & Close**.
  - Restart the **InputFileRepository** server.
  - Perform the following steps for **OutputFileRepository** server.
    - Double-click on **OutputFileRepository** server.
    - In Context menu click on **Properties**.
    - Type the path in **Temporary Directory**. (For Example: <installation directory of BOE>:\Program Files (x86)\Business Objects\BusinessObjects Enterprise12.0\FileStore\Output\temp)
    - Type the path in **File Store Directory**. (For Example: <installation directory of BOE>:\Program Files (x86)\Business Objects\BusinessObjects Enterprise12.0\FileStore\BO\Output).
    - Click on **Save & Close**.
    - Restart the **OutputFileRepository** server.



## For Management Database Table

To restore the management database table, follow these steps:

1. Log on to the SHR system.
2. **On Windows 2008:** From the Start menu, go to **Programs > PostgreSQL 9.0 > pgAdmin III**.  
**On Windows 2012:** Go to **Start** and type **pgAdmin III** in **Search**. Double-click on the pgAdmin III to open it.
3. Connect to the database by providing the password `PMDB92_admin@hp`. Launch the sql query analyzer by clicking the sql icon.



4. Run the following query to restore the database tables:

```
Delete From dwabc.aggregate_control
```

```
COPY dwabc.aggregate_control from '<Path of the backupfile>\\backup_AGGREGATE_
CONTROL.dat'
```

In this instance, *<Path of the backupfile>* is the directory where you placed the backup of management database table.

For Example: `COPY dwabc.aggregate_control from 'E:\\bo_backup\\backup_AGGREGATE_
CONTROL.dat'`

## Restoring SHR on Linux

**Note:** In a Custom Installation scenario, perform the following steps on the systems where you have installed the SHR components.

## For Sybase IQ Database

**Note:** Ensure sufficient space is available in the disk before performing the restore.

To restore the Sybase database, follow these steps:

1. Stop the HP\_PMDB\_Platform\_Sybase service:
  - `cd /etc/init.d`
  - `service HP_PMDB_Platform_Sybase stop`
2. Run this command:  
`ps -ef|grep iqsrv15`  
Note the process ID displayed by the command output.
3. Run this command by entering the process ID in `<pid>`: `kill -9 <pid>`
4. Search for all files with extensions `.db`, `.log`, and `.iq` from the database file location and move those files to any other location on the system. Those files are recreated by the restore process.
5. Start the Sybase IQ server. At the command prompt, run the following command in a single line:

```
start_iq @/opt/HP/BSM/PMDB/config/pmdbConfig.cfg
```

6. Connect to Sybase IQ server:

```
dbisql -nogui -c "uid=dba;pwd=sql;dbn=utility_db;eng=<server_name>;commlinks=tcPIP(host=<host_name>;port=21424)"
```

Example:

```
dbisql -nogui -c "uid=dba;pwd=sql;dbn=utility_db;eng=abc;commlinks=tcPIP(host=abc.com;port=21424)."
```

7. Restore the Full Backup on the same path/drive:

On the SQL Statements box, type the following SQL statement:

```
RESTORE DATABASE <location where database files were present> FROM <location where the backup file is saved>
```

For example:

```
RESTORE DATABASE '/root/SHR_Sybase/pmdb.db' FROM
'/root/HPSHR/backup/Full.Sunday'
```

**Tip:** If you notice the following error while restoring the Sybase database, ignore the error and continue with the restore process.

*"Unable to start specified database: Illegal character in database alias."*

8. Run the following command to restore the database on a different path/drive:

```
RESTORE DATABASE <location where database files were present> FROM <location where the backup file is saved>
```

```
RENAME IQ_SYSTEM_MAIN TO <path to pmdb.iq>
```

```
RENAME IQ_SYSTEM_TEMP TO <path to pmdb.iqtmp>
```

```
RENAME pmdb_user_main TO <path to pmdb_user_main01.iq>
```

Make sure the path to pmdb.db exists.

Run all the above commands together.

9. Restore the Incremental Backup, if any, after restoring a Full Backup.

If several incremental backup files are available, select and restore the latest incremental Backup.

To restore the Incremental Backup on the same path/drive in the SQL Statements box, type the following SQL statement:

```
RESTORE DATABASE<location where database files were present>FROM<location where
the incremental backup file is saved>
```

```
RENAME IQ_SYSTEM_MAIN TO <path to pmdb.iq>
```

```
RENAME IQ_SYSTEM_TEMP TO <path to pmdb.iqtmp>
```

```
RENAME pmdb_user_main TO <path to pmdb_user_main01.iq>
```

10. Stop and start the Sybase services:

- service HP\_PMDB\_Platform\_Sybase stop
- service HP\_PMDB\_Platform\_Sybase start

## For SAP BusinessObjects Database and File Store

To restore the SAP BusinessObjects database and file store follow these steps:

1. Copy the backup of SAP BusinessObjects database and file store on a system where SAP BusinessObjects is installed. The backup also includes the back up files of License, Configuration, CAC and Custom files.

2. Log on to the system as root.

3. Run the following command to stop the web server:

```
sh /opt/HP/BSM/BO/bobje/tomcatshutdown.sh
```

4. Switch to the SAP BusinessObjects administrator by running the following command:

```
su - SHRBOADMIN
```

5. Run the following command to stop all Server Intelligence Agent servers:

```
sh /opt/HP/BSM/BO/bobje/stopservers
```

6. Stop the SQL Anywhere service:

```
sh /opt/HP/BSM/BO/bobje/sawstop.sh
```

While prompted for password, specify the SQL Anywhere database password.

7. Take a backup of all SQL Anywhere Data Base files by running the following command:

```
cp /opt/HP/BSM/BO/bobje/SQLAW/Bin/*BOE120* <backup_path>
```

In this instance, <backup\_path> is the directory where you want to back up the existing SQL Anywhere database files.

8. Rename the existing frsoutput and frsinput files store folders. The default location of the file store is /opt/HP/BSM/BO/bobje/data.

Also, note down the rights granted to the users for these two folders.

9. Switch to root by running the following command:

```
su root
```

10. Copy the backup of SAP BusinessObjects database file (that you have taken a backup in "[For SAP BusinessObjects Database and File Store](#)" on page 159) perform the following:

```
cd /opt/HP/BSM/BO/bobje/SQLAW/Bin
```

```
cp <bo_backup_path>/SHRDisaster_Backup/Full_SQLAnWr_BackUP.Wednesday/*BOE120* .
```

**Note:** You must ensure that you type \*BOE120\* . with a space and (.).

Type *y* to overwrite the existing files.

11. Run the following commands to grant adequate rights to the SAP BusinessObjects user:

```
chown SHRBOADMIN:root *BOE120*
```

```
chmod 755 *BOE120*
```

12. Ensure that you log in as SHRBOADMIN user and not root.

```
su - SHRBOADMIN
```

13. Start the SQL Anywhere service. Execute the following command to start SQL Anywhere.

```
sh $PMDB_HOME/./BO/bobje/sawstartup.sh
```

You will see the following message:

```
STARTING SQL AnyWhere12 SERVER
```

```
SQL Anywhere Start Server In Background Utility Version 12.0.1.3457
```

14. Create a new Server Intelligence Agent by running the following command:

```
sh /opt/HP/BSM/BO/bobje/serverconfig.sh
```

The SAP BusinessObjects wizard opens in the command line console.

15. Type 1, and then press **Enter**.

```

SAP BusinessObjects
What would you like to do?
1 - Add a Server Intelligence Agent
2 - Delete a Server Intelligence Agent
3 - Modify a Server Intelligence Agent
4 - List all Server Intelligence Agents in the config file

[quit (0)]

[4]1
```

16. Type 3, and then press **Enter**.

```

SAP BusinessObjects

If it already exists in the CMS system database, do you want to recreate the
Server Intelligence Agent on the local host?

Use this option only if this Server Intelligence Agent does not exist on any hosts in the deployment.

[yes (3)/no (2)/back(1)/quit (0)]

[no]3
```

17. Specify a name for the agent (as a best practice, type the hostname of the system as the name of the agent), and then press **Enter**.

```

SAP BusinessObjects

Please enter the name of the new Server Intelligence Agent.

[back(1)/quit (0)]

[SHRLR02]SHRM2
```

18. Type 6400 as the port number, and then press **Enter**.

```

SAP BusinessObjects

Please enter the port of the new Server Intelligence Agent.

[back(1)/quit (0)]

[] 6410
```

19. Type 2 (default server), and then press **Enter**.

```

SAP BusinessObjects

noservers (Create no servers on the new node)
cms (Create CMS on the new node)
defaultservers (Create default servers on the new node)

[noservers (4) / cms (3) / defaultservers (2) / back (1) / quit (0)]

[noservers]2
```

20. Type 6400 as the port number, and then press **Enter**.

```

SAP BusinessObjects

Enter the port of the new CMS.

[back (1) / quit (0)]

[default (6400)]
```

21. Type 2 (SQL Anywhere), and then press **Enter**.

```

SAP BusinessObjects

Specify Destination CMS database connection information.

Select the type of database connection from the following:
[Oracle (6) / DB2 (5) / Sybase (4) / MySQL (3) / SQL Anywhere (2) / back (1) / quit (0)]

[Oracle]2
```

22. Press **Enter** (the correct server is selected by default).

```

SAP BusinessObjects

Specify Destination CMS database connection information.

Enter the ODBC data source name (DSN) for connecting to your SQL Anywhere database.

[back(1)/quit(0)]

[SHRLR02BOE120]
```

23. Press **Enter** (the correct user name is selected by default).

```

SAP BusinessObjects

Specify Destination CMS database connection information.

Enter the user name for connecting to your SQL Anywhere database.

[back(1)/quit(0)]

[SHR]
```

24. Type a password (note down for future reference), and then press **Enter**.

```

SAP BusinessObjects

Specify Destination CMS database connection information.

Enter the password for connecting to your SQL Anywhere database.

[back(1)/quit(0)]

[]
```

25. Select **Yes**, and then press **Enter**.

```

SAP BusinessObjects

Would you like to enable auditing?

[yes (3) /no (2) /back (1) /quit (0)]

[yes] █
```

26. Type 2 (SQL Anywhere), and then press **Enter**.

```

SAP BusinessObjects

Specify auditing database connection information.

Select the type of database connection from the following:
[Oracle (6) /DB2 (5) /Sybase (4) /MySQL (3) /SQL Anywhere (2) /back (1) /quit (0)]

[SQL Anywhere]2 █
```

27. Type the ODBC data source name, and then press **Enter**.

The data source name is of the following format:

<agent\_name>**BOE120\_Audit**

<agent\_name> is the name that you selected in step 14.

```

SAP BusinessObjects

Specify auditing database connection information.

Enter the ODBC data source name (DSN) for connecting to your SQL Anywhere database.

[back (1) /quit (0)]

[SHRLR02BOE120]SHRLR02BOE120_AUDIT █
```



28. Press **Enter** (the correct user name is selected by default).

```

SAP BusinessObjects

Specify auditing database connection information.

Enter the user name for connecting to your SQL Anywhere database.

[back(1)/quit(0)]

[SHR] █
```

29. Type a password (note down for future reference), and then press **Enter**.

```

SAP BusinessObjects

Specify auditing database connection information.

Enter the password for connecting to your SQL Anywhere database.

[back(1)/quit(0)]

[] █
```

30. Press **Enter**. The correct user (Administrator) is selected by default.

```

SAP BusinessObjects

Enter the user name to connect to this CMS.

[back(1)/quit(0)]

[Administrator] █
```

31. Press **Enter** when prompted for password.  
32. Type 1 (secEnterprise), and then press **Enter**.

```

SAP BusinessObjects

Choose the number of the type of authentication to
use when contacting the CMS

1 - secEnterprise
2 - secLDAP

[back/quit(0)]

[1]
```

33. Type **yes**, and then press **Enter**.

```

SAP BusinessObjects

The following information will be used to create the new
Server Intelligence Agent.

CMS Name: SHRLR02
Server Intelligence Agent Name: PRD_SHR
Server Intelligence Agent Port: 6410
Create Default Servers: yes
CMS Port: 6400
CMS Database: SHRLR02BOE120
Audit Database: SHRLR02BOE120_AUDIT

Do you want to create the Server Intelligence Agent?

[yes(3)/no(2)/back(1)/quit(0)]

[yes]
Adding Server Intelligence Agent...
.....
Please press Enter to continue...
█
```

34. Press **Enter**.

35. Type **4**, and then press **Enter**. You will see the list of all the Server Intelligence Agents.

```

SAP BusinessObjects

What would you like to do?

1 - Add a Server Intelligence Agent
2 - Delete a Server Intelligence Agent
3 - Modify a Server Intelligence Agent
4 - List all Server Intelligence Agents in the config file

[quit(0)]

[4]4
```

36. Type 0 to quit, and then press **Enter**. You will see the message "*Thank you for choosing SAP BusinessObjcets...*"
37. Run the following command to start the newly added agent:  
`sh /opt/HP/BSM/BO/bobje/startservers`
38. Run the following command:
  - a. `cd /opt/HP/BSM/BO/bobje`
  - b. `./ccm.sh -updateobjects -cms <SHR_hostname>:6400.`

If you have a password for CCM, then run the following command:

```
./ccm.sh -updateobjects -cms SHR_hostname>:6400 -username Administrator -
password <administratorpassword>
```

```
Creating session manager...
Logging onto CMS...
Creating infostore...
Objects requiring update: 0
Adding objects...
CMS Data Source setup finished.
```

## For Management Database Table

1. Run the following commands to launch PgAdminIII:
  - a. `cd $PMDB_HOME/./Postgres/bin`
  - b. `./psql -U pmdb_admin -d dwabc -p 21425`
2. Connect to the database by providing the same password which was configured during post installation.
3. Launch the SQL query analyzer.
4. Run the following query to restore the database tables:  
`Delete From aggregate_control`  
`COPY aggregate_control from '<backup_path>/backup_AGGREGATE_CONTROL.dat';`  
In this instance, *<backup\_path>* is the directory where you placed the backup of management database file.

# Part V: References

This section lists the SiteScope monitors that are used to collect the virtualization metrics and also provides information to install Xcelsius application.

## Appendix A: SiteScope Monitors for SHR

The following table lists the monitors that are used to collect the virtualization metrics:

| Monitor Name       | Counter                  | Measure Name                        |
|--------------------|--------------------------|-------------------------------------|
| VMware Performance | HostSystem\state         | hardware.memorySize                 |
| VMware Performance | HostSystem\state         | summary.hardware.numCpuCores        |
| VMware Performance | HostSystem\state         | summary.hardware.cpuMhz             |
| VMware Performance | HostSystem\state         | summary.hardware.numNics            |
| VMware Performance | HostSystem\Realtime\sys  | uptime.latest[]                     |
| VMware Performance | HostSystem\Realtime\mem  | usage.average[]                     |
| VMware Performance | HostSystem\Realtime\mem  | consumed average[]                  |
| VMware Performance | HostSystem\Realtime\cpu  | usage.average[]                     |
| VMware Performance | HostSystem\Realtime\cpu  | ready.summation[]                   |
| VMware Performance | HostSystem\Realtime\disk | usage.average[]                     |
| VMware Performance | HostSystem\Realtime\disk | read.average[]                      |
| VMware Performance | HostSystem\Realtime\disk | write.average[]                     |
| VMware Performance | HostSystem\Realtime\net  | received.average[]                  |
| VMware Performance | HostSystem\Realtime\net  | transmitted.average[]               |
| VMware Performance | HostSystem\Realtime\net  | packetsRx.summation[]               |
| VMware Performance | HostSystem\Realtime\net  | packetsTx.summation[]               |
| VMware Performance | HostSystem\Realtime\net  | usage.average[]                     |
| VMware Performance | HostSystem\Realtime\mem  | usage.average                       |
| VMware Performance | HostSystem\Realtime\mem  | consumed.average                    |
| VMware Performance | Virtual Machine\state    | config.hardware.memoryMB            |
| VMware Performance | Virtual Machine\state    | config.cpuAllocation.shares.shares  |
| VMware Performance | Virtual Machine\state    | config.hardware.numcpu              |
| VMware Performance | Virtual Machine\state    | config.memoryAllocation.reservation |

| Monitor Name       | Counter                      | Measure Name                     |
|--------------------|------------------------------|----------------------------------|
| VMware Performance | Virtual Machine\state        | config.memoryAllocation.limit    |
| VMware Performance | Virtual Machine\state        | config.cpuAllocation.reservation |
| VMware Performance | Virtual Machine\state        | config.cpuAllocation.limit       |
| VMware Performance | Virtual Machine\mem          | active.average[]                 |
| VMware Performance | Virtual Machine\Realtime\sys | uptime.latest[]                  |
| VMware Performance | Virtual Machine\Realtime\mem | usage.average[]                  |
| VMware Performance | Virtual Machine\Realtime\mem | consumed.average[]               |
| VMware Performance | Virtual Machine\Realtime\mem | active.average[]                 |
| VMware Performance | Virtual Machine\Realtime\mem | overhead.average[]               |
| VMware Performance | Virtual Machine\Realtime\mem | swpin.average[]                  |
| VMware Performance | Virtual Machine\Realtime\mem | swapout.average[]                |
| VMware Performance | Virtual Machine\Realtime\mem | vmmemctltarget.average[]         |
| VMware Performance | Virtual Machine\Realtime\mem | usage.average[]                  |
| VMware Performance | Virtual Machine\Realtime\mem | ready.summation[]                |
| VMware Performance | Virtual Machine\Realtime\mem | usagemhz.average[]               |
| VMware Performance | Virtual Machine\Realtime\mem | wait.summation[]                 |
| VMware Performance | Virtual Machine\Realtime\mem | ready.summation[]                |
| VMware Performance | Virtual Machine\Realtime\mem | usage.average[]                  |
| VMware Performance | Virtual                      | read.average[]                   |

| Monitor Name       | Counter                      | Measure Name          |
|--------------------|------------------------------|-----------------------|
|                    | Machine\Realtime\mem         |                       |
| VMware Performance | Virtual Machine\Realtime\mem | write.average[]       |
| VMware Performance | Virtual Machine\Realtime\mem | received.average[]    |
| VMware Performance | Virtual Machine\Realtime\mem | transmitted.average[] |
| VMware Performance | Virtual Machine\Realtime\mem | packetsRx.summation[] |
| VMware Performance | Virtual Machine\Realtime\mem | packetsTx.summation[] |
| VMware Performance | Virtual Machine\Realtime\mem | usage.average[]       |
| VMware Performance | Virtual Machine\Realtime\cpu | usage.average[]       |
| VMware Performance | Virtual Machine\Realtime\cpu | ready.summation[]     |
| VMware Performance | Virtual Machine\Realtime\cpu | usagemhz.average[]    |
| VMware Performance | Virtual Machine\Realtime\cpu | wait.summation[]      |
| VMware Performance | Virtual Machine\Realtime\cpu | ready.summation[]     |
| VMware Performance | Virtual Machine\Realtime\net | received.average[]    |
| VMware Performance | Virtual Machine\Realtime\net | transmitted.average[] |
| VMware Performance | Virtual Machine\Realtime\net | packetsRx.summation[] |
| VMware Performance | Virtual Machine\Realtime\net | packetsTx.summation[] |
| VMware Performance | Virtual Machine\Realtime\net | usage.average[]       |
| VMware Performance | Virtual                      | read.average[]        |

| Monitor Name       | Counter                       | Measure Name    |
|--------------------|-------------------------------|-----------------|
|                    | Machine\Realtime\disk         |                 |
| VMware Performance | Virtual Machine\Realtime\disk | write.average[] |
| VMware Performance | Virtual Machine\Realtime\disk | usage.average[] |

The following table lists the monitors that are used to collect the system management metrics:

| Monitor                     | Objects           | Counter                  | System Type            |
|-----------------------------|-------------------|--------------------------|------------------------|
| Microsoft Windows Resources | Memory            | % Committed Bytes In Use | Windows                |
| Microsoft Windows Resources | memory            | Pages Output/sec         | Windows                |
| Microsoft Windows Resources | System            | Processor Queue Length   | Windows                |
| Microsoft Windows Resources | System            | System Up Time           | Windows                |
| Microsoft Windows Resources | Physical Disk     | Total\Disk Bytes/sec     | Windows                |
| Microsoft Windows Resources | Physical Disk     | Disk Read Bytes/sec      | Windows                |
| Microsoft Windows Resources | Physical Disk     | Disk Write Bytes/sec     | Windows                |
| Microsoft Windows Resources | Physical Disk     | Disk Bytes/sec           | Windows                |
| Microsoft Windows Resources | Network Interface | %Packets Received/sec    | Windows                |
| Microsoft Windows Resources | Network Interface | %Bytes Received/sec      | Windows                |
| Microsoft Windows Resources | Network Interface | %Bytes Sent/sec          | Windows                |
| Microsoft Windows Resources | Network Interface | %Packets/sec             | Windows                |
| Microsoft Windows Resources | Network Interface | %Packets Sent/sec        | Windows                |
| Microsoft Windows Resources | Network Interface | BytesTotal/sec           | Windows                |
|                             |                   |                          |                        |
| Unix Resources              | Queue length      | Queue length\runq-sz     | Unix/Solaris           |
| Unix Resources              | Queue Statistics  | Queue Statistics\runq-sz | HP-UX/AIX              |
| Unix Resources              | Uptime            | Uptime\Uptime            | Unix /Linux, HP-UX/AIX |
| Unix Resources              | File System       | %\capacity               | Unix/Solaris           |
| Unix Resources              | File System       | %\kbytes                 | Unix/Solaris           |
| Unix Resources              | File System       | avail                    | Solaris                |



| Monitor            | Objects           | Counter           | System Type  |
|--------------------|-------------------|-------------------|--------------|
| Unix Resources     | File System       | used              | Solaris      |
| Unix Resources     | File System       | %\Use\%           | RHEL         |
| Unix Resources     | File System       | %\Used            | RHEL         |
| Unix Resources     | File System       | %\Capacity        | HP-UX        |
| Unix Resources     | File System       | %\%Used           | HP-UX, AIX   |
| Unix Resources     | File System       | %\1024-blocks     | AIX          |
| Unix Resources     | File System       | %\Free            |              |
| Unix Resources     | File System       | 1K-blocks         | RHEL         |
| Unix Resources     | File System       | Available         | RHEL         |
| Unix Resources     | Network Interface | %packets          | RHEL         |
| Unix Resources     | Network Interface | %ReceiveBytes     | RHEL         |
| Unix Resources     | Network Interface | %TransmitBytes    | RHEL         |
| Unix Resources     | Network Interface | %ipackets         | Solaris      |
| Unix Resources     | Network Interface | %opackets         | Solaris      |
| Unix Resources     | Network Interface | %rbytes           | Solaris      |
| Unix Resources     | Network Interface | %obytes           | Solaris      |
| Unix Resources     | Network Stats     | %lpkts            | HP-UX        |
| Unix Resources     | Network Stats     | %Opkts            | HP-UX        |
|                    |                   |                   |              |
| Dynamic Disk space | Disk/FileSystem   | %/MB free **      | Unix/Windows |
| Dynamic Disk space | Disk/FileSystem   | %/MB total **     | Unix/Windows |
| Dynamic Disk space | Disk/FileSystem   | %/percent full ** | Unix/Windows |
|                    |                   |                   |              |
| CPU                | N/A               | utilization       | Unix/Windows |
| CPU                | N/A               | utilization cpu%  | Unix/Windows |
|                    |                   |                   |              |
| Memory             | N/A               | Percent used      | Unix/Windows |

| Monitor | Objects | Counter                   | System Type  |
|---------|---------|---------------------------|--------------|
| Memory  | N/A     | virtual memory used %     | Unix/Windows |
| Memory  | N/A     | physical memory used % *  | Unix/Windows |
| Memory  | N/A     | swap space used %         | Unix/Windows |
| Memory  | N/A     | physical memory MB Free * | Unix/Windows |
| Memory  | N/A     | virtual memory MB Free    | Unix/Windows |
| Memory  | N/A     | MB Free                   | Unix/Windows |

\* The counter is available only when Windows node is connected with WMI method.

\*\* The counter is not available when Windows node is connected with WMI method.

## Appendix B: Installing Xcelsius

An Xcelsius report is an interactive Flash-based report created by using the SAP BusinessObjects Xcelsius Enterprise tool. To create Xcelsius Flash-based reports in SHR, you must install the Xcelsius application, which is included on the SHR installation media. Xcelsius is not essential for viewing the SHR reports. Therefore, installation it is optional.

**Note:** Microsoft Excel, as a base, is a prerequisite for Xcelsius.

## Hardware and Software Requirements

For the list of hardware and software requirements of Xcelsius 2008 Service Pack 5, see its documentation from [SAP](#).

## Installing Xcelsius (Optional)

The `setup` file for installing Xcelsius 2008 Service Pack 5 is bundled with the SHR installation media.

Perform the following steps to obtain the `setup` executable:

1. On the SHR installation media, browse to the `\packages` folder.
2. Select the `Xcelsius.zip` file, copy it to a location of your choice, and extract it.
3. From the extracted folder, browse to the `\Xcelsius_2008_SP5` folder and run the `setup` executable.

For more information on the installation, see the *SAP BusinessObjects Xcelsius 2008 Installation Guide* available from [SAP](#).

## Appendix C: Listing of ETLs

This section list the ETLs for the Content Packs. To generate reports, make sure to select atleast one domain Content Pack, ETL Content Pack, and report Content Pack. The dependent domain Content Pack get selected automatically, you have to select only the ETLs based on the data source.

The timer service will be stopped automatically during install/uninstall/upgrade operation and will be started once operation is complete.

During install/uninstall process, Deployment Manager does not allow you to interrupt the process. Instead, you must wait till the current process is complete before you can perform any other operations on the Deployment Manager page.

The following table list the ETLs for each content pack:

| Content Pack Name              | ETL                                   | Comments                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cross-Domain Operations Events | CrossOprEvent_ETL_OMi                 | If the topology source is OMi 10, select the CrossOprEvent_ETL_OMi10 component.                                                                                                                                                                                                                                                                        |
|                                | CrossOprEvent_ETL_OMi10               |                                                                                                                                                                                                                                                                                                                                                        |
|                                | CrossOprEvent_Domain_Reports          | The Content Pack components 'CrossOprEvent_ETL_OMi' and 'CrossOprEvent_ETL_OMi10' are mutually exclusive. Ensure that only one of them is selected.                                                                                                                                                                                                    |
|                                | CrossOprEvent_ETL_OMi10_Extended      |                                                                                                                                                                                                                                                                                                                                                        |
|                                | CrossOprEvent_ETL_OMi_Extended        | The Content Pack components 'CrossOprEvent_ETL_OMi_Extended' and 'CrossOprEvent_ETL_OMi10_Extended' are mutually exclusive. Ensure that only one of them is selected.                                                                                                                                                                                  |
|                                | CrossOprEvent_Domain_Reports_Extended |                                                                                                                                                                                                                                                                                                                                                        |
|                                |                                       | <p><b>Note:</b> Select the Extended ETLs to generate customized reports that involves Event detail attributes.</p> <p><b>Note:</b> You have to select one of the Health and Key Performance Indicators ETLs explicitly because Cross-Domain Operations Events Content Pack has a dependency on Health and Key Performance Indicators Content Pack.</p> |
| Health and Key Performance     | HIKPI_ETL_ServiceHealth               | If the topology source is OMi 10, select the HIKPI_ETL_ServiceHealth_OMi10                                                                                                                                                                                                                                                                             |

| Content Pack Name                | ETL                                   | Comments                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Indicators                       | HIKPI_ETL_ServiceHealth_OMi10         | component.<br><br>The Content Pack components 'HIKPI_ETL_ServiceHealth' and 'HIKPI_ETL_ServiceHealth_OMi10' are mutually exclusive. Ensure that only one of them is selected.                                                                                                                                                                                                            |
|                                  | HIKPI_Domain                          |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | HIKPI_Reports_ServiceHealth           |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  |                                       |                                                                                                                                                                                                                                                                                                                                                                                          |
| IBM WebSphere Application Server | IBMWebSphere_ETL_WebSphereSPI         | If you have installed IBM WebSphere SPI ETL already and are migrating from OM to OMi10 or upgrading to latest OMi Management Pack for WebSphere, uninstall the IBM WebSphere SPI ETL and deploy the latest IBM WebSphere MP ETL.                                                                                                                                                         |
|                                  | IBMWebSphere_Domain                   |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | IBMWebSphere_Reports                  |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | IBMWebSphere_ETL_WebSphereMP          |                                                                                                                                                                                                                                                                                                                                                                                          |
| Microsoft Active Directory       | MicrosoftActiveDirectory_ETL_ADSPI    |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | MicrosoftActiveDirectory_Reports      |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | MicrosoftActiveDirectory_Domain       |                                                                                                                                                                                                                                                                                                                                                                                          |
| Microsoft Exchange Server        | MicrosoftExchange_ETL_ExchangeSPI2007 | The MicrosoftExchange_ETL_ExchangeSPI2007 collects data from HP Operations SPI for Exchange Server 2007.<br><br>The MicrosoftExchange_ETL_ExchangeSPI2010 collects data from HP Operations SPI and OMi management pack for Exchange Server 2010.<br><br>The MicrosoftExchange_ETL_ExchangeSPI2013 collects data from HP Operations SPI and OMi management pack for Exchange Server 2013. |
|                                  | MicrosoftExchange_ETL_ExchangeSPI2010 |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | MicrosoftExchange_ETL_ExchangeSPI2013 |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | MicrosoftExchange_Domain              |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | MicrosoftExchange_Reports             |                                                                                                                                                                                                                                                                                                                                                                                          |
| Microsoft SQL Server             | MicrosoftSQLServer_ETL_DBSPI          |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | MicrosoftSQLServer_Domain             |                                                                                                                                                                                                                                                                                                                                                                                          |
|                                  | MicrosoftSQLServer_Reports            |                                                                                                                                                                                                                                                                                                                                                                                          |
| Network Performance              | NetworkPerf_ETL_PerfiSPI_NonRTSM      | The Content Pack components 'NetworkPerf_ETL_PerfiSPI_NonRTSM' and 'NetworkPerf_ETL_PerfiSPI_RTSM' are mutually exclusive. Ensure that only one of them is selected.                                                                                                                                                                                                                     |
|                                  | NetworkPerf_ETL_PerfiSPI_             |                                                                                                                                                                                                                                                                                                                                                                                          |

| Content Pack Name                | ETL                                                                                                                | Comments                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  | RTSM<br>NetworkPerf_Domain<br>NetworkPerf_Reports                                                                  | <p><b>Note:</b> If the NNMi topology is integrated to BSM/OMi RTSM, select NetworkPerf_ETL_PerfiSPI_RTSM Content Pack component. If else, select NetworkPerf_ETL_PerfiSPI_NonRTSM Content Pack component.</p> <p><b>Note:</b> The Network Performance Content Pack collects data only from Type2 NodeGroups, that is, routers and switches.</p> |
| Operations Events                | OprEvent_ETL_HPOM<br>OprEvent_Domain_Reports                                                                       |                                                                                                                                                                                                                                                                                                                                                 |
| Oracle                           | Oracle_ETL_DBSPI<br>Oracle_Domain<br>Oracle_Reports                                                                |                                                                                                                                                                                                                                                                                                                                                 |
| Oracle WebLogic Server           | OracleWebLogic_ETL_WebLogicSPI<br>OracleWebLogic_Domain<br>OracleWebLogic_Reports<br>OracleWebLogic_ETL_WebLogicMP | If you have installed WebLogic SPI ETL already and are migrating from OM to OMi10 or upgrading to latest OMi Management Pack for WebLogic, uninstall the Oracle WebLogic SPI ETL and deploy the latest Oracle WebLogic MP ETL.                                                                                                                  |
| Real User Transaction Monitoring | RealUsrTrans_ETL_RUM<br>RealUsrTrans_ETL_RUM_OMi<br>RealUsrTrans_Domain_Reports                                    | <p>If the topology source is OMi 10, select the RealUsrTrans_ETL_RUM_OMi component.</p> <p>The Content Pack components 'RealUsrTrans_ETL_RUM' and 'RealUsrTrans_ETL_RUM_OMi' are mutually exclusive. Ensure that only one of them is selected.</p>                                                                                              |
| Synthetic Transaction Monitoring | SynTrans_Domain_Reports<br>SynTrans_ETL_BPM<br>SynTrans_ETL_BPM_OMi                                                | <p>If the topology source is OMi 10, select the SynTrans_ETL_BPM_OMi component.</p> <p>The Content Pack components 'SynTrans_ETL_BPM' and 'SynTrans_ETL_BPM_OMi' are mutually exclusive. Ensure that only one of them is selected.</p>                                                                                                          |

| Content Pack Name               | ETL                                              | Comments                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Performance              | SysPerf_ETL_PerformanceAgent                     | If HP Operations Agent is the data source, select the SysPerf_ETL_PerformanceAgent Content Pack component.                                                                                                                                                                                                                                                                                                                                                                            |
|                                 | SysPerf_ETL_SiS                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | SysPerf_ETL_SiS_API                              | Select only one of the three Content Pack component, SysPerf_ETL_SiS or SysPerf_ETL_SiS_DB or SysPerf_ETL_SiS_API.                                                                                                                                                                                                                                                                                                                                                                    |
|                                 | SysPerf_ETL_SiS_DB                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | SysPerf_Domain                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | SysPerf_Reports                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 |                                                  | The SysPerf_ETL_SiS is deprecated in SHR 9.4. The SysPerf_ETL_SiS_DB is for Profile DB integration. If the topology source is BSM 9.x and you have already installed the SysPerf_ETL_SiS_DB, you can continue to use the same. The SysPerf_ETL_SiS_API is for OMi 10.0 integration. You can use this Content Pack component even in the absence of Profile DB. The list of metrics collected by SysPerf_ETL_SiS_DB and SysPerf_ETL_SiS_API are same.                                  |
| Virtual Environment Performance | VirtualEnvPerf_ETL_HyperV_PerformanceAgent       | If the data source is HP Operations Agent or Performance Agent, select Performance Agent based Content Pack components.                                                                                                                                                                                                                                                                                                                                                               |
|                                 | VirtualEnvPerf_ETL_IBMLPAR_PerformanceAgent      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | VirtualEnvPerf_ETL_SolarisZones_PerformanceAgent | If the data source is VMware vCenter, select VMWare_vCenter based Content Pack components.                                                                                                                                                                                                                                                                                                                                                                                            |
|                                 | VirtualEnvPerf_ETL_VMWare_PerformanceAgent       | Select either VirtualEnvPerf_ETL_VMware_SiteScope or VirtualEnvPerf_ETL_VMware_SiS_API Content Pack component.                                                                                                                                                                                                                                                                                                                                                                        |
|                                 | VirtualEnvPerf_ETL_VMware_SiS_API                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | VirtualEnvPerf_ETL_VMware_SiteScope              | The VirtualEnvPerf_ETL_VMware_SiteScope is for Profile DB integration. If the topology source is BSM 9.x and you have already installed the VirtualEnvPerf_ETL_VMware_SiteScope, you can continue to use the same. The VirtualEnvPerf_ETL_VMware_SiS_API is for OMi 10.0 integration. You can use this Content Pack component even in the absence of Profile DB. The list of metrics collected by VirtualEnvPerf_ETL_VMware_SiteScope and VirtualEnvPerf_ETL_VMware_SiS_API are same. |
|                                 | VirtualEnvPerf_Domain                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | VirtualEnvPerf_Domain_VMWare                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | VirtualEnvPerf_Reports                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | VirtualEnvPerf_Reports_VMWare                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Content Pack Name | ETL                               | Comments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | VirtualEnvPerf_ETL_VMWare_vCenter | <p>The Content Pack components 'VirtualEnvPerf_ETL_VMWare_vCenter' and 'VirtualEnvPerf_ETL_VMWare_PerformanceAgent' are mutually exclusive. Ensure that only one of them is selected.</p> <p><b>Note:</b> The HP Service Health Reporter supports HP Virtualization Performance Viewer (vPV). SHR collects data for reporting on performance, configuration, and capacity problems in the virtual environments from HP vPV. For more information on the integration of SHR with vPV, see User Guide from the following URL:</p> <p><a href="https://hpln.hp.com/contentoffering/hp-shr-vpv-integration-content">https://hpln.hp.com/contentoffering/hp-shr-vpv-integration-content</a></p> |



## Appendix D: Troubleshooting for Aggregation of Data Failed After Migration

**Description:** The aggregation of data fails if the `PMDB_HOME` directory structure in the new SHR system is different from System 1.

**Resolution:** Perform the following steps to resolve the issue:

1. In System 2 (the system where you have migrated the SHR component), go to the **Start > Programs > PostgreSQL 9.0 > pgAdmin III**.
2. Connect to the database by providing the password `PMDB92_admin@hp`.
3. Launch the sql query analyzer by clicking the sql icon.
4. Execute the following command:

```
update dwabc.job_stream_step_dt set arguments=replace(arguments,DRIVE_
LETTER'Path of the PMDB_FOLDER','%PMDB_HOME%') where
executableidentifier='AGGREGATE'
```

**Example:** `update dwabc.job_stream_step_dt set arguments=replace
(arguments,E'E:\\HP-SHR\\PMDB','%PMDB_HOME%') where
executableidentifier='AGGREGATE'`

**Note:** Ensure that the Path of the `PMDB_FOLDER` contains `\\` and not a `\`.

5. Ensure that all the SHR services are running,

# 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 Configuration 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](mailto:docfeedback@hp.com).

We appreciate your feedback!